II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2016/799 DER KOMMISSION

vom 18. März 2016

zur Durchführung der Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates zur Festlegung der Vorschriften über Bauart, Prüfung, Einbau, Betrieb und Reparatur von Fahrtenschreibern und ihren Komponenten

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr ([1]), insbesondere auf Artikel 11 und Artikel 12 Absatz 7,

in Erwägung nachstehender Gründe:

(1) Mit der Verordnung (EU) Nr. 165/2014 wurden digitale Fahrtenschreiber der zweiten Generation, sogenannte „intelligente Fahrtenschreiber", eingeführt, die auch eine Anbindung an das globale Satellitennavigationssystem („GNSS"), eine Ausrüstung zur Früherkennung per Fernkommunikation und eine Schnittstelle zu intelligenten Verkehrssystemen umfassen. Die Spezifikationen für die technischen Anforderungen an die Bauart von intelligenten Fahrtenschreibern sollten festgelegt werden.

(2) Die Ausrüstung zur Früherkennung per Fernkommunikation nach Artikel 9 Absatz 4 der Verordnung (EU) Nr. 165/2014 sollte den Kontrolleuren bei Straßenkontrollen die Daten des digitalen Fahrtenschreibers und die Angaben zu Gewicht und Achslast der gesamten Fahrzeugkombination (Zugmaschine und Anhänger oder Sattelanhänger) gemäß der Richtlinie 96/53/EG des Europäischen Parlaments und des Rates ([2]) übermitteln. Dies dürfte eine wirksame und rasche Prüfung von Fahrzeugen durch die Kontrollbehörden mit weniger elektronischen Geräten in der Fahrerkabine ermöglichen.

(3) Gemäß der Richtlinie 96/53/EG sollte die Ausrüstung zur Früherkennung per Fernkommunikation die in dieser Richtlinie genannten CEN DSRC-Normen ([3]) auf dem Frequenzband im Bereich zwischen 5 795-5 805 MHz verwenden. Da dieses Frequenzband auch für die elektronische Mauterhebung genutzt wird, sollten die Kontrolleure die Ausrüstung zur Früherkennung per Fernkommunikation nicht an einer Mautstelle nutzen, um Interferenzen zwischen Mauterhebungs- und Kontrollanwendungen zu vermeiden.

(4) Neue Sicherheitsmechanismen zur Aufrechterhaltung des Sicherheitsniveaus des digitalen Fahrtenschreibers sollten zusammen mit dem intelligenten Fahrtenschreiber eingeführt werden, um derzeitige Sicherheitsschwachstellen zu beseitigen. Eine dieser Schwachstellen ist das Fehlen von Ablaufdaten der digitalen Zertifikate. Gemäß bewährten Verfahren in Sicherheitsfragen wird empfohlen, die Verwendung von digitalen Zertifikaten ohne Ablaufdaten zu vermeiden. Die normale Gültigkeitsdauer für den Betrieb von Fahrzeugeinheiten sollte 15 Jahre betragen, gerechnet ab dem Ausstellungsdatum der digitalen Zertifikate für die Fahrzeugeinheit. Fahrzeugeinheiten sollten nach Ablauf dieser Gültigkeitsdauer ersetzt werden.

([1]) ABl. L 60 vom 28.2.2014, S. 1.
([2]) Richtlinie 96/53/EG des Rates vom 25. Juli 1996 zur Festlegung der höchstzulässigen Abmessungen für bestimmte Straßenfahrzeuge im innerstaatlichen und grenzüberschreitenden Verkehr in der Gemeinschaft sowie zur Festlegung der höchstzulässigen Gewichte im grenzüberschreitenden Verkehr (ABl. L 235 vom 17.9.1996, S. 59).
([3]) Die Normen für dedizierte Kurzstreckenkommunikation (DSRC) des Europäischen Komitees für Normung (CEN) EN 12253, EN 12795, EN 12834, EN 13372 sowie ISO 14906.

(5) Die Bereitstellung sicherer und verlässlicher Positionsbestimmungsinformationen ist ein wesentliches Element für den effektiven Betrieb der intelligenten Fahrtenschreiber. Es ist daher angezeigt, ihre Kompatibilität mit den in der Verordnung (EU) Nr. 1285/2013 des Europäischen Parlaments und des Rates ([1]) im Hinblick auf die Verbesserung der Sicherheit des digitalen Fahrtenschreibers dargelegten Mehrwertleistungen im Rahmen des Programms Galileo sicherzustellen.

(6) Gemäß Artikel 8 Absatz 1, Artikel 9 Absatz 1 und Artikel 10 Absätze 1 und 2 der Verordnung (EU) Nr. 165/2014 sollten die durch diese Verordnung eingeführten Sicherheitsmechanismen 36 Monate nach dem Inkrafttreten der erforderlichen Durchführungsrechtsakte zur Anwendung kommen, damit die Hersteller eine neue Generation intelligenter Fahrtenschreiber entwickeln und von den zuständigen Behörden die Typgenehmigungsbögen erhalten können.

(7) Gemäß der Verordnung (EU) Nr. 165/2014 sollten Fahrzeuge, die 36 Monate nach dem Inkrafttreten dieser Verordnung der Kommission erstmals in einem Mitgliedstaat zugelassen werden, mit einem intelligenten Fahrtenschreiber ausgerüstet sein, der den Anforderungen dieser Verordnung der Kommission entspricht. Auf jeden Fall sollten alle Fahrzeuge, die in einem anderen Mitgliedstaat als dem Zulassungsmitgliedstaat betrieben werden, 15 Jahre nach dem Zeitpunkt der Anwendung dieser Anforderungen mit einem intelligenten Fahrtenschreiber ausgerüstet sein.

(8) Gemäß der Verordnung (EG) Nr. 68/2009 der Kommission ([2]) war während eines Übergangszeitraums, der am 31. Dezember 2013 endete, die Verwendung eines Adapters gestattet, um den Einbau von Fahrtenschreibern in Fahrzeuge der Klassen M1 und N1 zu ermöglichen. Aufgrund technischer Schwierigkeiten bei der Suche nach einer Alternative für die Verwendung des Adapters sind Experten aus der Automobil- und der Fahrtenschreiberindustrie gemeinsam mit der Kommission zu dem Schluss gelangt, dass keine Alternativlösung zum Adapter besteht, die nicht mit übermäßig hohen Kosten für die Industrie, die in keinem Verhältnis zur Größe des Marktes stünden, verbunden wäre. Daher sollte die Verwendung des Adapters in Fahrzeugen der Klassen M1 und N1 Fahrzeuge unbefristet zugelassen werden.

(9) Die in der vorliegenden Verordnung vorgesehenen Maßnahmen stehen in Einklang mit der Stellungnahme des gemäß Artikel 42 Absatz 3 der Verordnung (EU) Nr. 165/2014 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand und Geltungsbereich

1. Diese Verordnung legt die notwendigen Bestimmungen für die einheitliche Behandlung folgender Aspekte des Fahrtenschreibers fest:

a) Aufzeichnung der Position des Fahrzeugs an bestimmten Punkten während der täglichen Arbeitszeit des Fahrers;

b) Früherkennung von möglicher Manipulation oder möglichem Missbrauch des intelligenten Fahrtenschreibers per Fernkommunikation;

c) Schnittstelle zu intelligenten Verkehrssystemen;

d) administrative und technische Anforderungen an Typgenehmigungsverfahren von Fahrtenschreibern, einschließlich der Sicherheitsmechanismen.

2. Bauart, Prüfung, Einbau, Nachprüfung, Betrieb und Reparatur von intelligenten Fahrtenschreibern und ihren Komponenten müssen den technischen Anforderungen des Anhangs 1C dieser Verordnung genügen.

3. Andere als intelligente Fahrtenschreiber müssen — hinsichtlich Bauart, Prüfung, Einbau, Nachprüfung, Betrieb und Reparatur — weiterhin den Anforderungen des Anhangs 1 bzw. des Anhangs 1B der Verordnung (EWG) Nr. 3821/85 des Rates ([3]) genügen.

([1]) Verordnung (EU) Nr. 1285/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 betreffend den Aufbau und den Betrieb der europäischen Satellitennavigationssysteme und zur Aufhebung der Verordnung (EG) Nr. 876/2002 des Rates und der Verordnung (EG) Nr. 683/2008 des Europäischen Parlaments und des Rates (ABl. L 347 vom 20.12.2013, S. 1).

([2]) Verordnung (EG) Nr. 68/2009 der Kommission vom 23. Januar 2009 zur neunten Anpassung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr an den technischen Fortschritt (ABl. L 21 vom 24.1.2009, S. 3).

([3]) Verordnung (EWG) Nr. 3821/85 des Rates vom 20. Dezember 1985 über das Kontrollgerät im Straßenverkehr (ABl. L 370 vom 31.12.1985, S. 8).

4. Gemäß Artikel 10d der Richtlinie 96/53/EG des Europäischen Parlaments und des Rates übermittelt die Ausrüstung zur Früherkennung per Fernkommunikation auch die von bordeigenen Wiegesystemen bereitgestellten Gewichtsdaten zum Zweck der frühzeitigen Aufdeckung von Betrugsfällen.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die Begriffsbestimmungen in Artikel 2 der Verordnung (EU) Nr. 165/2014.

Zusätzlich gelten folgende Begriffsbestimmungen:

1) „digitaler Fahrtenschreiber" oder „Fahrtenschreiber der ersten Generation" ist ein digitaler Fahrtenschreiber, bei dem es sich nicht um einen intelligenten Fahrtenschreiber handelt;

2) „externe GNSS-Ausrüstung" ist eine Ausrüstung, die den GNSS-Empfänger (wenn die Fahrzeugeinheit nicht aus einem Einzelgerät besteht) sowie andere Komponenten enthält, die erforderlich sind für den Schutz der Kommunikation der Positionsdaten an die übrige Fahrzeugeinheit;

3) „Informationsdossier" ist das Gesamtdossier in elektronischer Form oder auf Papier, das alle Angaben enthält, die der Hersteller oder dessen Beauftragter der Typgenehmigungsbehörde für die Zwecke der Typgenehmigung des Fahrtenschreibers oder einer seiner Komponenten vorgelegt hat, einschließlich der Zertifikate nach Artikel 12 Absatz 3 der Verordnung (EU) Nr. 165/2014, der Durchführung der Prüfungen gemäß Anhang 1C dieser Verordnung sowie Zeichnungen, Fotografien und anderer relevanter Unterlagen;

4) „Informationspaket" ist das Informationsdossier in elektronischer Form oder auf Papier, zusammen mit etwaigen anderen Unterlagen, die die Typgenehmigungsbehörde im Zuge der Wahrnehmung ihrer Aufgaben dem Informationsdossier beigefügt hat, darunter auch — am Ende des Typgenehmigungsverfahrens — der EG-Typgenehmigungsbogen des Fahrtenschreibers oder einer seiner Komponenten;

5) „Inhaltsverzeichnis des Informationspakets" ist die Unterlage, in der der nummerierte Inhalt des Informationspakets einschließlich aller relevanten Teile dieses Pakets aufgeführt ist. Das Format dieser Unterlage muss die Unterscheidung der aufeinander folgenden Schritte im Verfahren für die Erteilung der EG-Typgenehmigung, einschließlich der Daten etwaiger Überarbeitungen und Aktualisierungen dieses Pakets, erlauben;

6) „Ausrüstung zur Früherkennung per Fernkommunikation" ist die Ausrüstung der Fahrzeugeinheit, die zur Durchführung gezielter Straßenkontrollen verwendet wird;

7) „intelligenter Fahrtenschreiber" oder „Fahrtenschreiber der zweiten Generation" ist ein digitaler Fahrtenschreiber gemäß den Artikeln 8, 9 und 10 der Verordnung (EU) Nr. 165/2014 sowie gemäß Anhang 1C dieser Verordnung.

8) „Komponente eines Fahrtenschreibers" oder „Komponente" ist eines der folgenden Bestandteile: die Fahrzeugeinheit, der Bewegungssensor, die Fahrtenschreiberkarte, das Schaublatt, die externe GNSS-Ausrüstung oder die Ausrüstung zur Früherkennung per Fernkommunikation;

9) „Typgenehmigungsbehörde" ist die Behörde eines Mitgliedstaats, die für die Durchführung der Typgenehmigung des Fahrtenschreibers oder seiner Komponenten, das Zulassungsverfahren, die Ausstellung und gegebenenfalls den Entzug von Typgenehmigungsbögen zuständig ist, die als Kontaktstelle für die Genehmigungsbehörden der anderen Mitgliedstaaten fungiert und sicherstellt, dass die Hersteller ihren Verpflichtungen im Hinblick auf die Erfüllung der Anforderungen dieser Verordnung nachkommen.

Artikel 3

Standortgestützte Dienste

1. Die Hersteller gewährleisten, dass intelligente Fahrtenschreiber mit den durch das Satelliten-Navigationssystem Galileo und die Europäische Erweiterung des geostationären Navigationssystems (EGNOS) erbrachten Positionsbestimmungsdiensten kompatibel sind.

2. Zusätzlich zu den in Absatz 1 genannten Systemen können die Hersteller auch die Kompatibilität mit anderen Satellitennavigationssystemen gewährleisten.

Artikel 4

Verfahren für die Typgenehmigung von Fahrtenschreibern und Komponenten des Fahrtenschreibers

1. Der Hersteller oder dessen Beauftragter beantragt die Typgenehmigung für einen Fahrtenschreiber oder eine seiner Komponenten oder Gruppe von Komponenten bei der von einem Mitgliedstaat benannten Typgenehmigungsbehörde. Der Antrag umfasst ein Informationsdossier mit den Angaben zu jeder einzelnen Komponente, einschließlich, falls vorhanden, der Typgenehmigungsbögen von anderen, zur Vervollständigung des Fahrtenschreibers erforderlichen Komponenten, sowie alle sonstigen relevanten Unterlagen.

2. Ein Mitgliedstaat erteilt die Typgenehmigung für den Fahrtenschreiber, die Komponente oder Gruppe von Komponenten, die den administrativen und technischen Anforderungen nach Artikel 1 Absätze 2 bzw. 3 genügen. In diesem Fall stellt die Typgenehmigungsbehörde dem Antragsteller einen Typgenehmigungsbogen nach dem Muster in Anhang II dieser Verordnung aus.

3. Die Typgenehmigungsbehörde kann vom Hersteller oder dessen Beauftragtem zusätzliche Informationen verlangen.

4. Der Hersteller oder dessen Beauftragter stellt den Typgenehmigungsbehörden sowie den für die Ausstellung der Zertifikate nach Artikel 12 Absatz 3 der Verordnung (EU) Nr. 165/2014 zuständigen Stellen so viele Fahrtenschreiber oder Komponenten des Fahrtenschreibers zur Verfügung, wie für die ordnungsgemäße Durchführung des Typgenehmigungsverfahrens erforderlich sind.

5. Beantragt der Hersteller oder dessen Beauftragter eine Typgenehmigung für bestimmte Komponenten oder Gruppen von Komponenten eines Fahrtenschreibers, so stellt er den für die Typgenehmigung zuständigen Behörden die übrigen Komponenten, für die bereits eine Typgenehmigung vorliegt, sowie andere für den Bau des vollständigen Fahrtenschreibers erforderliche Teile zur Verfügung, damit diese Behörden die erforderlichen Prüfungen durchführen können.

Artikel 5

Änderungen der Typgenehmigungen

1. Der Hersteller oder dessen Beauftragter unterrichtet die Typgenehmigungsbehörden, die die ursprüngliche Typgenehmigung erteilt haben, unverzüglich über jegliche Änderung der Software oder Hardware des Fahrtenschreibers oder der für dessen Herstellung verwendeten Werkstoffe, die im Informationspaket verzeichnet sind, und beantragt die Änderung der Typgenehmigung.

2. Die Typgenehmigungsbehörden können je nach Art und Merkmalen der Änderungen eine bestehende Typgenehmigung ändern oder erweitern oder eine neue Typgenehmigung erteilen.

Eine „Änderung“ wird vorgenommen, wenn die Genehmigungsbehörde der Auffassung ist, dass es sich um geringfügige Änderungen an der Software oder Hardware des Fahrtenschreibers oder der für seine Herstellung verwendeten Werkstoffe handelt. In diesem Fall stellt die Typgenehmigungsbehörde die geänderten Unterlagen des Informationspakets aus, aus denen die Art der Änderungen und das Datum ihrer Genehmigung hervorgehen. Eine aktualisierte Fassung des Informationspakets in konsolidierter Form zusammen mit einer ausführlichen Beschreibung der vorgenommenen Änderungen reicht zur Erfüllung dieser Anforderung aus.

Eine „Erweiterung“ wird vorgenommen, wenn die Genehmigungsbehörde der Auffassung ist, dass es sich um wesentliche Änderungen an der Software oder Hardware des Fahrtenschreibers oder der für seine Herstellung verwendeten Werkstoffe handelt. In diesem Fall kann sie die Durchführung neuer Prüfungen verlangen und teilt dies dem Hersteller oder dessen Beauftragtem mit. Verlaufen diese Prüfungen zufriedenstellend, stellt die Typgenehmigungsbehörde einen geänderten Typgenehmigungsbogen aus, dessen Nummer auf die gewährte Erweiterung hinweist. Auf dem Typgenehmigungsbogen sind der Grund für die Erweiterung und das Ausstellungsdatum anzugeben.

3. Im Inhaltsverzeichnis zum Informationspaket ist das Datum der jüngsten Erweiterung oder Änderung der Typgenehmigung oder das Datum der jüngsten Konsolidierung der aktualisierten Fassung der Typgenehmigung anzugeben.

4. Eine neue Typgenehmigung ist erforderlich, wenn die beantragten Änderungen des zugelassenen Fahrtenschreibers oder seiner Komponenten zur Erteilung eines neuen Sicherheits- oder Interoperabilitätszertifikats führen würden.

Artikel 6

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab 2. März 2016.

Die Anhänge gelten jedoch ab 2. März 2019, ausgenommen Anlage 16, die ab 2. März 2016 gilt.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 18. März 2016

Für die Kommission
Der Präsident
Jean-Claude JUNCKER

ANHANG I C

Vorschriften für Bau, Prüfung, Einbau und Nachprüfung

EINLEITUNG 12

1 BEGRIFFSBESTIMMUNGEN 13

2 ALLGEMEINE FUNKTIONSMERKMALE DES KONTROLLGERÄTS 19

2.1 Allgemeine Merkmale 19

2.2 Funktionen 20

2.3 Betriebsarten 21

2.4 Sicherheit 22

3 BAUART- UND FUNKTIONSMERKMALE DES KONTROLLGERÄTS 22

3.1 Überwachung des Einsteckens und Entnehmens von Karten 22

3.2 Geschwindigkeits-, Positions- und Wegstreckenmessung 23

3.2.1 Messung der zurückgelegten Wegstrecke 23

3.2.2 Geschwindigkeitsmessung 23

3.2.3 Messung der Position 24

3.3 Zeitmessung 24

3.4 Überwachung der Fahrertätigkeiten 24

3.5 Überwachung des Status der Fahrzeugführung 25

3.6 Eingaben durch die Fahrer 25

3.6.1 Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages 25

3.6.2 Manuelle Eingabe der Fahrertätigkeiten und Zustimmung des Fahrers für die ITS-Schnittstelle 25

3.6.3 Eingabe spezifischer Bedingungen 27

3.7 Unternehmenssperren 27

3.8 Überwachung von Kontrollen 28

3.9 Feststellung von Ereignissen und/oder Störungen 28

3.9.1 Ereignis „Einstecken einer ungültigen Karte“ 28

3.9.2 Ereignis „Kartenkonflikt“ 28

3.9.3 Ereignis „Zeitüberlappung“ 28

3.9.4 Ereignis „Lenken ohne geeignete Karte“ 29

3.9.5 Ereignis „Einstecken der Karte während des Lenkens“ 29

3.9.6 Ereignis „Letzter Vorgang nicht korrekt abgeschlossen“ 29

3.9.7 Ereignis „Geschwindigkeitsüberschreitung“ 29

3.9.8 Ereignis „Unterbrechung der Stromversorgung“ 29

3.9.9 Ereignis „Kommunikationsfehler mit der Fernkommunikationsausrüstung“ 29

3.9.10 Ereignis „Fehlende Positionsdaten des GNSS-Empfängers“ 29

3.9.11	Ereignis „Kommunikationsfehler mit der externen GNSS-Ausrüstung“	30
3.9.12	Ereignis „Datenfehler Bewegungssensor“	30
3.9.13	Ereignis „Datenkonflikt Fahrzeugbewegung“	30
3.9.14	Ereignis „Versuch einer Sicherheitsverletzung“	30
3.9.15	Ereignis „Zeitkonflikt“	30
3.9.16	Störung „Kartenfehlfunktion“	30
3.9.17	Störung „Kontrollgerät“	30
3.10	Integrierte Tests und Selbsttests	31
3.11	Auslesen von Daten aus dem Massenspeicher	31
3.12	Aufzeichnung und Speicherung von Daten im Massenspeicher	31
3.12.1	Gerätekenndaten	32
3.12.1.1	Kenndaten der Fahrzeugeinheit	32
3.12.1.2	Kenndaten des Bewegungssensors	32
3.12.1.3	Kenndaten der globalen Satellitennavigationssysteme	33
3.12.2	Schlüssel und Zertifikate	33
3.12.3	Einsteck- und Entnahmedaten der Fahrer- oder der Werkstattkarte	33
3.12.4	Fahrertätigkeitsdaten	34
3.12.5	Orte und Positionen, an denen die tägliche Arbeitszeit beginnt, endet und/oder eine ununterbrochene Lenkzeit von 3 Stunden erreicht wird	34
3.12.6	Kilometerstandsdaten	35
3.12.7	Detaillierte Geschwindigkeitsdaten	35
3.12.8	Ereignisdaten	35
3.12.9	Störungsdaten	37
3.12.10	Kalibrierungsdaten	38
3.12.11	Zeiteinstellungsdaten	39
3.12.12	Kontrolltätigkeitsdaten	39
3.12.13	Unternehmenssperrdaten	39
3.12.14	Erfassen des Herunterladens	39
3.12.15	Daten zu spezifischen Bedingungen	40
3.12.16	Daten der Fahrtenschreiberkarte	40
3.13	Auslesen von Daten aus Fahrtenschreiberkarten	40
3.14	Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten	40
3.14.1	Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten der ersten Generation	40
3.14.2	Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten der zweiten Generation	41
3.15	Anzeige	41
3.15.1	Standardanzeige	42

3.15.2	Warnanzeige	43
3.15.3	Menübedienung	43
3.15.4	Sonstige Anzeigen	43
3.16	Drucken	43
3.17	Warnsignale	44
3.18	Herunterladen von Daten auf externe Datenträger	45
3.19	Fernkommunikation für die Durchführung gezielter Straßenkontrollen	45
3.20	Datenausgabe an externe Zusatzgeräte	46
3.21	Kalibrierung	47
3.22	Straßenseitige Kalibrierungsüberprüfung	47
3.23	Zeiteinstellung	48
3.24	Leistungsmerkmale	48
3.25	Werkstoffe	48
3.26	Markierungen	49
4	BAUART- UND FUNKTIONSMERKMALE DER FAHRTENSCHREIBERKARTEN	49
4.1	Sichtbare Daten	49
4.2	Sicherheit	52
4.3	Normen	53
4.4	Spezifikationen für Umgebung und Elektrizität	53
4.5	Datenspeicherung	53
4.5.1	Elementardateien für Kennung und Kartenverwaltung	54
4.5.2	IS-Kartenkennung	54
4.5.2.1	Chipkennung	54
4.5.2.2	DIR (nur in Fahrtenschreiberkarten der zweiten Generation enthalten)	54
4.5.2.3	ATR-Angaben (eingeschränkt, nur in Fahrtenschreiberkarten der zweiten Generation enthalten)	54
4.5.2.4	Erweiterte Längenangabe (eingeschränkt, nur in Fahrtenschreiberkarten der zweiten Generation enthalten)	55
4.5.3	Fahrerkarte	55
4.5.3.1	Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation)	55
4.5.3.1.1	Anwendungskennung	55
4.5.3.1.2	Schlüssel und Zertifikate	55
4.5.3.1.3	Kartenkennung	55
4.5.3.1.4	Karteninhaberkennung	55
4.5.3.1.5	Herunterladen von der Karte	55
4.5.3.1.6	Führerscheininformationen	55
4.5.3.1.7	Ereignisdaten	56

4.5.3.1.8 Störungsdaten 56

4.5.3.1.9 Fahrertätigkeitsdaten 57

4.5.3.1.10 Daten zu gefahrenen Fahrzeugen 57

4.5.3.1.11 Ort des Beginns und/oder des Endes des Arbeitstages 58

4.5.3.1.12 Kartenvorgangsdaten 58

4.5.3.1.13 Kontrolltätigkeitsdaten 58

4.5.3.1.14 Daten zu spezifischen Bedingungen 58

4.5.3.2 Fahrtenschreiberanwendung der zweiten Generation (für Fahrzeugeinheiten der ersten Generation nicht zugänglich) 59

4.5.3.2.1 Anwendungskennung 59

4.5.3.2.2 Schlüssel und Zertifikate 59

4.5.3.2.3 Kartenkennung 59

4.5.3.2.4 Karteninhaberkennung 59

4.5.3.2.5 Herunterladen von der Karte 59

4.5.3.2.6 Führerscheininformationen 59

4.5.3.2.7 Ereignisdaten 59

4.5.3.2.8 Störungsdaten 60

4.5.3.2.9 Fahrertätigkeitsdaten 61

4.5.3.2.10 Daten zu gefahrenen Fahrzeugen 61

4.5.3.2.11 Ort und Position des Beginns und/oder des Endes des Arbeitstages 62

4.5.3.2.12 Kartenvorgangsdaten 62

4.5.3.2.13 Kontrolltätigkeitsdaten 62

4.5.3.2.14 Daten zu spezifischen Bedingungen 63

4.5.3.2.15 Daten zu den genutzten Fahrzeugeinheiten 63

4.5.3.2.16 Ortsdaten zu drei Stunden ununterbrochener Lenkzeit 63

4.5.4 Werkstattkarte 63

4.5.4.1 Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation) 63

4.5.4.1.1 Anwendungskennung 63

4.5.4.1.2 Schlüssel und Zertifikate 63

4.5.4.1.3 Kartenkennung 64

4.5.4.1.4 Karteninhaberkennung 64

4.5.4.1.5 Herunterladen von der Karte 64

4.5.4.1.6 Kalibrierungs- und Zeiteinstellungsdaten 64

4.5.4.1.7 Ereignis- und Störungsdaten 65

4.5.4.1.8 Fahrertätigkeitsdaten 65

4.5.4.1.9 Daten zu gefahrenen Fahrzeugen 65

4.5.4.1.10 Daten zum Beginn und/oder Ende des Arbeitstages 65

4.5.4.1.11 Kartenvorgangsdaten 65

4.5.4.1.12 Kontrolltätigkeitsdaten 65

4.5.4.1.13 Daten zu spezifischen Bedingungen 65

4.5.4.2 Fahrtenschreiberanwendung der zweiten Generation (für Fahrzeugeinheiten der ersten Generation nicht zugänglich) 65

4.5.4.2.1 Anwendungskennung 65

4.5.4.2.2 Schlüssel und Zertifikate 66

4.5.4.2.3 Kartenkennung 66

4.5.4.2.4 Karteninhaberkennung 66

4.5.4.2.5 Herunterladen von der Karte 66

4.5.4.2.6 Kalibrierungs- und Zeiteinstellungsdaten 66

4.5.4.2.7 Ereignis- und Störungsdaten 67

4.5.4.2.8 Fahrertätigkeitsdaten 67

4.5.4.2.9 Daten zu gefahrenen Fahrzeugen 67

4.5.4.2.10 Daten zum Beginn und/oder Ende des Arbeitstages 67

4.5.4.2.11 Kartenvorgangsdaten 67

4.5.4.2.12 Kontrolltätigkeitsdaten 67

4.5.4.2.13 Daten zu den genutzten Fahrzeugeinheiten 67

4.5.4.2.14 Ortsdaten zu drei Stunden ununterbrochener Lenkzeit 68

4.5.4.2.15 Daten zu spezifischen Bedingungen 68

4.5.5 Kontrollkarte 68

4.5.5.1 Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation) 68

4.5.5.1.1 Anwendungskennung 68

4.5.5.1.2 Schlüssel und Zertifikate 68

4.5.5.1.3 Kartenkennung 68

4.5.5.1.4 Karteninhaberkennung 68

4.5.5.1.5 Kontrolltätigkeitsdaten 69

4.5.5.2 Fahrtenschreiberanwendung G2 (für Fahrzeugeinheiten der ersten Generation nicht zugänglich) 69

4.5.5.2.1 Anwendungskennung 69

4.5.5.2.2 Schlüssel und Zertifikate 69

4.5.5.2.3	Kartenkennung	69
4.5.5.2.4	Karteninhaberkennung	69
4.5.5.2.5	Kontrolltätigkeitsdaten	70
4.5.6	Unternehmenskarte	70
4.5.6.1	Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation)	70
4.5.6.1.1	Anwendungskennung	70
4.5.6.1.2	Schlüssel und Zertifikate	70
4.5.6.1.3	Kartenkennung	70
4.5.6.1.4	Karteninhaberkennung	70
4.5.6.1.5	Unternehmensaktivitätsdaten	70
4.5.6.2	Fahrtenschreiberanwendung G2 (für Fahrzeugeinheiten der ersten Generation nicht zugänglich)	71
4.5.6.2.1	Anwendungskennung	71
4.5.6.2.2	Schlüssel und Zertifikate	71
4.5.6.2.3	Kartenkennung	71
4.5.6.2.4	Karteninhaberkennung	71
4.5.6.2.5	Unternehmensaktivitätsdaten	71
5	EINBAU EINES KONTROLLGERÄTS	72
5.1	Einbau	72
5.2	Einbauplakette	73
5.3	Plombierung	74
6	EINBAUPRÜFUNGEN, NACHPRÜFUNGEN UND REPARATUREN	74
6.1	Zulassung der Einbaubetriebe, Werkstätten und Fahrzeughersteller	74
6.2	Prüfung neuer oder reparierter Geräte	75
6.3	Einbauprüfung	75
6.4	Regelmäßige Nachprüfungen	75
6.5	Messung der Anzeigefehler	76
6.6	Reparaturen	76
7	KARTENAUSGABE	76
8	TYPGENEHMIGUNG VON KONTROLLGERÄTEN UND FAHRTENSCHREIBERKARTEN	77
8.1	Allgemeines	77
8.2	Sicherheitszertifikat	78
8.3	Funktionszertifikat	78
8.4	Interoperabilitätszertifikat	78
8.5	Typgenehmigungsbogen	79
8.6	Ausnahmeverfahren: für die ersten Interoperabilitätszertifikate für Kontrollgeräte und Fahrtenschreiberkarten der zweiten Generation	80

EINLEITUNG

Das digitale Fahrtenschreibersystem der ersten Generation wird seit dem 1. Mai 2006 eingesetzt. Es kann im Inlandsverkehr bis zum Ablauf seiner Lebensdauer weiter verwendet werden. Im grenzüberschreitenden Verkehr müssen dagegen 15 Jahre nach dem Inkrafttreten dieser Verordnung der Kommission alle Fahrzeuge mit einem intelligenten Fahrtenschreiber der zweiten Generation ausgerüstet sein, der durch diese Verordnung eingeführt wird.

Dieser Anhang enthält die Anforderungen an die Kontrollgeräte und Fahrtenschreiberkarten der zweiten Generation.

Ab dem Einführungstermin werden Kontrollgeräte der zweiten Generation in erstmals zugelassene Fahrzeuge eingebaut und Fahrtenschreiberkarten der zweiten Generation ausgestellt.

— Im Hinblick auf eine reibungslose Einführung des Fahrtenschreibersystems der zweiten Generation müssen Fahrtenschreiberkarten der zweiten Generation so ausgelegt sein, dass sie auch in Fahrzeugeinheiten der ersten Generation verwendet werden können;

— müssen gültige Fahrtenschreiberkarten der ersten Generation nicht zum Einführungstermin ersetzt werden.

Dadurch können Fahrer ihre einzige Fahrerkarte behalten und in beiden Systemen verwenden.

Kontrollgeräte der zweiten Generation dürfen jedoch nur unter Verwendung von Werkstattkarten der zweiten Generation kalibriert werden.

Dieser Anhang enthält sämtliche Anforderungen in Bezug auf die Interoperabilität zwischen den Fahrtenschreibersystemen der ersten und der zweiten Generation.

Anlage 15 enthält weitere Einzelheiten zur Koexistenz der beiden Systeme.

Verzeichnis der Anlagen

Anlage 1: DATENGLOSSAR

Anlage 2: SPEZIFIKATION DER FAHRTENSCHREIBERKARTEN

Anlage 3: PIKTOGRAMME

Anlage 4: AUSDRUCKE

Anlage 5: ANZEIGE

Anlage 6: STECKANSCHLUSS AN DER VORDERSEITE FÜR KALIBRIERUNG UND HERUNTERLADEN

Anlage 7: PROTOKOLLE ZUM HERUNTERLADEN DER DATEN

Anlage 8: KALIBRIERUNGSPROTOKOLL

Anlage 9: TYPGENEHMIGUNG MINDESTANFORDERUNG AN DIE DURCHZUFÜHRENDEN PRÜFUNGEN

Anlage 10: SICHERHEITSANFORDERUNGEN

Anlage 11: GEMEINSAME SICHERHEITSMECHANISMEN

Anlage 12: POSITIONSBESTIMMUNG MITHILFE EINES GLOBALEN SATELLITENNAVIGATIONSSYSTEMS (GNSS)

Anlage 13: ITS-SCHNITTSTELLE

Anlage 14: FERNKOMMUNIKATIONSFUNKTION

Anlage 15: MIGRATION: VERWALTUNG GLEICHZEITIG VORHANDENER AUSRÜSTUNGSGENERATIONEN

Anlage 16: ADAPTER FÜR FAHRZEUGE DER KLASSEN M1 UND N1

1 BEGRIFFSBESTIMMUNGEN

Im Sinne dieses Anhangs bedeutet:

a) „Aktivierung“

Phase, in der der Fahrtenschreiber mithilfe einer Werkstattkarte seine volle Einsatzbereitschaft erlangt und alle Funktionen, einschließlich Sicherheitsfunktionen, erfüllt;

b) „Authentisierung“

Funktion zur Feststellung und Überprüfung der Identität einer Person;

c) „Authentizität“

Eigenschaft einer Information, die von einem Beteiligten stammt, dessen Identität überprüft werden kann;

d) „Integrierter Test“

Tests auf Anforderung, ausgelöst durch den Bediener oder durch ein externes Gerät;

e) „Kalendertag“

einen von 0.00 Uhr bis 24.00 Uhr dauernden Tag. Alle Kalendertage beziehen sich auf UTC-Zeitangaben (koordinierte Weltzeit);

f) „Kalibrierung“ eines intelligenten Fahrtenschreibers

die Aktualisierung oder Bestätigung von Fahrzeugparametern, die im Massenspeicher zu speichern sind. Zu den Fahrzeugparametern gehören die Fahrzeugkennung (Fahrzeugidentifizierungsnummer (VIN), amtliches Kennzeichen (VRN) und zulassender Mitgliedstaat) sowie Fahrzeugmerkmale (Wegdrehzahl, Kontrollgerätkonstante, tatsächlicher Reifenumfang, Reifengröße, Einstellung des Geschwindigkeitsbegrenzers (wenn zutreffend), aktuelle UTC-Zeit, aktueller Kilometerstand); während der Kalibrierung eines Kontrollgeräts sind auch Art und Kennung aller vorhandenen, die Typgenehmigung betreffenden Plombierungen im Massenspeicher zu speichern;

eine Aktualisierung oder Bestätigung lediglich der UTC-Zeit gilt als Zeiteinstellung und nicht als Kalibrierung, sofern sie nicht im Widerspruch zu Randnummer 409 steht;

Zum Kalibrieren eines Kontrollgeräts muss eine Werkstattkarte verwendet werden.

g) „Kartennummer“

eine aus 16 alphanumerischen Zeichen bestehende Nummer zur eindeutigen Identifizierung einer Fahrtenschreiberkarte innerhalb eines Mitgliedstaates. Die Kartennummer enthält (gegebenenfalls) einen fortlaufenden Kartenindex, einen Kartenersatzindex und einen Kartenerneuerungsindex;

Die eindeutige Zuordnung einer Karte erfolgt somit anhand des Codes des ausstellenden Mitgliedstaates und der Kartennummer;

h) „Fortlaufender Kartenindex“

das 14. alphanumerische Zeichen einer Kartennummer zur Unterscheidung der verschiedenen Karten, die für ein(e) zum Empfang mehrerer Fahrtenschreiberkarten berechtigte(s) Unternehmen, Werkstatt oder Kontrollbehörde ausgestellt wurden. Die eindeutige Identifizierung des Unternehmens, der Werkstatt bzw. der Kontrollbehörde erfolgt durch die 13 ersten Zeichen der Kartennummer;

i) „Kartenerneuerungsindex“

das 16. alphanumerische Zeichen einer Kartennummer, das bei jeder Erneuerung der Fahrtenschreiberkarte um eine Stelle erhöht wird;

j) „Kartenersatzindex“

das 15. alphanumerische Zeichen einer Kartennummer, das sich um eine Stelle erhöht, wenn die Fahrtenschreiberkarte ersetzt wird;

k) „Wegdrehzahl des Kraftfahrzeugs“

die Kenngröße, die den Zahlenwert des Ausgangssignals angibt, das am Anschlussstutzen für das Kontrollgerät am Kraftfahrzeug (Getriebestutzen bzw. Radachse) bei einer unter normalen Prüfbedingungen zurückgelegten Wegstrecke von einem Kilometer gemäß Randnummer 414 entsteht. Die Wegdrehzahl wird in Impulsen je Kilometer (w = … Imp/km) ausgedrückt;

l) „Unternehmenskarte“

eine Fahrtenschreiberkarte, die die Behörden eines Mitgliedstaats einem Verkehrsunternehmen ausstellen, das mit einem Fahrtenschreiber ausgerüstete Fahrzeuge betreiben muss, und die das Verkehrsunternehmen ausweist und das Anzeigen, Herunterladen und Ausdrucken der Daten ermöglicht, die in dem von diesem Verkehrsunternehmen gesperrten Fahrtenschreiber gespeichert sind;

m) „Konstante des Kontrollgerätes“

die Kenngröße, die den Wert des Eingangssignals angibt, der für das Anzeigen und Aufzeichnen einer zurückgelegten Wegstrecke von 1 km erforderlich ist; diese Konstante wird in Impulsen je Kilometer (k = … Imp/km) ausgedrückt;

n) „ununterbrochene Lenkzeit“, im Kontrollgerät errechnet als ([1]):

die jeweiligen akkumulierten Lenkzeiten eines bestimmten Fahrers seit Ende seiner letzten BEREITSCHAFT oder UNTERBRECHUNG/RUHE oder UNBEKANNTEN Zeit ([2]) von 45 oder mehr Minuten (dieser Zeitraum kann gemäß der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates ([3]) aufgeteilt worden sein). Bei den Berechnungen werden nach Bedarf die auf der Fahrerkarte gespeicherten bisherigen Tätigkeiten berücksichtigt. Hat der Fahrer seine Karte nicht eingesteckt, beruhen die Berechnungen auf den Massenspeicheraufzeichnungen zu dem Zeitraum, in dem keine Karte eingesteckt war, und zum entsprechenden Steckplatz;

o) „Kontrollkarte“

eine Fahrtenschreiberkarte, die die Behörden eines Mitgliedstaats einer zuständigen nationalen Kontrollbehörde ausstellen, die die Kontrollbehörde, und fakultativ den Kontrolleur, ausweist und das Auslesen, Ausdrucken und/oder Herunterladen der im Massenspeicher, auf Fahrerkarten, und fakultativ auf Werkstattkarten gespeicherten Daten, ermöglicht;

sie ermöglicht außerdem den Zugriff auf die Funktion straßenseitige Kalibrierungsüberprüfung und die Daten im Fernabfragegerät.

p) „kumulative Unterbrechungszeit“, im Kontrollgerät errechnet als ([1]):

die kumulative Lenkzeitunterbrechung eines bestimmten Fahrers wird errechnet als die jeweilige akkumulierte Zeit aus BEREITSCHAFT, UNTERBRECHUNG/RUHE oder UNBEKANNT ([2]) von 15 oder mehr Minuten seit dem Ende der letzten BEREITSCHAFT oder UNTERBRECHUNG/RUHE oder UNBEKANNTEN Zeit ([2]) von 45 oder mehr Minuten (dieser Zeitraum kann gemäß der Verordnung (EG) Nr. 561/2006 aufgeteilt worden sein).

Bei den Berechnungen werden nach Bedarf die auf der Fahrerkarte gespeicherten bisherigen Tätigkeiten berücksichtigt. Unbekannte Zeiträume mit negativer Dauer (Beginn des unbekannten Zeitraums > Ende des unbekannten Zeitraums) aufgrund von zeitlichen Überlappungen verschiedener Kontrollgeräte werden bei der Berechnung nicht berücksichtigt.

Hat der Fahrer seine Karte nicht eingesteckt, beruhen die Berechnungen auf den Massenspeicheraufzeichnungen für den Zeitraum, in dem keine Karte eingesteckt war, und den entsprechenden Steckplatz;

([1]) Diese Art der Berechnung der ununterbrochenen Lenkzeit und der kumulativen Unterbrechungszeit dient dem Kontrollgerät zur Errechnung der Warnung für ununterbrochene Lenkzeit. Sie stellt keinen Vorgriff auf die rechtliche Auslegung dieser Zeiten dar. Alternative Arten der Berechnung der ununterbrochenen Lenkzeit und der kumulativen Unterbrechungszeit können als Ersatz für diese Begriffsbestimmungen verwendet werden, falls diese durch Aktualisierungen anderer einschlägiger Rechtsvorschriften hinfällig werden.

([2]) UNBEKANNT sind Zeiträume, in denen die Fahrerkarte nicht in ein Kontrollgerät eingesteckt war und für die kein manueller Eintrag über die Fahrertätigkeit vorgenommen wurde.

([3]) Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates vom 15. März 2006 zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr und zur Änderung der Verordnungen (EWG) Nr. 3821/85 und (EG) Nr. 2135/98 des Rates sowie zur Aufhebung der Verordnung (EWG) Nr. 3820/85 des Rates (ABl. L 102 vom 11.4.2006, S. 1).

q) „Massenspeicher“

ein in das Kontrollgerät eingebautes Speichermedium;

r) „digitale Signatur“

die an einen Datenblock angehängte Datenmenge oder die verschlüsselte Umwandlung eines Datenblocks, die es dem Empfänger des Datenblocks ermöglicht, sich der Authentizität und Integrität des Datenblocks zu vergewissern;

s) „Herunterladen“

das Kopieren eines Teils oder aller im Massenspeicher der Fahrzeugeinheit oder der im Speicher einer Fahrtenschreiberkarte enthaltenen Datendateien zusammen mit der digitalen Signatur, sofern gespeicherte Daten dabei weder verändert noch gelöscht werden;

die Hersteller von intelligenten Fahrtenschreiber-Fahrzeugeinheiten und die Hersteller der zum Herunterladen von Datendateien konzipierten und bestimmten Geräte treffen alle zumutbaren Maßnahmen, um zu gewährleisten, dass das Herunterladen dieser Daten unter möglichst geringen Zeitverlusten durch die Verkehrsunternehmen und Fahrer erfolgen kann.

Die Datei mit detaillierten Geschwindigkeitsdaten muss möglicherweise zur Feststellung der Einhaltung der Verordnung (EG) Nr. 561/2006 nicht heruntergeladen werden, kann aber für andere Zwecke, z. B. zur Ermittlung eines Unfallhergangs, verwendet werden.

t) „Fahrerkarte“

eine Fahrtenschreiberkarte, die einem bestimmten Fahrer von den Behörden eines Mitgliedstaats ausgestellt wird, den Fahrer ausweist und die Speicherung von Tätigkeitsdaten des Fahrers ermöglicht;

u) „tatsächlicher Umfang der Fahrzeugreifen“

der Mittelwert der von jedem Antriebsrad bei einer vollen Umdrehung zurückgelegten Wegstrecke. Die Messung dieser Wegstrecken muss unter normalen Prüfbedingungen gemäß Randnummer 414 erfolgen und wird in folgender Form ausgedrückt: „l = … mm“. Fahrzeughersteller können die Messung dieser Wegstrecken durch eine theoretische Berechnung ersetzen, bei der die Achslastverteilung des fahrbereiten, unbeladenen Fahrzeugs berücksichtigt wird [1]. Die Verfahren für diese theoretische Berechnung bedürfen der Genehmigung durch eine zuständige Behörde des Mitgliedstaats und können nur vor der Aktivierung des Fahrtenschreibers durchgeführt werden;

v) „Ereignis“

eine vom intelligenten Fahrtenschreiber festgestellte Betriebsabweichung, die möglicherweise auf einen Betrugsversuch zurückgeht;

w) „externe GNSS-Ausrüstung“

eine Ausrüstung, die den GNSS-Empfänger (wenn die Fahrzeugeinheit (VU) nicht aus einem Einzelgerät besteht) sowie andere Komponenten enthält, die erforderlich sind für den Schutz der Kommunikation der Positionsdaten an die übrige Fahrzeugeinheit;

x) „Störung“

eine vom intelligenten Fahrtenschreiber festgestellte Betriebsabweichung, die möglicherweise auf eine technische Fehlfunktion oder ein technisches Versagen zurückgeht;

y) „GNSS-Empfänger“

ein elektronisches Gerät, das die Signale von einem oder mehreren globalen Satellitennavigationssystem(en) (GNSS) empfängt und digital verarbeitet, um Positions-, Geschwindigkeits- und Zeitangaben liefern zu können;

z) „Einbau“

die Montage eines Fahrtenschreibers in einem Fahrzeug;

---

[1] Verordnung (EU) Nr. 1230/2012 der Kommission vom 12. Dezember 2012 zur Durchführung der Verordnung (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern bezüglich ihrer Massen und Abmessungen und zur Änderung der Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates (ABl. L 353 vom 21.12.2012, S. 31), in der zuletzt geänderten Fassung.

aa) „Interoperabilität“

die Fähigkeit von Systemen, Daten auszutauschen und Informationen weiterzugeben, sowie die ihnen zugrundeliegenden Geschäftsabläufe;

bb) „Schnittstelle“

„Schnittstelle“ ist eine Einrichtung zwischen Systemen, die der Verbindung und der Kommunikation zwischen den Systemen dient;

cc) „Position“

geografische Koordinaten des Fahrzeugs zu einem bestimmten Zeitpunkt;

dd) „Bewegungssensor“

den Bestandteil des Fahrtenschreibers, der ein Signal bereitstellt, das die Fahrzeuggeschwindigkeit und/oder die zurückgelegte Wegstrecke darstellt;

ee) „ungültige Karte“

eine Karte, die als fehlerhaft festgestellt wurde oder deren Erstauthentisierung fehlgeschlagen oder deren Gültigkeitsbeginn noch nicht erreicht oder deren Ablaufdatum überschritten ist;

ff) „offene Norm“

eine Norm, die in einem Normenspezifikationsdokument aufgeführt ist, das kostenlos oder gegen eine Schutzgebühr zur Verfügung steht und gebührenfrei oder gegen eine Schutzgebühr kopiert, verteilt oder benutzt werden darf;

gg) „Kontrollgerät nicht erforderlich“

wenn die Anwendung des Kontrollgeräts gemäß den Bestimmungen der Verordnung (EG) Nr. 561/2006 nicht erforderlich ist;

hh) „Geschwindigkeitsüberschreitung“

die Überschreitung der zulässigen Fahrzeuggeschwindigkeit, definiert als Zeitraum von mehr als 60 Sekunden, in dem die gemessene Fahrzeuggeschwindigkeit den Höchstwert für die Einstellung des Geschwindigkeitsbegrenzers gemäß Richtlinie 92/6/EWG des Rates vom 10. Februar 1992 über Einbau und Benutzung von Geschwindigkeitsbegrenzern für bestimmte Kraftfahrzeugklassen in der Gemeinschaft [1] in der zuletzt geänderten Fassung überschreitet;

ii) „regelmäßige Nachprüfung“

einen Komplex von Arbeitsgängen zur Überprüfung der ordnungsgemäßen Funktion des Fahrtenschreibers und der Übereinstimmung seiner Einstellungen mit den Fahrzeugparametern sowie zur Kontrolle, dass keine Manipulationsvorrichtungen an den Fahrtenschreiber angeschlossen sind;

jj) „Drucker“

eine Komponente des Kontrollgeräts, das Ausdrucke gespeicherter Daten liefert;

kk) „Fernkommunikation zur Früherkennung“

die Kommunikation zwischen der Ausrüstung zur Früherkennung per Fernkommunikation und dem Fernabfragegerät im Rahmen gezielter Straßenkontrollen zur Fernerkennung möglicher Manipulationen oder möglichen Missbrauchs des Kontrollgeräts;

ll) „Ausrüstung zur Fernkommunikation“

das Gerät der Fahrzeugeinheit, das zur Durchführung gezielter Straßenkontrollen eingesetzt wird;

[1] Richtlinie 92/6/EWG des Rates vom 10. Februar 1992 über Einbau und Benutzung von Geschwindigkeitsbegrenzern für bestimmte Kraftfahrzeugklassen in der Gemeinschaft (ABl. L 57 vom 2.3.1992, S. 27).

mm) „Fernabfragegerät“

das von den Kontrolleuren bei gezielten Straßenkontrollen verwendete System;

nn) „Erneuerung“

die Ausgabe einer neuen Fahrtenschreiberkarte bei Ablauf der Gültigkeit einer vorhandenen Karte oder wenn die vorhandene Karte defekt ist und der ausstellenden Behörde zurückgegeben wurde. Bei einer Erneuerung besteht stets die Gewissheit, dass nicht zwei gültige Karten gleichzeitig vorhanden sind;

oo) „Reparatur“

die Reparatur eines Bewegungssensors oder einer Fahrzeugeinheit oder eines Kabels, wozu die Trennung von der Stromversorgung oder die Trennung von anderen Komponenten des Fahrtenschreibers oder die Öffnung des Bewegungssensors oder der Fahrzeugeinheit erforderlich ist;

pp) „Kartenersatz“

die Ausgabe einer Fahrtenschreiberkarte als Ersatz für eine vorhandene Karte, die als verloren, gestohlen oder defekt gemeldet und der ausstellenden Behörde nicht zurückgegeben wurde. Ein Ersatz birgt immer das Risiko, dass möglicherweise zwei gültige Karten gleichzeitig vorhanden sind;

qq) „Sicherheitszertifizierung“

der Prozess der Zertifizierung durch eine Common-Criteria-Zertifizierungsstelle, dass das untersuchte Kontrollgerät (oder die Komponente) oder die untersuchte Fahrtenschreiberkarte die in den jeweiligen Schutzprofilen festgelegten Sicherheitsanforderungen erfüllt;

rr) „Selbsttest“

zyklisch und automatisch vom Kontrollgerät durchgeführte Tests zur Feststellung von Störungen;

ss) „Zeitmessung“

die ununterbrochene digitale Aufzeichnung der koordinierten Weltzeit aus Kalenderdatum und Uhrzeit (UTC);

tt) „Zeiteinstellung“

ist die in regelmäßigen Abständen vorgenommene automatische Einstellung der aktuellen Zeit mit einer Höchsttoleranz von einer Minute oder die während der Kalibrierung vorgenommene Einstellung;

uu) „Reifengröße“

die Bezeichnung der Abmessungen der Reifen (äußere Antriebsräder) gemäß Richtlinie 92/23/EWG des Rates ([1]) in der zuletzt geänderten Fassung;

vv) „Fahrzeugkennung“

Nummern, mit deren Hilfe das Fahrzeug identifiziert werden kann: amtliches Kennzeichen (VRN) mit Angabe des zulassenden Mitgliedstaats und der Fahrzeug-Identifizierungsnummer (VIN) ([2]);

ww) „Woche“ (zu Berechnungszwecken im Kontrollgerät)

den Zeitraum zwischen Montag 0.00 Uhr UTC und Sonntag 24.00 Uhr UTC;

([1]) Richtlinie 92/23/EWG des Rates vom 31. März 1992 über Reifen von Kraftfahrzeugen und Kraftfahrzeuganhängern und über ihre Montage (ABl. L 129 vom 14.5.1992, S. 95).

([2]) Richtlinie 76/114/EWG des Rates vom 18. Dezember 1975 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Schilder, vorgeschriebene Angaben, deren Lage und Anbringungsart an Kraftfahrzeugen und Kraftfahrzeuganhängern (ABl. L 24 vom 30.1.1976, S. 1).

xx) „Werkstattkarte“

eine Fahrtenschreiberkarte, die die Behörden eines Mitgliedstaats benannten Mitarbeitern eines von diesem Mitgliedstaat zugelassenen Fahrtenschreiberherstellers, Einbaubetriebs, Fahrzeugherstellers oder einer von ihm zugelassenen Werkstatt ausstellen, den Karteninhaber ausweist und das Prüfen, Kalibrieren und Aktivieren von Fahrtenschreibern und/oder das Herunterladen der Daten von diesen ermöglicht;

yy) „Adapter“

ein Gerät, das ein anderes als das für die unabhängige Bewegungserkennung verwendete, permanent die Fahrzeuggeschwindigkeit und/oder die zurückgelegte Wegstrecke darstellendes Signal bereitstellt und

— ausschließlich in erstmals seit 1. Mai 2006 in Betrieb genommenen Fahrzeuge der Klassen M1 und N1 (gemäß der Begriffsbestimmung in Anhang II der Richtlinie 2007/46/EG des Europäischen Parlaments des Rates ([1]) in der zuletzt geänderten Fassung) eingebaut ist und eingesetzt wird;

— an einem Ort eingebaut ist, an dem der Einbau eines bestehenden Bewegungssensors anderer Art, der ansonsten den Bestimmungen dieses Anhangs und dessen Anlagen 1 bis 15 entspricht, mechanisch unmöglich ist;

— zwischen der Fahrzeugeinheit und dem Ort der Erzeugung von Geschwindigkeits-/Entfernungsimpulsen durch integrierte Sensoren oder alternative Schnittstellen eingebaut ist,

— aus Sicht einer Fahrzeugeinheit verhält sich der Adapter ebenso, als wäre ein den Bestimmungen dieses Anhangs und dessen Anlagen 1 bis 16 entsprechender Bewegungssensor an die Fahrzeugeinheit angeschlossen;

Der Einsatz eines solchen Adapters in den oben beschriebenen Fahrzeugen muss den Einbau und die ordnungsgemäße Nutzung einer Fahrzeugeinheit im Einklang mit allen Vorschriften dieses Anhangs ermöglichen.

Der intelligente Fahrtenschreiber für diese Fahrzeuge besteht aus Verbindungskabeln, einem Adapter und einer Fahrzeugeinheit;

zz) „Datenintegrität“

die Richtigkeit und Konsistenz gespeicherter Daten, die dadurch angezeigt wird, dass zwischen zwei Aktualisierungen eines Datensatzes die Daten nicht verändert werden. Integrität bedeutet, dass es sich bei den Daten um eine genaue Kopie der Originalfassung handelt, d. h., dass sie während des Schreibens auf bzw. beim Auslesen eine(r) Fahrtenschreiberkarte oder eine(r) spezielle(n) Ausrüstung oder bei der Übermittlung durch einen Kommunikationskanal nicht verfälscht wurde;

aaa) „Datenschutz“

die gesamten technischen Maßnahmen zur Gewährleistung der ordnungsgemäßen Umsetzung der Grundsätze, die in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([2]) sowie der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([3]) niedergelegt wurden;

bbb) „intelligentes Fahrtenschreibersystem“

das Kontrollgerät, die Fahrtenschreiberkarten und die gesamte direkt oder indirekt interagierende Ausrüstung während Bau, Einbau, Benutzung, Prüfung und Kontrolle, u. a. Karten, das Fernabfragegerät und sonstige Ausrüstungen für das Herunterladen von Daten, Datenanalysen, die Kalibrierung, die Erstellung, Verwaltung oder Einführung von Sicherheitselementen;

ccc) „Einführungstermin“

36 Monate nach Inkrafttreten der Einzelvorschriften gemäß Artikel 11 der Verordnung (EU) Nr. 165/2014 Europäischen Parlaments und des Rates ([4]).

([1]) Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates vom 5. September 2007 zur Schaffung eines Rahmens für die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge (Rahmenrichtlinie) (ABl. L 263 vom 9.10.2007, S. 1).

([2]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

([3]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

([4]) Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr, zur Aufhebung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr und zur Änderung der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr (ABl. L 60 vom 28.2.2014, S. 1).

Dies ist das Datum, ab dem erstmals zugelassene Fahrzeuge

— *mit einem Fahrtenschreiber ausgerüstet sein müssen, der an einen Positionsbestimmungsdienst auf der Basis eines Satellitennavigationssystems angebunden ist;*

— *fähig sein müssen, den zuständigen Kontrollbehörden Daten für gezielte Straßenkontrollen zu übermitteln, während sich das Fahrzeug in Bewegung befindet;*

— *und mit genormten Schnittstellen ausgerüstet werden können, die in der Betriebsart Betrieb die Nutzung der vom Fahrtenschreiber aufgezeichneten oder erzeugten Daten durch externe Geräte ermöglichen;*

ddd) „Schutzprofil"

ein im Rahmen des Common-Criteria-Zertifizierungsverfahrens verwendetes Dokument mit implementationsneutralen Spezifikationen von Sicherheitsanforderungen für die Informationssicherung;

eee) „GNSS-Genauigkeit"

im Rahmen der Aufzeichnung der Position über das globale Satellitennavigationssystem (GNSS) mit Fahrtenschreibern den Wert der Horizontalgenauigkeit (Horizontal Dilution of Precision, HDOP), berechnet als das Minimum der von den verfügbaren GNSS-Systemen erfassten HDOP-Werte.

2 ALLGEMEINE FUNKTIONSMERKMALE DES KONTROLLGERÄTS

2.1 **Allgemeine Merkmale**

Aufgabe des Kontrollgeräts ist das Aufzeichnen, Speichern, Anzeigen, Ausdrucken und Ausgeben von tätigkeitsbezogenen Daten des Fahrers.

Ein Fahrzeug, das mit einem den Bestimmungen dieses Anhangs genügenden Kontrollgerät ausgestattet ist, muss über eine Geschwindigkeitsanzeige und einen Kilometerzähler verfügen. Diese Funktionen können in das Kontrollgerät integriert sein.

01) Das Kontrollgerät besteht aus Verbindungskabeln, einem Bewegungssensor und einer Fahrzeugeinheit.

02) Die Schnittstelle zwischen Bewegungssensoren und Fahrzeugeinheiten muss den Vorschriften gemäß Anlage 11 entsprechen.

03) Die Fahrzeugeinheit muss an ein oder mehrere globale(s) Satellitennavigationssystem(e) gemäß Anlage 12 angebunden sein.

04) Die Fahrzeugeinheit muss mit den Fernabfragegeräten gemäß Anlage 14 kommunizieren.

05) Die Fahrzeugeinheit kann eine in Anlage 13 spezifizierte ITS-Schnittstelle umfassen.

Das Kontrollgerät kann durch zusätzliche Schnittstellen und/oder durch die optionale ITS-Schnittstelle auch mit anderen Ausrüstungen verbunden werden.

06) Werden Zusatzeinrichtungen in das Kontrollgerät eingebaut oder daran angeschlossen, dürfen sie unabhängig davon, ob sie zugelassen sind, die einwandfreie Arbeitsweise des Kontrollgeräts und die Bestimmungen dieser Verordnung weder faktisch noch potenziell beeinträchtigen.

Benutzer des Kontrollgeräts weisen sich gegenüber dem Gerät mit Fahrtenschreiberkarten aus.

07) Je nach Art und/oder Identität des Benutzers bietet das Kontrollgerät einen selektiven Zugang zu Daten und Funktionen.

Das Kontrollgerät zeichnet Daten auf und speichert sie in seinem Massenspeicher, der Fernkommunikationsausrüstung und auf Fahrtenschreiberkarten.

Dies geschieht in Übereinstimmung mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1], der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [2] und im Einklang mit Artikel 7 der Verordnung (EU) Nr. 165/2014.

2.2 **Funktionen**

08) Das Kontrollgerät muss folgende Funktionen gewährleisten:

- Überwachung des Einsteckens und Entnehmens von Karten,
- Geschwindigkeits-, Wegstrecken- und Positionsmessung,
- Zeitmessung,
- Überwachung der Fahrertätigkeiten,
- Überwachung des Status der Fahrzeugführung,
- manuelle Eingabe durch die Fahrer:
  - Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages,
  - manuelle Eingabe der Fahrertätigkeiten,
  - Eingabe spezifischer Bedingungen,
- Unternehmenssperren,
- Überwachung von Kontrollen,
- Feststellung von Ereignissen und/oder Störungen,
- integrierte Tests und Selbsttests,
- Auslesen von Daten aus dem Massenspeicher,
- Aufzeichnung und Speicherung von Daten im Massenspeicher,
- Auslesen von Daten aus Fahrtenschreiberkarten,
- Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten,
- Datenanzeige,
- Ausdrucken,
- Warnsignale,
- Herunterladen von Daten auf externe Datenträger,
- Fernkommunikation für die Durchführung gezielter Straßenkontrollen,
- Datenausgabe an zusätzliche Ausrüstungen,
- Kalibrierung,
- straßenseitige Kalibrierungsüberprüfung,
- Zeiteinstellung.

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 201 vom 31.7.2002, S. 37.

2.3 **Betriebsarten**

09) Das Kontrollgerät verfügt über vier Betriebsarten:

— Betrieb,

— Kontrolle,

— Kalibrierung,

— Unternehmen.

10) Je nachdem, welche gültige Fahrtenschreiberkarte in die Kartenschnittstellen eingesteckt ist, schaltet das Kontrollgerät auf folgende Betriebsart. Für die Wahl der Betriebsart ist es unerheblich, zu welcher Generation die Fahrtenschreiberkarte gehört, sofern die eingesteckte Karte gültig ist. Eine Werkstattkarte der ersten Generation gilt immer als ungültig, wenn sie in eine Fahrzeugeinheit (VU) der zweiten Generation eingesteckt wird.

Betriebsart		Steckplatz des Fahrers				
		Keine Karte	Fahrerkarte	Kontrollkarte	Werkstattkarte	Unternehmens-karte
Steckplatz des Beifahrers	Keine Karte	Betrieb	Betrieb	Kontrolle	Kalibrierung	Unternehmen
	Fahrerkarte	Betrieb	Betrieb	Kontrolle	Kalibrierung	Unternehmen
	Kontrollkarte	Kontrolle	Kontrolle	Kontrolle (*)	Betrieb	Betrieb
	Werkstattkarte	Kalibrierung	Kalibrierung	Betrieb	Kalibrierung (*)	Betrieb
	Unternehmens-karte	Unternehmen	Unternehmen	Betrieb	Betrieb	Unternehmen (*)

(*) In diesen Zuständen verwendet das Kontrollgerät nur die im Steckplatz des Fahrers eingesteckte Fahrtenschreiberkarte.

11) Ungültige Karten, die eingesteckt werden, sind vom Kontrollgerät zu ignorieren, doch müssen das Anzeigen, Ausdrucken oder Herunterladen von auf abgelaufenen Karten gespeicherten Daten möglich sein.

12) Alle in 2.2 aufgeführten Funktionen sind in jeder Betriebsart zu gewährleisten, wobei folgende Ausnahmen gelten:

— die Funktion Kalibrierung ist nur in der Betriebsart Kalibrierung verfügbar,

— die Funktion straßenseitige Kalibrierungsüberprüfung ist nur in der Betriebsart Kontrolle verfügbar,

— die Funktion Unternehmenssperre ist nur in der Betriebsart Unternehmen verfügbar,

— die Funktion Überwachung von Kontrollen ist nur in der Betriebsart Kontrolle verfügbar,

— Die Funktion Herunterladen von Daten ist in der Betriebsart Betrieb nicht verfügbar (außer gemäß Randnummer 193), abgesehen vom Herunterladen einer Fahrerkarte, wenn keine andere Karte in die Fahrzeugeinheit eingesteckt ist.

13) Das Kontrollgerät kann jegliche Daten an Anzeige-, Drucker- oder externe Schnittstellen ausgeben, wobei folgende Ausnahmen gelten:

— in der Betriebsart Betrieb werden persönliche Daten (Vor- und Zuname), die nicht zur einer eingesteckten Fahrtenschreiberkarte gehören, ausgeblendet, und eine Kartennummer, die nicht zu einer eingesteckten Fahrtenschreiberkarte gehört, wird teilweise ausgeblendet (von links nach rechts jedes zweite Zeichen),

— in der Betriebsart Unternehmen (Randnummern 102, 105 und 108) lassen sich Fahrerdaten nur für Zeiträume ausgeben, für die keine Sperrung besteht oder kein anderes Unternehmen (ausgewiesen durch die ersten 13 Stellen der Unternehmenskartennummer) eine Sperrung innehat.

— ist keine Karte in das Kontrollgerät eingesteckt, lassen sich Fahrerdaten nur für den aktuellen und die 8 vorhergehenden Kalendertage ausgeben,

— personenbezogene Daten aus der Fahrzeugeinheit dürfen nur dann durch die ITS-Schnittstelle der VU ausgegeben werden, wenn die Zustimmung des Fahrers, auf den sich die Daten beziehen, überprüft wurde;

— die Fahrzeugeinheiten haben eine normale Gültigkeitsdauer von 15 Jahren ab dem Ausstellungsdatum der Zertifikate für die Fahrzeugeinheit; die Fahrzeugeinheiten können jedoch für weitere 3 Monate nur für das Herunterladen von Daten verwendet werden.

2.4 **Sicherheit**

Durch die Systemsicherheit soll folgender Schutz gewährleistet sein: Schutz des Massenspeichers, so dass ein unbefugter Zugriff auf die Daten und deren Manipulation ausgeschlossen ist und alle entsprechenden Versuche entdeckt werden, Schutz der Integrität und Authentizität der zwischen Bewegungssensor und Fahrzeugeinheit ausgetauschten Daten, Schutz der Integrität und Authentizität der zwischen dem Kontrollgerät und den Fahrtenschreiberkarten ausgetauschten Daten, Schutz der Integrität und Authentizität der zwischen dem Kontrollgerät und der externen GNSS-Ausrüstung ausgetauschten Daten, Schutz der Vertraulichkeit, Integrität und Authentizität der zu Kontrollzwecken durch Früherkennung per Fernkommunikation ausgetauschten Daten sowie Überprüfung der Integrität und Authentizität heruntergeladener Daten.

14) Zur Gewährleistung der Systemsicherheit müssen folgende Komponenten die in ihren Schutzprofilen spezifizierten Sicherheitsanforderungen gemäß Anlage 10 erfüllen:

— Fahrzeugeinheit,

— Fahrtenschreiberkarte,

— Bewegungssensor,

— externe GNSS-Ausrüstung (dieses Profil ist nur für die externe GNSS-Variante erforderlich und anwendbar).

3 BAUART- UND FUNKTIONSMERKMALE DES KONTROLLGERÄTS

3.1 **Überwachung des Einsteckens und Entnehmens von Karten**

15) Das Kontrollgerät überwacht die Kartenschnittstellen und erkennt das Einstecken und Entnehmen einer Karte.

16) Beim Einstecken einer Karte erkennt das Kontrollgerät, ob es sich um eine gültige Fahrtenschreiberkarte handelt, und identifiziert in diesem Fall die Kartenart und die Kartengeneration.

Wurde eine Karte mit derselben Kartennummer und einem höheren Erneuerungsindex bereits in das Kontrollgerät eingesteckt, wird die Karte für ungültig erklärt.

Wurde eine Karte mit derselben Kartennummer und demselben Erneuerungsindex, aber einem höheren Ersatzindex bereits in das Kontrollgerät eingesteckt, wird die Karte für ungültig erklärt.

17) Die Fahrtenschreiberkarten der ersten Generation gelten für das Kontrollgerät als ungültig, nachdem die Möglichkeit der Verwendung von Fahrtenschreiberkarten der ersten Generation von einer Werkstatt in Übereinstimmung mit Anlage 15 (Anforderung MIG003) unterdrückt wurde.

18) Werkstattkarten der ersten Generation, die in ein Kontrollgerät der zweiten Generation eingesteckt werden, gelten als ungültig.

19) Das Kontrollgerät muss so ausgelegt sein, dass die Fahrtenschreiberkarten nach dem ordnungsgemäßen Einstecken in die Kartenschnittstelle einrasten.

20) Das Entnehmen der Fahrtenschreiberkarten darf nur bei stehendem Fahrzeug und nach der Speicherung der jeweiligen Daten auf die Karten sowie durch entsprechende Einwirkung des Benutzers möglich sein.

3.2 **Geschwindigkeits-, Positions- und Wegstreckenmessung**

21) Der (möglicherweise in den Adapter eingebettete) Bewegungssensor ist die wichtigste Quelle für die Geschwindigkeits- und Wegstreckenmessung.

22) Diese Funktion muss unter Verwendung der vom Bewegungssensor bereitgestellten Impulse kontinuierlich den Kilometerstand entsprechend der gesamten vom Fahrzeug zurückgelegten Wegstrecke messen und angeben können.

23) Diese Funktion muss unter Verwendung der vom Bewegungssensor bereitgestellten Impulse kontinuierlich die Geschwindigkeit des Fahrzeugs messen und angeben können.

24) Die Geschwindigkeitsmessfunktion liefert auch Informationen darüber, ob das Fahrzeug fährt oder steht. Das Fahrzeug gilt als fahrend, sobald die Funktion vom Bewegungssensor mindestens 5 Sekunden lang mehr als 1 Imp/s erhält; ansonsten gilt das Fahrzeug als stehend.

25) Geräte zur Anzeige der Geschwindigkeit (Tachometer) und der zurückgelegten Gesamtwegstrecke (Kilometerzähler), die in einem mit einem verordnungsgemäßen Kontrollgerät ausgerüsteten Fahrzeug eingebaut sind, müssen den Vorschriften über die in diesem Anhang (siehe 3.2.1 und 3.2.2) festgelegten zulässigen Fehlergrenzen entsprechen.

26) Zur Ermittlung einer etwaigen Manipulation der Bewegungsdaten sind die vom Bewegungssensor stammenden Informationen durch Daten zur Fahrzeugbewegung zu untermauern, die aus dem GNSS-Empfänger oder anderen vom Bewegungssensor unabhängigen Quellen gewonnen werden.

27) Diese Funktion misst die Position des Fahrzeugs, um die automatische Aufzeichnung der

— Positionen, an denen der Fahrer und/oder der Beifahrer seinen Arbeitstag beginnt,

— Positionen, an denen die ununterbrochene Lenkzeit des Fahrer ein Vielfaches von drei Stunden erreicht,

— Positionen, an denen der Fahrer und/oder der Beifahrer seinen Arbeitstag beendet, zu ermöglichen.

3.2.1 *Messung der zurückgelegten Wegstrecke*

28) Die zurückgelegte Wegstrecke kann gemessen werden:

— als Kumulierung der Vorwärts- und der Rückwärtsfahrt oder

— nur beim Vorwärtsfahren.

29) Das Kontrollgerät misst Wegstrecken von 0 bis 9 999 999,9 km.

30) Die gemessene Wegstrecke muss innerhalb folgender Fehlergrenzen liegen (Strecken von mindestens 1 000 m):

— ± 1 % vor dem Einbau,

— ± 2 % beim Einbau und bei den regelmäßigen Nachprüfungen,

— ± 4 % während des Betriebs.

31) Die Wegstreckenmessung erfolgt auf mindestens 0,1 km genau.

3.2.2 *Geschwindigkeitsmessung*

32) Das Kontrollgerät misst die Geschwindigkeit von 0 bis 220 km/h.

33) Zur Gewährleistung einer zulässigen Fehlergrenze der angezeigten Geschwindigkeit im Betrieb von ± 6 km/h und unter Berücksichtigung

— einer Fehlergrenze von ± 2 km/h für Inputabweichungen (Reifenabweichungen, …),

— einer Fehlergrenze von ± 1 km/h bei Messungen beim Einbau oder bei den regelmäßigen Nachprüfungen

misst das Kontrollgerät bei Geschwindigkeiten zwischen 20 und 180 km/h und bei Wegdrehzahlen des Fahrzeugs zwischen 4 000 und 25 000 Imp/km die Geschwindigkeit innerhalb einer Fehlergrenze von ± 1 km/h (bei konstanter Geschwindigkeit).

Anmerkung: Aufgrund der Auflösung der Datenspeicherung ergibt sich eine weitere zulässige Fehlergrenze von ± 0,5 km/h für die vom Kontrollgerät gespeicherte Geschwindigkeit.

34) Die Geschwindigkeit muss innerhalb der zulässigen Fehlergrenzen innerhalb von 2 Sekunden nach Abschluss einer Geschwindigkeitsänderung korrekt gemessen werden, wenn sich die Geschwindigkeit mit bis zu 2 m/s^2 geändert hat.

35) Die Geschwindigkeitsmessung erfolgt auf mindestens 1 km/h genau.

3.2.3 *Messung der Position*

36) Das Kontrollgerät misst die absolute Position des Fahrzeugs unter Verwendung des GNSS-Empfängers.

37) Die absolute Position wird in geografischen Koordinaten der Breite und Länge in Grad und Minuten mit einer Auflösung von 1/10 Minute gemessen.

3.3 Zeitmessung

38) Die Zeitmessfunktion läuft ständig und stellt Datum und Uhrzeit digital in UTC bereit.

39) Für Datierungsdaten im Kontrollgerät (Aufzeichnungen, Datenaustausch) und für sämtliche in Anlage 4 „Ausdrucke“ aufgeführten Ausdrucke sind durchgängig Datum und Uhrzeit in UTC zu verwenden.

40) Zur Anzeige der Ortszeit muss es möglich sein, den Versatz der angezeigten Zeit in Halbstundenschritten zu ändern. Ein anderer Versatz als negative oder positive Vielfache von halben Stunden ist nicht zulässig.

41) Die Zeitabweichung darf bei fehlender Zeiteinstellung ± 2 Sekunden/Tag unter Typgenehmigungsbedingungen betragen.

42) Die Zeitmessung erfolgt auf mindestens 1 Sekunde genau.

43) Die Zeitmessung darf durch eine Unterbrechung der externen Stromversorgung von weniger als 12 Monaten unter Typgenehmigungsbedingungen nicht beeinträchtigt werden.

3.4 Überwachung der Fahrertätigkeiten

44) Diese Funktion überwacht ständig und gesondert die Tätigkeiten des Fahrers und des Beifahrers.

45) Fahrertätigkeiten sind LENKEN, ARBEIT, BEREITSCHAFT und UNTERBRECHUNG/RUHE.

46) ARBEIT, BEREITSCHAFT sowie UNTERBRECHUNG/RUHE müssen vom Fahrer und/oder vom Beifahrer manuell ausgewählt werden können.

47) Während der Fahrt wird für den Fahrer automatisch LENKEN und für den Beifahrer automatisch BEREITSCHAFT ausgewählt.

48) Bei Halt wird für den Fahrer automatisch ARBEIT ausgewählt.

49) Bei der ersten Tätigkeitsänderung auf RUHE oder BEREITSCHAFT innerhalb von 120 Sekunden nach dem automatischen Wechsel auf ARBEIT infolge des Anhaltens des Fahrzeugs wird davon ausgegangen, dass diese zum Zeitpunkt des Anhaltens eingetreten ist (so dass möglicherweise der Wechsel auf ARBEIT aufgehoben wird).

50) Die Ausgabe von Tätigkeitsveränderungen an die Aufzeichnungsfunktionen erfolgt auf eine Minute genau.

51) Wird zu irgendeinem Zeitpunkt innerhalb der unmittelbar der Kalenderminute vorausgehenden und nachfolgenden Minute die Tätigkeit LENKEN registriert, gilt die gesamte Minute als LENK-Zeit.

52) Für eine Kalenderminute, die aufgrund der Randnummer 051 nicht als LENK-Zeit gilt, wird die Tätigkeit angesetzt, die als längste Tätigkeit innerhalb der Minute ausgeführt wurde (oder bei gleichlangen Tätigkeiten diejenige, die zuletzt ausgeführt wurde).

53) Diese Funktion dient auch der ständigen Überwachung der ununterbrochenen Lenkzeit und der kumulativen Unterbrechungszeit des Fahrers.

3.5 **Überwachung des Status der Fahrzeugführung**

54) Diese Funktion überwacht ständig und automatisch den Status der Fahrzeugführung.

55) Wenn zwei gültige Fahrerkarten in das Gerät eingesteckt sind, wird automatisch der Status TEAM gewählt, in allen anderen Fällen der Status EINMANNBETRIEB.

3.6 **Eingaben durch die Fahrer**

3.6.1 *Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages*

56) Diese Funktion ermöglicht dem Fahrer und/oder dem Beifahrer die Eingabe des Ortes, an dem sein jeweiliger Arbeitstag beginnt und/oder endet.

57) Als Ort gilt ein Land und gegebenenfalls zusätzlich die entsprechende Region, die manuell eingegeben und bestätigt werden.

58) Bei Entnahme einer Fahrerkarte wird der Fahrer/Beifahrer vom Kontrollgerät aufgefordert, den „Ort des Endes des Arbeitstages“ einzugeben.

59) Der Fahrer muss dann den derzeitigen Ort des Fahrzeugs eingeben, was als temporäre Eingabe gilt.

60) Die Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages muss durch Befehle in den Menus möglich sein. Erfolgt innerhalb einer Kalenderminute mehr als eine Eingabe, so wird nur die jeweils letzte in dieser Zeit vorgenommene Eingabe des Orts des Beginns und des Endes des Arbeitstages aufgezeichnet.

3.6.2 *Manuelle Eingabe der Fahrertätigkeiten und Zustimmung des Fahrers für die ITS-Schnittstelle*

61) Beim Einstecken der Fahrerkarte (oder der Werkstattkarte), und nur zu diesem Zeitpunkt, lässt das Kontrollgerät manuelle Eingaben von Tätigkeiten zu. Manuelle Eingaben von Tätigkeiten werden unter Nutzung der aktuell für die Fahrzeugeinheit eingestellten Ortszeit- und –datumswerte (UTC-Versatz) vorgenommen.

Beim Einstecken der Fahrerkarte oder der Werkstattkarte zeigt das Gerät dem Karteninhaber Folgendes an:

— Datum und Uhrzeit der letzten Kartenentnahme,

— optional: derzeit für die Fahrzeugeinheit eingestellter Ortszeitversatz.

Beim ersten Einstecken einer bestimmten Fahrerkarte oder Werkstattkarte, die der Fahrzeugeinheit noch nicht bekannt ist, wird der Karteninhaber aufgefordert, seine Zustimmung zur Ausgabe personenbezogener Daten im Zusammenhang mit dem Fahrtenschreiber über die optionale ITS-Schnittstelle zu erteilen.

Die Zustimmung des Fahrers (bzw. der Werkstatt) kann jederzeit durch Menübefehle aktiviert oder deaktiviert werden, sofern die Fahrerkarte (bzw. die Werkstattkarte) eingesteckt ist.

Es muss möglich sein, Tätigkeiten mit den folgenden Einschränkungen einzugeben:

— Tätigkeitsart ist ARBEIT, BEREITSCHAFT oder UNTERBRECHUNG/RUHE,

— Beginn- und Endzeit jeder Tätigkeit liegen ausschließlich in dem Zeitraum zwischen der letzten Entnahme und dem aktuellen Einstecken der Karte,

— zeitliche Überschneidungen von Tätigkeiten sind nicht zulässig.

Beim ersten Einstecken einer zuvor unbenutzten Fahrerkarte (oder Werkstattkarte) sind erforderlichenfalls manuelle Eingaben möglich.

Das Verfahren für manuelle Eingaben von Tätigkeiten umfasst so viele aufeinanderfolgende Schritte, wie notwendig sind, um für jede Tätigkeit eine Tätigkeitsart sowie eine Beginn- und Endzeit einzustellen. Der Karteninhaber hat für jeden Abschnitt des Zeitraums zwischen der letzten Entnahme und dem aktuellen Einstecken der Karte die Option, keine Tätigkeit anzugeben.

Während der manuellen Eingaben im Rahmen des Karteneinsteckens hat der Karteninhaber gegebenenfalls die Möglichkeit,

— für die betreffende Zeit einen Ort einzugeben, an dem ein vorhergehender Arbeitstag endete (wodurch die bei der letzten Kartenentnahme erfolgte Eingabe überschrieben wird)

— für die betreffende Zeit einen Ort einzugeben, an dem der aktuelle Arbeitstag beginnt.

Gibt der Karteninhaber während der manuellen Eingaben beim Einstecken der Karte keinen Ort ein, an dem der Arbeitstag beginnt oder endete, so gilt dies als Erklärung, dass sein Arbeitstag sich seit der letzten Kartenentnahme nicht geändert hat. Durch den nächsten Eintrag eines Orts, an dem ein vorhergehender Arbeitstag endet, wird dann die temporäre Eingabe bei der letzten Kartenentnahme überschrieben.

Bei Eingabe eines Ortes wird dieser auf der entsprechenden Fahrtenschreiberkarte aufgezeichnet.

Manuelle Eingaben werden in folgenden Fällen unterbrochen:

— wenn die Karte entnommen wird oder

— wenn das Fahrzeug fährt, während die Karte in den Kartensteckplatz des Fahrers eingesteckt ist.

Weitere Unterbrechungen, z. B. ein Timeout nach einer bestimmten Inaktivitätszeit des Nutzers, sind möglich. Im Falle der Unterbrechung manueller Eingaben validiert das Kontrollgerät alle bereits vorgenommenen vollständigen Orts- und Tätigkeitseingaben (mit eindeutiger Angabe von Ort und Zeit oder Tätigkeitsart, Beginn- und Endzeit).

Wird eine zweite Fahrer- oder Werkstattkarte eingesteckt, während manuelle Eingaben von Tätigkeiten für eine zuvor eingesteckte Karte vorgenommen werden, so ist die Fertigstellung der manuellen Eingaben für diese vorherige Karte vor Beginn der manuellen Eingaben für die zweite Karte zu erlauben.

Der Karteninhaber hat die Option, nach folgendem Minimalverfahren manuelle Eingaben vorzunehmen:

— Manuelle Eingabe von Tätigkeiten in zeitlicher Reihenfolge für den Zeitraum zwischen der letzten Kartenentnahme und dem aktuellen Einstecken der Karte.

— Der Zeitpunkt des Beginns der ersten Tätigkeit wird auf den Zeitpunkt der Kartenentnahme festgelegt. Für jede nachfolgende Eingabe wird der Zeitpunkt des Beginns so voreingestellt, dass er unmittelbar auf den Zeitpunkt des Endes der vorherigen Eingabe folgt. Für jede Tätigkeit wird die Tätigkeitsart sowie der Zeitpunkt des Beginns und des Endes gewählt.

Das Verfahren endet, wenn der Zeitpunkt des Endes einer manuell eingegebenen Tätigkeit dem Zeitpunkt des Einsteckens der Karte entspricht. Anschließend kann das Kontrollgerät dem Karteninhaber optional die Möglichkeit einräumen, Änderungen an den manuell eingegebenen Tätigkeiten vorzunehmen, bis mittels eines speziellen Befehls die Validierung erfolgt. Danach sind solche Änderungen nicht mehr zulässig.

3.6.3 *Eingabe spezifischer Bedingungen*

62) Das Kontrollgerät gestattet dem Fahrer die Eingabe der folgenden beiden spezifischen Bedingungen in Echtzeit:

— „KONTROLLGERÄT NICHT ERFORDERLICH“ (Anfang, Ende)

— „FÄHRÜBERFAHRT/ZUGFAHRT“ (Anfang, Ende).

Bei eingeschalteter Bedingung „KONTROLLGERÄT NICHT ERFORDERLICH“ darf keine „FÄHRÜBERFAHRT/ZUGFAHRT“ erfolgen.

Beim Einstecken oder Entnehmen einer Fahrerkarte muss die eingeschaltete Bedingung „KONTROLLGERÄT NICHT ERFORDERLICH“ automatisch ausgeschaltet werden.

Die eingeschaltete Bedingung „KONTROLLGERÄT NICHT ERFORDERLICH“ muss die folgenden Ereignisse und Warnsignale unterbinden:

— Lenken ohne geeignete Karte,

— mit der ununterbrochenen Lenkzeit verbundene Warnsignale.

Der Merker für den Anfang der Bedingung „FÄHRÜBERFAHRT/ZUGFAHRT“ muss vor dem Abstellen des Motors auf der Fähre/im Zug gesetzt werden.

Die eingeschaltete Bedingung „FÄHRÜBERFAHRT/ZUGFAHRT“ muss enden, wenn eine der folgenden Optionen gilt:

— der Fahrer beendet „FÄHRÜBERFAHRT/ZUGFAHRT“ manuell

— der Fahrer entnimmt seine Karte.

Eine eingeschaltete Bedingung „FÄHRÜBERFAHRT/ZUGFAHRT“ muss enden, wenn sie gemäß der Verordnung (EG) Nr. 561/2006 nicht mehr gültig ist.

3.7 **Unternehmenssperren**

63) Diese Funktion ermöglicht die Verwaltung der Sperren, die ein Unternehmen einsetzt, um den Datenzugang in der Betriebsart Unternehmen auf sich selbst zu beschränken.

64) Unternehmenssperren bestehen aus einem Anfangszeitpunkt (Datum/Uhrzeit) (Sperrung, Lock-in) und einem Endzeitpunkt (Datum/Uhrzeit) (Entsperrung, Lock-out) im Zusammenhang mit der Identifizierung des Unternehmens anhand der Unternehmenskartennummer (bei der Sperrung).

65) Sperren können nur in Echtzeit ein- oder ausgeschaltet werden.

66) Das Ausschalten der Sperre kann nur durch das Unternehmen (ausgewiesen durch die ersten 13 Stellen der Unternehmenskartennummer) erfolgen, dessen Sperre eingeschaltet ist, oder

67) erfolgt automatisch, wenn ein anderes Unternehmen seine Sperre einschaltet.

68) Aktiviert ein Unternehmen die Sperrung (Lock-in) und die vorhergehende Sperrung war für dasselbe Unternehmen, dann wird davon ausgegangen, dass vorher keine Entsperrung vorgenommen worden ist und die Sperre noch eingeschaltet ist.

3.8 **Überwachung von Kontrollen**

69) Diese Funktion überwacht die Aktivitäten ANZEIGE, DRUCK, FAHRZEUGEINHEIT sowie HERUNTERLADEN von der Karte und STRASSENSEITIGE KALIBRIERUNGSÜBERPRÜFUNG in der Betriebsart Kontrolle.

70) Diese Funktion überwacht darüber hinaus in der Betriebsart Kontrolle die KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG. Eine Kontrolle Geschwindigkeitsüberschreitung gilt als erfolgt, wenn in der Betriebsart Kontrolle der Ausdruck „Geschwindigkeitsüberschreitung" an den Drucker oder an die Anzeige gesandt wurde oder wenn „Ereignis- und Störungsdaten" aus dem Massenspeicher der Fahrzeugeinheit heruntergeladen wurden.

3.9 **Feststellung von Ereignissen und/oder Störungen**

71) Diese Funktion stellt folgende Ereignisse und/oder Störungen fest:

3.9.1 *Ereignis „Einstecken einer ungültigen Karte"*

72) Dieses Ereignis wird beim Einstecken einer ungültigen Karte, beim Einstecken einer bereits ersetzen Fahrerkarte und/oder beim Ablauf einer eingesteckten gültigen Karte ausgelöst.

3.9.2 *Ereignis „Kartenkonflikt"*

73) Dieses Ereignis wird ausgelöst, wenn eine der in der folgenden Tabelle mit X gekennzeichneten Kombinationen von gültigen Karten vorliegt:

Kartenkonflikt		Steckplatz des Fahrers				
		Keine Karte	Fahrerkarte	Kontrollkarte	Werkstattkarte	Unternehmens-karte
Steckplatz des Beifahrers	Keine Karte					
	Fahrerkarte				X	
	Kontrollkarte			X	X	X
	Werkstattkarte		X	X	X	X
	Unternehmens-karte			X	X	X

3.9.3 *Ereignis „Zeitüberlappung"*

74) Dieses Ereignis wird ausgelöst, wenn Datum/Uhrzeit der letzten Entnahme einer Fahrerkarte beim Auslesen der Karte der aktuellen Datums-/Uhrzeiteinstellung des Kontrollgeräts voraus sind.

3.9.4 *Ereignis „Lenken ohne geeignete Karte“*

75) Dieses Ereignis wird bei einer in der folgenden Tabelle mit X gekennzeichneten Kombination gültiger Fahrtenschreiberkarten ausgelöst, wenn die Fahrertätigkeit auf LENKEN wechselt oder wenn während der Fahrertätigkeit LENKEN eine Änderung der Betriebsart erfolgt.

Lenken ohne geeignete Karte		Steckplatz des Fahrers				
		Keine (oder ungültige) Karte	Fahrerkarte	Kontrollkarte	Werkstattkarte	Unternehmenskarte
Steckplatz des Beifahrers	Keine (oder ungültige) Karte	X		X		X
	Fahrerkarte	X		X	X	X
	Kontrollkarte	X	X	X	X	X
	Werkstattkarte	X	X	X		X
	Unternehmenskarte	X	X	X	X	X

3.9.5 *Ereignis „Einstecken der Karte während des Lenkens“*

76) Dieses Ereignis wird ausgelöst, wenn eine Fahrtenschreiberkarte während der Fahrertätigkeit LENKEN in einen der Steckplätze eingesteckt wird.

3.9.6 *Ereignis „Letzter Vorgang nicht korrekt abgeschlossen“*

77) Dieses Ereignis wird ausgelöst, wenn das Kontrollgerät beim Einstecken der Karte feststellt, dass trotz der Bestimmungen in Nummer 3.1 der vorherige Kartenvorgang nicht korrekt abgeschlossen wurde (Kartenentnahme, bevor alle relevanten Daten auf der Karte gespeichert wurden). Dieses Ereignis wird nur von Fahrer- und Werkstattkarten ausgelöst.

3.9.7 *Ereignis „Geschwindigkeitsüberschreitung“*

78) Dieses Ereignis wird bei jeder Geschwindigkeitsüberschreitung ausgelöst.

3.9.8 *Ereignis „Unterbrechung der Stromversorgung“*

79) Dieses Ereignis wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung oder Kontrolle befindet, bei einer 200 Millisekunden überschreitenden Unterbrechung der Stromversorgung des Bewegungssensors und/oder der Fahrzeugeinheit ausgelöst. Die Unterbrechungsschwelle wird vom Hersteller festgelegt. Nicht ausgelöst wird das Ereignis durch den Stromabfall beim Starten des Fahrzeugmotors.

3.9.9 *Ereignis „Kommunikationsfehler mit der Fernkommunikationsausrüstung“*

80) Dieses Ereignis wird, sofern sich das Kontrollgerät **nicht in der Betriebsart Kalibrierung** befindet, ausgelöst, wenn die Fernkommunikationsausrüstung nach mehr als drei Versuchen nicht den erfolgreichen Empfang der von der Fahrzeugeinheit übermittelten Fernkommunikationsdaten bestätigt.

3.9.10 *Ereignis „Fehlende Positionsdaten des GNSS-Empfängers“*

81) Dieses Ereignis wird, sofern sich das Kontrollgerät **nicht in der Betriebsart Kalibrierung** befindet, ausgelöst, wenn während der Fahrt vom (internen oder externen) GNSS-Empfänger stammende Positionsdaten für mehr als 3 Stunden kumulierte Lenkzeit fehlen.

3.9.11 *Ereignis „Kommunikationsfehler mit der externen GNSS-Ausrüstung“*

82) Dieses Ereignis wird, sofern sich das Kontrollgerät **nicht in der Betriebsart Kalibrierung** befindet, ausgelöst, wenn während der Fahrt die Kommunikation zwischen der externen GNSS-Ausrüstung und dem Fahrzeug für mehr als 20 Minuten durchgehend unterbrochen ist.

3.9.12 *Ereignis „Datenfehler Bewegungssensor“*

83) Dieses Ereignis wird, sofern sich das Kontrollgerät **nicht in der Betriebsart Kalibrierung** befindet, bei einer Unterbrechung des normalen Datenflusses zwischen dem Bewegungssensor und der Fahrzeugeinheit und/oder bei einem Datenintegritäts- oder Datenauthentizitätsfehler während des Datenaustauschs zwischen Bewegungssensor und Fahrzeugeinheit ausgelöst.

3.9.13 *Ereignis „Datenkonflikt Fahrzeugbewegung“*

84) Dieses Ereignis wird, sofern sich das Kontrollgerät **nicht in der Betriebsart Kalibrierung** befindet, ausgelöst, wenn die vom Bewegungssensor berechneten Bewegungsangaben in Widerspruch zu den vom internen GNSS-Empfänger oder von der externen GNSS-Ausrüstung berechneten Bewegungsangaben und optional zu den Bewegungsangaben aus anderen unabhängigen Quellen gemäß Anlage 12 steht. Dieses Ereignis wird nicht ausgelöst während einer Fährüberfahrt/Zugfahrt, einer Bedingung „KONTROLLGERÄT NICHT ERFORDERLICH“ oder wenn keine Positionsdaten des GNSS-Empfängers verfügbar sind.

3.9.14 *Ereignis „Versuch einer Sicherheitsverletzung“*

85) Dieses Ereignis wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet, bei jedem sonstigen Ereignis ausgelöst, das die Sicherheit des Bewegungssensors und/oder der Fahrzeugeinheit und/oder der externen GNSS-Ausrüstung gemäß Anlage 10 beeinträchtigt.

3.9.15 *Ereignis „Zeitkonflikt“*

86) Dieses Ereignis wird, sofern sich das Kontrollgerät **nicht in der Betriebsart Kalibrierung** befindet, ausgelöst, wenn die Fahrzeugeinheit eine Abweichung von mehr als 1 Minute zwischen der Zeit der Zeitmessfunktion der Fahrzeugeinheit und der vom GNSS-Empfänger stammenden Zeit feststellt. Dieses Ereignis wird gemeinsam mit dem Wert der Systemuhr der Fahrzeugeinheit aufgezeichnet und geht mit einer automatischen Zeiteinstellung einher. Nachdem ein Ereignis „Zeitkonflikt“ ausgelöst wurde, erzeugt die Fahrzeugeinheit in den nächsten 12 Stunden keine weiteren Zeitkonflikt-Ereignisse. Das Ereignis wird nicht ausgelöst, wenn der GNSS-Empfänger innerhalb der letzten 30 Tage kein gültiges GNSS-Signal feststellen konnte. Wenn jedoch Positionsdaten des GNSS-Empfänger wieder verfügbar sind, erfolgt die automatische Zeiteinstellung.

3.9.16 *Störung „Kartenfehlfunktion“*

87) Diese Störung wird ausgelöst, wenn während des Betriebs eine Fehlfunktion der Fahrtenschreiberkarte auftritt.

3.9.17 *Störung „Kontrollgerät“*

88) Diese Störung wird bei folgenden Fehlfunktionen ausgelöst, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet:

— interne Störung der Fahrzeugeinheit

— Druckerstörung

— Anzeigestörung

— Störung beim Herunterladen

— Sensorstörung

— Störung des GNSS-Empfängers oder der externen GNSS-Ausrüstung

— Störung der Fernkommunikationsausrüstung.

3.10 **Integrierte Tests und Selbsttests**

89) Mit Hilfe der Funktion „Integrierte Tests und Selbsttests" muss das Kontrollgerät zur automatischen Störungserkennung anhand der folgenden Tabelle in der Lage sein:

Zu testende Unterbaugruppe	Selbsttest	Integrierter Test
Software		Integrität
Massenspeicher	Zugang	Zugang, Datenintegrität
Kartenschnittstellen	Zugang	Zugang
Tastatur		Manuelle Prüfung
Drucker	(dem Hersteller überlassen)	Ausdruck
Datenanzeige		Sichtprüfung
Herunterladen (nur während des Herunterladens)	Ordnungsgemäßer Betrieb	
Sensor	Ordnungsgemäßer Betrieb	Ordnungsgemäßer Betrieb
Fernkommunikationsausrüstung	Ordnungsgemäßer Betrieb	Ordnungsgemäßer Betrieb
GNSS-Ausrüstung	Ordnungsgemäßer Betrieb	Ordnungsgemäßer Betrieb

3.11 **Auslesen von Daten aus dem Massenspeicher**

90) Das Kontrollgerät muss sämtliche in seinem Massenspeicher gespeicherte Daten auslesen können.

3.12 **Aufzeichnung und Speicherung von Daten im Massenspeicher**

Im Sinne dieses Absatzes

— sind „365 Tage" 365 Kalendertage mit durchschnittlicher Fahrertätigkeit in einem Fahrzeug. Als durchschnittliche Tätigkeit je Tag in einem Fahrzeug gelten mindestens 6 Fahrer oder Beifahrer, 6 Karteneinsteck-/-entnahmevorgänge und 256 Tätigkeitswechsel. Somit umfassen „365 Tage" mindestens 2 190 Fahrer/Beifahrer, 2 190 Karteneinsteck-/-entnahmevorgänge und 93 440 Tätigkeitswechsel;

— gelten als durchschnittliche Zahl der Positionen je Tag mindestens 6 Positionen, an denen die tägliche Arbeitszeit beginnt, 6 Positionen, wenn die ununterbrochene Lenkzeit des Fahrers ein Vielfaches von drei Stunden erreicht, und 6 Positionen, an denen die tägliche Arbeitszeit endet, so dass „365 Tage" mindestens 6 570 Positionen umfassen;

— erfolgt die Zeitaufzeichnung auf eine Minute genau, sofern nicht anders angegeben;

— erfolgt die Aufzeichnung des Kilometerstands auf einen Kilometer genau;

— erfolgt die Geschwindigkeitsaufzeichnung auf 1 km/h genau;

— werden Positionen (Längen- und Breitengrade) in Grad und Minuten mit einer Auflösung von 1/10 Minute des GNSS aufgezeichnet, zusammen mit der jeweiligen GNSS-Genauigkeit und dem Aufnahmezeitpunkt.

91) Die im Massenspeicher gespeicherten Daten dürfen durch eine Unterbrechung der externen Stromversorgung von weniger als 12 Monaten unter Typgenehmigungsbedingungen nicht beeinträchtigt werden. Darüber hinaus dürfen in der Fernkommunikationsausrüstung nach Anlage 14 gespeicherte Daten nicht durch eine Unterbrechung der Stromversorgung von weniger als 28 Tagen beeinträchtigt werden.

92) Das Kontrollgerät muss in seinem Massenspeicher Folgendes implizit oder explizit aufzeichnen und speichern können:

3.12.1 *Gerätekenndaten*

3.12.1.1 Kenndaten der Fahrzeugeinheit

93) Das Kontrollgerät muss in seinem Massenspeicher folgende Kenndaten der Fahrzeugeinheit speichern können:

— Name des Herstellers,

— Anschrift des Herstellers,

— Teilnummer,

— Seriennummer,

— Generation der Fahrzeugeinheit,

— Fähigkeit zur Verwendung von Fahrtenschreiberkarten der ersten Generation,

— Softwareversionsnummer,

— Installationsdatum der Softwareversion,

— Herstellungsjahr,

— Typgenehmigungsnummer,

94) Die Kenndaten der Fahrzeugeinheit werden von deren Hersteller aufgezeichnet und dauerhaft gespeichert; eine Ausnahme bilden die softwarebezogenen Daten und die Typgenehmigungsnummer, die bei einer Aktualisierung der Software verändert werden dürfen, sowie die Fähigkeit zur Verwendung von Fahrtenschreiberkarten der ersten Generation.

3.12.1.2 Kenndaten des Bewegungssensors

95) Der Bewegungssensor muss in seinem Speicher folgende Kenndaten speichern können:

— Name des Herstellers,

— Seriennummer,

— Typgenehmigungsnummer,

— Bezeichner der eingebetteten Sicherheitskomponenten (z. B. Teilnummer des internen Chips/Prozessors),

— Betriebssystembezeichner (z. B. Softwareversionsnummer).

96) Die Kenndaten des Bewegungssensors werden von dessen Hersteller aufgezeichnet und dauerhaft gespeichert.

97) Die Fahrzeugeinheit muss in ihrem Massenspeicher folgende Daten in Bezug auf die 20 jüngsten Koppelungen von Bewegungssensoren speichern können (erfolgen mehrere Koppelungen binnen eines Kalendertages, so sind nur die erste und die letzte Koppelung des Tages zu speichern):

Zu den einzelnen Koppelungen sind folgende Daten zu speichern:

— Kenndaten des Bewegungssensors:

— Seriennummer

— Typgenehmigungsnummer,

— Koppelungsdaten des Bewegungssensors:

— Koppelungsdatum.

3.12.1.3 Kenndaten der globalen Satellitennavigationssysteme

98) Die externe GNSS-Ausrüstung muss in ihrem Speicher folgende Kenndaten speichern können:

— Name des Herstellers,

— Seriennummer,

— Typgenehmigungsnummer,

— Bezeichner der eingebetteten Sicherheitskomponenten (z. B. Teilnummer des internen Chips/Prozessors),

— Betriebssystembezeichner (z. B. Softwareversionsnummer).

99) Die Kenndaten werden vom Hersteller der externen GNSS-Ausrüstung aufgezeichnet und dauerhaft gespeichert.

100) Die Fahrzeugeinheit muss in ihrem Massenspeicher folgende Daten in Bezug auf die 20 jüngsten Kopplungen von externen GNSS-Ausrüstungen speichern können (erfolgen mehrere Kopplungen binnen eines Kalendertages, so sind nur die erste und die letzte Kopplung des Tages zu speichern):

Zu den einzelnen Kopplungen sind folgende Daten zu speichern:

— Kenndaten der externen GNSS-Ausrüstung:

— Seriennummer,

— Typgenehmigungsnummer,

— Kopplungsdaten der externen GNSS-Ausrüstung:

— Kopplungsdatum.

3.12.2 *Schlüssel und Zertifikate*

101) Das Kontrollgerät muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil A und Teil B speichern können.

3.12.3 *Einsteck- und Entnahmedaten der Fahrer- oder der Werkstattkarte*

102) Bei jedem Einsteck-/Entnahmevorgang einer Fahrer- oder Werkstattkarte registriert und speichert das Kontrollgerät folgende Daten in seinem Massenspeicher:

— Name und Vorname(n) des Karteninhabers in der auf der Karte gespeicherten Form,

— Kartennummer, ausstellender Mitgliedstaat und Ablauf der Gültigkeit in der auf der Karte gespeicherten Form,

— die Kartengeneration,

— Datum und Uhrzeit des Einsteckens,

— Kilometerstand beim Einstecken der Karte,

— Steckplatz, in den die Karte eingesteckt wurde,

— Datum und Uhrzeit der Entnahme,

— Kilometerstand bei Kartenentnahme,

— folgende Informationen über das zuvor vom Fahrer benutzte Fahrzeug in der auf der Karte gespeicherten Form:

— amtliches Kennzeichen und zulassender Mitgliedstaat,

— Generation der Fahrzeugeinheit (sofern verfügbar),

— Datum und Uhrzeit der Kartenentnahme,

— Merker zur Angabe, ob der Karteninhaber beim Einstecken Tätigkeiten manuell eingegeben hat oder nicht.

103) Die Speicherdauer dieser Daten im Massenspeicher muss mindestens 365 Tage betragen können.

104) Ist die Speicherkapazität erschöpft, werden die ältesten Daten durch neue überschrieben.

3.12.4 *Fahrertätigkeitsdaten*

105) Bei jedem Wechsel der Tätigkeit des Fahrers und/oder Beifahrers und/oder bei jedem Wechsel des Status der Fahrzeugführung und/oder bei jedem Einstecken bzw. jeder Entnahme einer Fahrer- oder Werkstattkarte wird im Massenspeicher des Kontrollgeräts aufgezeichnet und gespeichert:

— der Status der Fahrzeugführung (TEAM, EINMANNBETRIEB),

— den Steckplatz (FAHRER, BEIFAHRER),

— der Kartenstatus im jeweiligen Steckplatz (EINGESTECKT, NICHT EINGESTECKT),

— die Tätigkeit (LENKEN, BEREITSCHAFT, ARBEIT, UNTERBRECHUNG/RUHE),

— Datum und Uhrzeit des Wechsels.

EINGESTECKT bedeutet, dass eine gültige Fahrer- oder Werkstattkarte im Steckplatz eingesteckt ist. NICHT EINGESTECKT bedeutet das Gegenteil, d. h. es ist keine gültige Fahrer- oder Werkstattkarte eingesteckt (z. B. ist eine Unternehmenskarte oder keine Karte eingesteckt).

Vom Fahrer manuell eingegebene Tätigkeitsdaten werden im Massenspeicher nicht aufgezeichnet.

106) Die Speicherdauer der Fahrertätigkeitsdaten im Massenspeicher muss mindestens 365 Tage betragen können.

107) Ist die Speicherkapazität erschöpft, werden die ältesten Daten durch neue überschrieben.

3.12.5 *Orte und Positionen, an denen die tägliche Arbeitszeit beginnt, endet und/oder eine ununterbrochene Lenkzeit von 3 Stunden erreicht wird*

108) Das Kontrollgerät registriert und speichert in seinem Massenspeicher:

— Orte und Positionen, an denen der Fahrer und/oder der Beifahrer seinen Arbeitstag beginnt,

— Positionen, an denen die ununterbrochene Lenkzeit des Fahrer ein Vielfaches von drei Stunden erreicht,

— Orte und Positionen, an denen der Fahrer und/oder der Beifahrer seinen Arbeitstag beendet.

109) Wenn die Position des Fahrzeugs zu diesen Zeiten nicht über den GNSS-Empfänger verfügbar ist, verwendet das Kontrollgerät die letzte verfügbare Position und das entsprechende Datum und die entsprechende Uhrzeit.

110) Zusammen mit jedem Ort bzw. jeder Position registriert das Kontrollgerät und speichert in seinem Massenspeicher:

— die Nummer der (Bei-)Fahrerkarte und den ausstellenden Mitgliedstaat,

— die Kartengeneration,

— Datum und Uhrzeit der Eingabe,

— Art der Eingabe (Beginn, Ende oder ununterbrochene Lenkzeit von 3 Stunden),

— die damit verbundene GNSS-Genauigkeit, Datum und Uhrzeit, falls zutreffend,

— Kilometerstand.

111) Die Speicherdauer der Orte und Positionen, an denen die tägliche Arbeitszeit beginnt, endet und/oder eine ununterbrochene Lenkzeit von 3 Stunden erreicht wird, im Massenspeicher muss mindestens 365 Tage betragen können.

112) Ist die Speicherkapazität erschöpft, werden die ältesten Daten durch neue überschrieben.

3.12.6 *Kilometerstandsdaten*

113) Das Kontrollgerät registriert in seinem Massenspeicher an jedem Kalendertag um Mitternacht den Kilometerstand des Fahrzeugs und das dazugehörige Datum.

114) Die Speicherdauer des mitternächtlichen Kilometerstands im Massenspeicher muss mindestens 365 Tage betragen können.

115) Ist die Speicherkapazität erschöpft, werden die ältesten Daten durch neue überschrieben.

3.12.7 *Detaillierte Geschwindigkeitsdaten*

116) Das Kontrollgerät registriert und speichert in seinem Massenspeicher zu jeder Sekunde mindestens der letzten 24 Stunden, in denen das Fahrzeug gefahren wurde, die Momentangeschwindigkeit des Fahrzeugs mit den dazugehörigen Datums- und Uhrzeitangaben.

3.12.8 *Ereignisdaten*

Im Sinne dieses Unterabsatzes erfolgt die Zeitspeicherung auf 1 Sekunde genau.

117) Bei jedem festgestellten Ereignis registriert und speichert das Kontrollgerät die folgenden Daten entsprechend den nachfolgend aufgeführten Speicherungsvorschriften:

Ereignis	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Einstecken einer ungültigen Karte	— Die 10 jüngsten Ereignisse.	— Datum und Uhrzeit des Ereignisses, — Kartentyp, Nummer, ausstellender Mitgliedstaat und Generation der Karte, die das Ereignis hervorgerufen hat. — Anzahl gleichartiger Ereignisse an diesem Tag.
Kartenkonflikt	— Die 10 jüngsten Ereignisse.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation der beiden Karten, die den Konflikt hervorrufen.
Lenken ohne geeignete Karte	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Kartentyp, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.

Ereignis	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Einstecken der Karte während des Lenkens	— Das letzte Ereignis an jedem der letzten 10 Tage des Auftretens,	— Datum und Uhrzeit des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation, — Anzahl gleichartiger Ereignisse an diesem Tag.
Letzter Vorgang nicht korrekt abgeschlossen	— Die 10 jüngsten Ereignisse.	— Datum und Uhrzeit des Einsteckens der Karte, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation, — Daten des letzten Vorgangs beim Auslesen der Karte: — Datum und Uhrzeit des Einsteckens der Karte, — amtliches Kennzeichen, Zulassungsmitgliedstaat und Generation der Fahrzeugeinheit.
Geschwindigkeitsüberschreitung (1)	— Das schwerwiegendste Ereignis an jedem der letzten 10 Tage des Auftretens (d. h. das Ereignis mit der höchsten Durchschnittsgeschwindigkeit), — die 5 schwerwiegendsten Ereignisse in den letzten 365 Tagen — das erste Ereignis oder die erste Störung nach der letzten Kalibrierung	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — die während des Ereignisses gemessene Höchstgeschwindigkeit, — die während des Ereignis gemessene arithmetische Durchschnittsgeschwindigkeit, — Typ der Karte, Nummer, ausstellender Mitgliedstaat und Generation der Fahrerkarte (falls zutreffend), — Anzahl gleichartiger Ereignisse an diesem Tag.
Unterbrechung der Stromversorgung (2)	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.
Kommunikationsfehler mit der Fernkommunikationsausrüstung	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.
Fehlende Positionsdaten des GNSS-Empfängers	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.

Ereignis	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Datenfehler Weg und Geschwindigkeit	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.
Datenkonflikt Fahrzeugbewegung	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.
Versuch einer Sicherheitsverletzung	— Die 10 jüngsten Ereignisse je Ereignisart,	— Datum und Uhrzeit des Beginns des Ereignisses, — Datum und Uhrzeit des Endes des Ereignisses(sofern relevant), — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Art des Ereignisses.
Zeitkonflikt	— Das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit Kontrollgerät — GNSS-Datum und -Uhrzeit, — Typ der Karte(n), Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag.

(1) Im Massenspeicher des Kontrollgeräts sind darüber hinaus folgende Daten aufzuzeichnen und zu speichern:

— Datum und Uhrzeit der letzten KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG,

— Datum und Uhrzeit der ersten Geschwindigkeitsüberschreitung nach dieser KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG,

— Anzahl der Ereignisse Geschwindigkeitsüberschreitung seit der letzten KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG.

(2) Diese Daten können erst nach Wiederherstellung der Stromversorgung aufgezeichnet werden, wobei die Genauigkeit hier eine Minute betragen kann.

3.12.9 *Störungsdaten*

Im Sinne dieses Unterabsatzes erfolgt die Zeitaufzeichnung auf 1 Sekunde genau.

118) Bei jeder festgestellten Störung muss das Kontrollgerät versuchen, die folgenden Daten entsprechend den nachfolgend aufgeführten Speicherungsvorschriften aufzuzeichnen und zu speichern:

Störung	Speicherungsvorschriften	Je Störung aufzuzeichnende Daten
Kartenfehlfunktion	— Die 10 jüngsten Fahrerkartenfehlfunktionen.	— Datum und Uhrzeit des Beginns der Störung, — Datum und Uhrzeit des Endes der Störung, — Typ der Karte (n), Nummer, ausstellender Mitgliedstaat und Generation.
Störungen Kontrollgerät	— Die 10 jüngsten Störungen jeder Störungsart, — die erste Störung nach der letzten Kalibrierung.	— Datum und Uhrzeit des Beginns der Störung, — Datum und Uhrzeit des Endes der Störung, — Art der Störung, — Typ der Karte(n), Nummer und ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende der Störung eingesteckten Karte.

3.12.10 *Kalibrierungsdaten*

119) Im Massenspeicher des Kontrollgeräts sind Daten aufzuzeichnen und zu speichern, die folgendes betreffen:

— bekannte Kalibrierungsparameter zum Zeitpunkt der Aktivierung,

— seine erste Kalibrierung nach der Aktivierung,

— seine erste Kalibrierung im derzeitigen Fahrzeug (identifiziert anhand von dessen Fahrzeug-Identifizierungsnummer),

— die 20 jüngsten Kalibrierungen (erfolgen an einem Kalendertag mehrere Kalibrierungen, sind nur die erste und die letzte des Tages zu speichern).

120) Zu den einzelnen Kalibrierungen sind folgende Daten zu speichern:

— Zweck der Kalibrierung (Aktivierung, Ersteinbau, Einbau, regelmäßige Nachprüfung),

— Name und Anschrift der Werkstatt,

— Werkstattkartennummer, ausstellender Mitgliedstaat und Ablauf der Gültigkeit der Karte,

— Fahrzeugkennung,

— aktualisierte oder bestätigte Parameter: Wegdrehzahl (w), Kontrollgerätkonstante (k), tatsächlicher Reifenumfang (l), Reifengröße, Einstellung des Geschwindigkeitsbegrenzers, Kilometerstand (alt und neu), Datum und Uhrzeit (alte und neue Werte),

— Typ und Kennung aller vorhandenen Plombierungen.

121) Zusätzlich ist im Massenspeicher des Kontrollgeräts seine Fähigkeit zur Verwendung von Fahrtenschreiberkarten der ersten Generation (noch aktiviert oder nicht) aufzuzeichnen und zu speichern.

122) Im Speicher des Bewegungssensors sind folgende Einbaudaten aufzuzeichnen und zu speichern:

— erste Koppelung mit einer Fahrzeugeinheit (Datum, Uhrzeit, VU-Typgenehmigungsnummer, VU-Seriennummer),

— letzte Koppelung mit einer Fahrzeugeinheit (Datum, Uhrzeit, VU-Typgenehmigungsnummer, VU-Seriennummer).

123) Im Speicher der externen GNSS-Ausrüstung sind folgende Einbaudaten aufzuzeichnen und zu speichern:

— erste Kopplung mit einer Fahrzeugeinheit (Datum, Uhrzeit, VU-Typgenehmigungsnummer, VU-Seriennummer),

— letzte Kopplung mit einer Fahrzeugeinheit (Datum, Uhrzeit, VU-Typgenehmigungsnummer, VU-Seriennummer).

3.12.11 *Zeiteinstellungsdaten*

124) Im Massenspeicher des Kontrollgeräts sind Daten zu Zeiteinstellungen, die in der Betriebsart Kalibrierung außerhalb einer normalen Kalibrierung (Begriffsbestimmung f) vorgenommen werden, aufzuzeichnen und zu speichern:

— die jüngste Zeiteinstellung,

— die 5 größten Zeiteinstellungen.

125) Zu den einzelnen Zeiteinstellungen sind folgende Daten zu speichern:

— Datum und Uhrzeit, alter Wert,

— Datum und Uhrzeit, neuer Wert,

— Name und Anschrift der Werkstatt,

— Werkstattkartennummer, ausstellender Mitgliedstaat, Kartengeneration und Ablauf der Gültigkeit der Karte.

3.12.12 *Kontrolltätigkeitsdaten*

126) Im Massenspeicher des Kontrollgeräts sind folgende Daten in Bezug auf die 20 jüngsten Kontrolltätigkeiten aufzuzeichnen und zu speichern:

— Datum und Uhrzeit der Kontrolle,

— Kontrollkartennummer, ausstellender Mitgliedstaat und Kartengeneration,

— Art der Kontrolle (Anzeige und/oder Drucken und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte und/oder straßenseitige Kalibrierungsüberprüfung).

127) Beim Herunterladen sind zudem die ältesten und die jüngsten heruntergeladenen Tage aufzuzeichnen.

3.12.13 *Unternehmenssperrdaten*

128) Im Massenspeicher des Kontrollgeräts sind folgende Daten in Bezug auf die 255 jüngsten Unternehmenssperren aufzuzeichnen und zu speichern:

— Sperrung (/Lock-in) — Datum und Uhrzeit,

— Entsperrung (/Lock-out) — Datum und Uhrzeit,

— Unternehmenskartennummer, ausstellender Mitgliedstaat und Kartengeneration,

— Name und Anschrift des Unternehmens.

Daten, die zuvor durch eine Sperre gesperrt waren, die aufgrund obiger Begrenzung aufgehoben wurde, werden als nicht gesperrt behandelt.

3.12.14 *Erfassen des Herunterladens*

129) Im Massenspeicher des Kontrollgeräts sind in Bezug auf das letzte Herunterladen vom Massenspeicher auf externe Datenträger in den Betriebsarten Unternehmen oder Kalibrierung folgende Daten aufzuzeichnen und zu speichern:

— Datum und Uhrzeit des Herunterladens,

— Unternehmens- oder Werkstattkartennummer, ausstellender Mitgliedstaat und Kartengeneration,

— Name des Unternehmens oder der Werkstatt.

3.12.15 *Daten zu spezifischen Bedingungen*

130) Im Massenspeicher des Kontrollgeräts sind folgende Daten in Bezug auf spezifische Bedingungen aufzuzeichnen:

— Datum und Uhrzeit der Eingabe,

— Art der spezifischen Bedingung.

131) Die Speicherdauer der Daten zu spezifischen Bedingungen im Massenspeicher muss mindestens 365 Tage betragen können (unter der Annahme, dass pro Tag 1 Bedingung ein- und ausgeschaltet wird). Ist die Speicherkapazität erschöpft, werden die ältesten Daten durch neue überschrieben.

3.12.16 *Daten der Fahrtenschreiberkarte*

132) Das Kontrollgerät muss die folgenden Daten in Bezug auf die verschiedenen in der Fahrzeugeinheit verwendeten Fahrtenschreiberkarten speichern können:

— Nummer und Seriennummer der Fahrtenschreiberkarte,

— Hersteller der Fahrtenschreiberkarte,

— Art der Fahrtenschreiberkarte,

— Version der Fahrtenschreiberkarte.

133) Das Kontrollgerät muss mindestens 88 derartige Datensätze speichern können.

3.13 **Auslesen von Daten aus Fahrtenschreiberkarten**

134) Das Kontrollgerät muss aus Fahrtenschreiberkarten der ersten und der zweiten Generation die erforderlichen Daten

— zur Identifizierung der Kartenart, des Karteninhabers, des zuvor genutzten Fahrzeugs, des Datums und der Uhrzeit der letzten Kartenentnahme und der zu jenem Zeitpunkt gewählten Tätigkeit,

— zur Kontrolle des korrekten Abschlusses des letzten Kartenvorgangs,

— zur Berechnung der ununterbrochenen Lenkzeit, der kumulativen Unterbrechungszeit und der kumulierten Lenkzeit für die vorangegangene und für die laufende Woche,

— zur Anfertigung von Ausdrucken von auf einer Fahrerkarte aufgezeichneten Daten,

— zum Herunterladen einer Fahrerkarte auf externe Datenträger auslesen können.

Diese Anforderung gilt für Fahrtenschreiberkarten der ersten Generation nur, wenn ihre Verwendung nicht von einer Werkstatt unterdrückt wurde.

135) Bei einem Lesefehler verwendet das Kontrollgerät maximal dreimal erneut den gleichen Lesebefehl. Schlagen alle Versuche fehl, wird die Karte für fehlerhaft und ungültig erklärt.

3.14 **Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten**

3.14.1 *Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten der ersten Generation*

136) Sofern die Verwendung von Fahrtenschreiberkarten der ersten Generation nicht von einer Werkstatt unterdrückt wurde, registriert und speichert das Kontrollgerät Daten in genau der gleichen Weise wie ein Kontrollgerät der ersten Generation.

137) Sofort nach dem Einstecken der Karte stellt das Kontrollgerät die „Kartenvorgangsdaten“ auf der Fahrer- oder Werkstattkarte ein.

138) Das Kontrollgerät aktualisiert die auf gültigen Fahrer-, Werkstatt-, Unternehmens- und/oder Kontrollkarten gespeicherten Daten mit sämtlichen erforderlichen Daten, die für den Karteninhaber und für den Zeitraum, in dem die Karte eingesteckt ist, relevant sind. Die auf diesen Karten gespeicherten Daten sind in Kapitel 4 spezifiziert.

139) Das Kontrollgerät aktualisiert die auf gültigen Fahrer- und Werkstattkarten gespeicherten Fahrertätigkeits- und Ortsdaten (gemäß den Kapiteln 4.5.3.1.9 und 4.5.3.1.11) mit Tätigkeits- und Ortsdaten, die vom Karteninhaber manuell eingegeben werden.

140) Alle Ereignisse, die für Kontrollgeräte der ersten Generation nicht definiert sind, werden nicht auf der Fahrer- und der Werkstattkarte gespeichert.

141) Die Aktualisierung der Fahrtenschreiberkarten erfolgt so, dass bei Bedarf und unter Berücksichtigung der Speicherkapazität der Karte die jeweils ältesten Daten durch die jüngsten Daten ersetzt werden.

142) Bei einem Schreibfehler verwendet das Kontrollgerät maximal dreimal erneut den gleichen Schreibbefehl. Schlagen alle Versuche fehl, wird die Karte für fehlerhaft und ungültig erklärt.

143) Vor der Entnahme einer Fahrerkarte und nach Speicherung aller relevanten Daten auf der Karte setzt das Kontrollgerät alle „Kartenvorgangsdaten“ zurück.

3.14.2 *Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten der zweiten Generation*

144) Fahrtenschreiberkarten der zweiten Generation enthalten 2 verschiedene Kartenanwendungen; bei der ersten handelt es sich um genau dieselbe Anwendung wie die TACHO-Anwendung für Fahrtenschreiberkarten der ersten Generation, bei der zweiten um die „TACHO_G2“-Anwendung, gemäß Kapitel 4 und Anlage 2.

145) Sofort nach dem Einstecken der Karte stellt das Kontrollgerät die „Kartenvorgangsdaten“ auf der Fahrer- oder Werkstattkarte ein.

146) Das Kontrollgerät aktualisiert die auf den beiden Kartenanwendungen gültiger Fahrer-, Werkstatt-, Unternehmens- und/oder Kontrollkarten gespeicherten Daten mit sämtlichen erforderlichen Daten, die für den Karteninhaber und für den Zeitraum, in dem die Karte eingesteckt ist, relevant sind. Die auf diesen Karten gespeicherten Daten sind in Kapitel 4 spezifiziert.

147) Das Kontrollgerät aktualisiert die auf gültigen Fahrer- und Werkstattkarten gespeicherten Fahrertätigkeits-, Orts- und Positionsdaten (gemäß den Kapiteln 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 und 4.5.3.2.11) mit Tätigkeits- und Ortsdaten, die vom Karteninhaber manuell eingegeben werden.

148) Die Aktualisierung der Fahrtenschreiberkarten erfolgt so, dass bei Bedarf und unter Berücksichtigung der Speicherkapazität der Karte die jeweils ältesten Daten durch die jüngsten Daten ersetzt werden.

149) Bei einem Schreibfehler verwendet das Kontrollgerät maximal dreimal erneut den gleichen Schreibbefehl. Schlagen alle Versuche fehl, wird die Karte für fehlerhaft und ungültig erklärt.

150) Vor der Entnahme einer Fahrerkarte und nach Speicherung aller relevanten Daten auf beiden Kartenanwendungen der Karte setzt das Kontrollgerät alle „Kartenvorgangsdaten“ zurück.

3.15 **Anzeige**

151) Die Anzeige enthält mindestens 20 Zeichen.

152) Die Mindesthöhe der Zeichen beträgt 5 mm und die Mindestbreite 3,5 mm.

153) Die Anzeige muss die in Anlage 1 Kapitel 4 „Zeichensätze“ spezifizierten Zeichen unterstützen. Die Anzeige kann vereinfachte Zeichen verwenden (z. B. können mit Akzent versehene Zeichen ohne Akzent oder Kleinbuchstaben als Großbuchstaben dargestellt werden).

154) Die Anzeige ist mit einer blendfreien Beleuchtung auszustatten.

155) Die in der Anzeige dargestellten Zeichen müssen von außerhalb des Kontrollgeräts gut sichtbar sein.

156) Vom Kontrollgerät müssen folgende Daten angezeigt werden können:

— Standarddaten,

— Warndaten,

— Menüzugangsdaten,

— andere von einem Benutzer angeforderte Daten.

Vom Kontrollgerät können zusätzliche Informationen angezeigt werden, sofern sie von den vorstehend verlangten Informationen deutlich unterscheidbar sind.

157) Die Anzeige des Kontrollgeräts verwendet die in Anlage 3 aufgeführten Piktogramme oder Piktogrammkombinationen. Es können auch zusätzliche Piktogramme oder Piktogrammkombinationen angezeigt werden, sofern sie sich deutlich von den genannten Piktogrammen und Piktogrammkombinationen unterscheiden.

158) Die Anzeige muss sich bei fahrendem Fahrzeug stets im eingeschalteten Zustand befinden.

159) Das Kontrollgerät kann eine manuelle oder automatische Abschaltvorrichtung für die Anzeige aufweisen, wenn sich das Fahrzeug nicht in Fahrt befindet.

Das Anzeigeformat ist in Anlage 5 spezifiziert.

3.15.1 *Standardanzeige*

160) Wenn keine anderen Informationen angezeigt werden müssen, sind vom Kontrollgerät standardmäßig folgende Angaben anzuzeigen:

— die Ortszeit (UTC + durch den Fahrer eingestellter Versatz),

— die Betriebsart,

— die derzeitige Tätigkeit des Fahrers und die derzeitige Tätigkeit des Beifahrers,

— Informationen zum Fahrer:

— Falls derzeitige Tätigkeit LENKEN ist: aktuelle ununterbrochene Lenkzeit und aktuelle kumulative Unterbrechungszeit,

— falls derzeitige Tätigkeit nicht LENKEN ist: aktuelle Dauer der anderen Tätigkeit (seit der Auswahl) und aktuelle kumulative Unterbrechungszeit.

161) Die Anzeige von Daten zu den Fahrern muss klar, deutlich und eindeutig sein. Lassen sich Fahrer- und Beifahrerinformationen nicht gleichzeitig anzeigen, zeigt das Kontrollgerät standardmäßig die Informationen zum Fahrer an und ermöglicht dem Benutzer, auf die Anzeige der Informationen zum Beifahrer umzuschalten.

162) Lässt die Anzeigebreite eine ständige Anzeige der Betriebsart nicht zu, zeigt das Kontrollgerät bei Betriebsartwechsel die neue Betriebsart kurz an.

163) Beim Einstecken der Karte wird der Name des Karteninhabers kurz angezeigt.

164) Ist die Bedingung KONTROLLGERÄT NICHT ERFORDERLICH oder FÄHRÜBERFAHRT/ZUGFAHRT eingeschaltet, muss die Standardanzeige das entsprechende Piktogramm aufweisen (es ist zulässig, dass die aktuelle Fahrertätigkeit nicht gleichzeitig angezeigt wird).

3.15.2 *Warnanzeige*

165) Das Kontrollgerät zeigt Warninformationen vorrangig unter Verwendung der Piktogramme gemäß Anlage 3 an, die gegebenenfalls durch zahlencodierte Informationen ergänzt werden. Darüber hinaus kann zusätzlich eine textliche Beschreibung der Warnung in der bevorzugten Sprache des Fahrers erfolgen.

3.15.3 *Menübedienung*

166) Das Kontrollgerät stellt die erforderlichen Befehle über eine geeignete Menüstruktur bereit.

3.15.4 *Sonstige Anzeigen*

167) Nach Bedarf müssen sich folgende Anzeigen auswählen lassen:

— Datum und Uhrzeit in UTC sowie Ortszeitversatz,

— der Inhalt der sechs Ausdrucke in den gleichen Formaten wie die Ausdrucke selbst,

— ununterbrochene Lenkzeit und kumulative Unterbrechungszeit des Fahrers,

— ununterbrochene Lenkzeit und kumulative Unterbrechungszeit des Beifahrers,

— kumulierte Lenkzeit des Fahrers für die Vorwoche und die laufende Woche,

— kumulierte Lenkzeit des Beifahrers für die Vorwoche und die laufende Woche,

optional:

— aktuelle Dauer der Tätigkeit des Beifahrers (seit der Auswahl),

— kumulierte Lenkzeit des Fahrers für die laufende Woche,

— kumulierte Lenkzeit des Beifahrers für den aktuellen Arbeitstag,

— kumulierte Lenkzeit des Fahrers für den aktuellen Arbeitstag.

168) Die Anzeige des Ausdruckinhalts erfolgt sequenziell, Zeile für Zeile. Beträgt die Anzeigebreite weniger als 24 Zeichen, erhält der Benutzer die vollständige Information durch ein geeignetes Mittel (mehrere Zeilen, Rollen usw.).

Für handschriftliche Einträge vorgesehene Ausdruckzeilen brauchen nicht angezeigt zu werden.

3.16 **Drucken**

169) Das Kontrollgerät muss Informationen aus seinem Massenspeicher und/oder von Fahrtenschreiberkarten anhand der folgenden sieben Ausdrucke drucken können:

— täglicher Ausdruck Fahrertätigkeiten von der Karte,

— täglicher Ausdruck Fahrertätigkeiten von der Fahrzeugeinheit,

— Ausdruck Ereignisse und Störungen von der Karte,

— Ausdruck Ereignisse und Störungen von der Fahrzeugeinheit,

— Ausdruck Technische Daten,

— Ausdruck Geschwindigkeitsüberschreitung,

— Fahrtenschreiberkartenvorgänge für eine bestimmte Fahrzeugeinheit (siehe Kapitel 3.12.16)

Genaue Angaben zu Format und Inhalt dieser Ausdrucke sind in Anlage 4 enthalten.

Am Ende der Ausdrucke können zusätzliche Daten bereitgestellt werden.

Vom Kontrollgerät können auch zusätzliche Ausdrucke bereitgestellt werden, sofern sie von den vorgenannten sieben Ausdrucken deutlich unterscheidbar sind.

170) Der „tägliche Ausdruck Fahrertätigkeiten von der Karte“ und der „Ausdruck Ereignisse und Störungen von der Karte“ dürfen verfügbar sein, wenn eine Fahrerkarte oder eine Werkstattkarte in das Kontrollgerät eingesetzt sind. Das Kontrollgerät muss die auf der betreffenden Karte gespeicherten Daten vor Beginn des Ausdrucks aktualisieren.

171) Zur Herstellung des „täglichen Ausdrucks Fahrertätigkeiten von der Karte“ und des „Ausdrucks Ereignisse und Störungen von der Karte“

— wählt das Kontrollgerät entweder automatisch die Fahrerkarte oder die Werkstattkarte, wenn nur eine dieser Karten eingesteckt ist,

— oder ermöglicht einen Befehl zur Auswahl der Quellenkarte oder zur Auswahl der Karte im Fahrersteckplatz, wenn beide Kartenarten im Kontrollgerät eingesteckt sind.

172) Der Drucker muss 24 Zeichen pro Zeile drucken können.

173) Die Mindesthöhe der Zeichen beträgt 2,1 mm und die Mindestbreite 1,5 mm.

174) Der Drucker muss die in Anlage 1 Kapitel 4 „Zeichensätze“ spezifizierten Zeichen unterstützen.

175) Drucker müssen von ihrer Auslegung her diese Ausdrucke mit einem Auflösungsniveau liefern, das Missverständnisse beim Lesen ausschließt.

176) Die Abmessungen der Ausdrucke und die Eintragungen auf den Ausdrucken dürfen unter normalen Feuchtigkeits- (10-90 %) und Temperaturbedingungen keinerlei Veränderungen unterliegen.

177) Auf dem vom Kontrollgerät verwendeten typgenehmigten Papier sind das Typgenehmigungszeichen und der Typ/die Typen des Kontrollgeräts anzugeben, mit dem/denen es eingesetzt werden kann.

178) Die Ausdrucke müssen unter normalen Aufbewahrungsbedingungen hinsichtlich Lichtintensität, Feuchtigkeit und Temperatur mindestens zwei Jahre lang deutlich lesbar und identifizierbar bleiben.

179) Die Ausdrucke müssen mindestens den Prüfspezifikationen gemäß Anlage 9 entsprechen.

180) Es muss möglich sein, auf diesen Ausdrucken zusätzliche manuelle Eintragungen wie die Unterschrift des Fahrers vorzunehmen.

181) Tritt während des Druckens das Ereignis „Kein Papier“ auf, muss das Kontrollgerät nach dem Nachladen des Papiers den Druckvorgang vom Anfang des Ausdrucks starten oder den Druck fortsetzen, wobei ein eindeutiger Hinweis auf den zuvor gedruckten Teil zu erfolgen hat.

3.17 **Warnsignale**

182) Bei Feststellung eines Ereignisses und/oder einer Störung erhält der Fahrer vom Kontrollgerät ein Warnsignal.

183) Das Warnsignal für das Ereignis Unterbrechung der Stromversorgung kann bis zur Wiederherstellung der Stromversorgung aufgeschoben werden.

184) Das Kontrollgerät warnt den Fahrer 15 Minuten vor dem Zeitpunkt sowie zum Zeitpunkt der Überschreitung der höchstzulässigen ununterbrochenen Lenkzeit.

185) Die Warnsignale erfolgen optisch. Zusätzlich zu optischen können auch akustische Warnsignale abgegeben werden.

186) Optische Warnsignale müssen für den Benutzer eindeutig erkennbar sein, sich im Sichtfeld des Fahrers befinden und sowohl am Tage als auch in der Nacht deutlich lesbar sein.

187) Optische Warnsignale können in das Kontrollgerät eingebaut oder gerätefern installiert sein.

188) Im letzteren Fall erfolgt die Kennzeichnung mit einem „T"-Symbol.

189) Die Warnsignale haben eine Dauer von mindestens 30 Sekunden, sofern sie nicht vom Benutzer durch Betätigen einer Taste am Kontrollgerät bestätigt werden. Mit dieser ersten Bestätigung darf die im nächsten Absatz angeführte Anzeige des Grundes für das Warnsignal nicht gelöscht werden.

190) Der Grund für das Warnsignal wird am Kontrollgerät angezeigt und bleibt so lange sichtbar, bis der Benutzer ihn mit einer bestimmten Taste oder mit einem bestimmten Befehl über das Kontrollgerät bestätigt.

191) Es können zusätzliche Warnsignale abgegeben werden, solange sie bei den Fahrern zu keinen Verwechslungen mit den vorstehend festgelegten Warnsignalen führen.

3.18 Herunterladen von Daten auf externe Datenträger

192) Das Kontrollgerät muss bei Bedarf über den Steckanschluss zum Kalibrieren/Herunterladen Daten aus seinem Massenspeicher oder von einer Fahrerkarte an externe Speichermedien herunterladen können. Das Kontrollgerät muss die auf der betreffenden Karte gespeicherten Daten vor Beginn des Herunterladens aktualisieren.

193) Zusätzlich und als optionales Leistungsmerkmal kann das Kontrollgerät in jeder Betriebsart Daten auf anderem Wege an ein auf diesem Weg authentisiertes Unternehmen herunterladen. In diesem Fall gelten für das Herunterladen die Datenzugriffsrechte der Betriebsart Unternehmen.

194) Beim Herunterladen dürfen gespeicherte Daten weder verändert noch gelöscht werden.

195) Die elektrische Schnittstelle des Anschlusses zum Kalibrieren/Herunterladen ist in Anlage 6 spezifiziert.

196) Die Protokolle zum Herunterladen sind in Anlage 7 spezifiziert.

3.19 Fernkommunikation für die Durchführung gezielter Straßenkontrollen

197) Bei eingeschalteter Zündung speichert die Fahrzeugeinheit alle 60 Sekunden in der Fernkommunikationsausrüstung die jüngsten für die Zwecke der gezielten Straßenkontrolle erforderlichen Daten. Diese Daten werden gemäß Anlage 11 und Anlage 14 verschlüsselt und unterzeichnet.

198) Aus der Ferne zu kontrollierende Daten müssen für Fernabfragegeräte durch drahtlose Kommunikation gemäß Anlage 14 verfügbar sein.

199) Daten für die Zwecke der gezielten Straßenkontrolle beziehen sich auf:

— den letzten Versuch einer Sicherheitsverletzung,

— die längste Unterbrechung der Stromversorgung,

— Sensorstörung,

— Datenfehler Weg und Geschwindigkeit,

— Datenkonflikt Fahrzeugbewegung,

— Fahren ohne gültige Karte,

— Einstecken der Karte während des Lenkens,

— Zeiteinstellungsdaten,

— Kalibrierungsdaten einschließlich der Daten der zwei zuletzt gespeicherten Kalibrierungsdatensätze,

— amtliches Kennzeichen des Fahrzeugs,

— vom Fahrtenschreiber aufgezeichnete Geschwindigkeit.

3.20 **Datenausgabe an externe Zusatzgeräte**

200) Das Kontrollgerät kann auch mit genormten Schnittstellen ausgerüstet werden, die in den Betriebsarten Betrieb oder Kalibrierung die Nutzung der vom Fahrtenschreiber aufgezeichneten oder erzeugten Daten durch eine externe Ausrüstung ermöglichen.

In Anlage 13 ist eine optionale ITS-Schnittstelle spezifiziert und genormt. Parallel dazu können ähnliche Schnittstellen bestehen, sofern sie in vollem Umfang den Anforderungen in Bezug auf die in Anlage 13 festgelegte Minimalliste von Daten, die Sicherheit und die Zustimmung des Fahrers genügen.

Folgende Anforderungen gelten für über diese Schnittstelle zur Verfügung gestellte ITS-Daten:

— bei diesen Daten handelt es sich um einen Satz ausgewählter bestehender Daten aus dem Datenglossar des Fahrtenschreibers (Anlage 1),

— ein Teilsatz dieser ausgewählten Daten ist als „personenbezogene Daten" gekennzeichnet,

— der Teilsatz „personenbezogene Daten" ist nur dann verfügbar, wenn die nachweisbare Zustimmung des Fahrers dazu, dass seine persönlichen Daten das Fahrzeugnetzwerk verlassen dürfen, aktiviert ist,

— die Zustimmung des Fahrers kann jederzeit durch Menübefehle aktiviert oder deaktiviert werden, sofern die Fahrerkarte eingesteckt ist,

— der Datensatz und der Datenteilsatz werden über Bluetooth-Funkprotokoll im Umkreis der Fahrerkabine mit einer Aktualisierungsrate von 1 Minute übertragen,

— die Koppelung der ITS-Schnittstelle mit dem externen Gerät wird durch eine spezielle und nach dem Zufallsprinzip erstellte, mindestens 4-stellige PIN geschützt, die in jeder Fahrzeugeinheit gespeichert und über deren Anzeige verfügbar ist,

— durch eine vorhandene ITS-Schnittstelle darf unter keinen Umständen das ordnungsgemäße Funktionieren und die Sicherheit der Fahrzeugeinheit gestört oder beeinträchtigt werden.

Zusätzlich zum Satz ausgewählter vorhandener Daten, der als Minimalliste gilt, können noch weitere Daten ausgegeben werden, sofern sie nicht als personenbezogene Daten gelten können.

Das Kontrollgerät meldet den anderen externen Einrichtungen die Zustimmung des Fahrers.

Bei eingeschalteter Zündung werden diese Daten ständig ausgesendet.

201) Im Hinblick auf die Rückwärtskompatibilität können Fahrtenschreiber weiterhin mit der Schnittstelle für die serielle Verbindung gemäß Anhang 1B der Verordnung (EWG) Nr. 3821/85 in der zuletzt geänderten Fassung ausgerüstet sein. Allerdings ist die Zustimmung des Fahrers weiterhin erforderlich, wenn personenbezogene Daten übermittelt werden.

3.21 **Kalibrierung**

202) Die Kalibrierungsfunktion gestattet folgende Vorgänge:

— automatische Koppelung des Bewegungssensors mit der Fahrzeugeinheit,

— automatische Kopplung der externen GNSS-Ausrüstung mit der Fahrzeugeinheit, falls zutreffend,

— digitale Angleichung der Konstante des Kontrollgeräts (k) an die Wegdrehzahl des Fahrzeugs (w),

— Einstellung der aktuellen Uhrzeit innerhalb der Gültigkeitsdauer der eingesteckten Werkstattkarte,

— Einstellung des aktuellen Kilometerstands,

— Aktualisierung der im Massenspeicher gespeicherten Kenndaten des Bewegungssensors,

— gegebenenfalls Aktualisierung der im Massenspeicher gespeicherten Kenndaten der externen GNSS-Ausrüstung,

— Aktualisierung von Typ und Kennung aller vorhandenen Plombierungen,

— Aktualisierung oder Bestätigung anderer dem Kontrollgerät bekannter Parameter: Fahrzeugkennung, Wegdrehzahl (w), Reifenumgang (l), Reifengröße und gegebenenfalls Einstellung des Geschwindigkeitsbegrenzers.

203) Darüber hinaus ermöglicht es die Kalibrierungsfunktion, die Fähigkeit zur Verwendung von Fahrtenschreiberkarten der ersten Generation im Kontrollgerät zu unterdrücken, sofern die in Anlage 15 festgelegten Bedingungen erfüllt sind.

204) Die Koppelung des Bewegungssensors mit der Fahrzeugeinheit besteht mindestens

— in der Aktualisierung der vom Bewegungssensor gespeicherten Installationsdaten (nach Bedarf),

— im Kopieren erforderlicher Kenndaten des Bewegungssensors von diesem in den Massenspeicher der Fahrzeugeinheit.

205) Die Kopplung der externen GNSS-Ausrüstung mit der Fahrzeugeinheit besteht mindestens

— in der Aktualisierung der von der externen GNSS-Ausrüstung gespeicherten Einbaudaten (nach Bedarf),

— im Kopieren erforderlicher Kenndaten der externen GNSS-Ausrüstung von dieser in den Massenspeicher der Fahrzeugeinheit, einschließlich der Seriennummer der externen GNSS-Ausrüstung.

Nach der Kopplung werden die GNSS-Positionsdaten überprüft.

206) Mit der Kalibrierungsfunktion muss es möglich sein, die erforderlichen Daten über den Anschluss zum Kalibrieren/Herunterladen gemäß dem in Anlage 8 festgelegten Kalibrierungsprotokoll einzugeben. Die Eingabe erforderlicher Daten durch die Kalibrierungsfunktion kann auch auf anderem Wege erfolgen.

3.22 **Straßenseitige Kalibrierungsüberprüfung**

207) Die Funktion straßenseitige Kalibrierungsüberprüfung ermöglicht das Auslesen der Seriennummer des (möglicherweise in den Adapter eingebetteten) Bewegungssensors und der Seriennummer der zum Zeitpunkt der Anforderung mit der Fahrzeugeinheit verbundenen externen GNSS-Ausrüstung (falls zutreffend).

208) Dieses Auslesen muss zumindest auf der Anzeige der Fahrzeugeinheit durch Menübefehle möglich sein.

209) Die Funktion straßenseitige Kalibrierungsüberprüfung ermöglicht ferner die Steuerung der Auswahl der E/A-Betriebsart der Kalibrierungs-E/A-Signalleitung gemäß Anlage 6 über die Schnittstelle der K-Leitung. Dies erfolgt über den Einstellvorgang „ECUAdjustmentSession“ gemäß Anlage 8 Abschnitt 7 „Prüfimpulssteuerung — Funktionseinheit Eingabe/Ausgabe-Steuerung“.

3.23 **Zeiteinstellung**

210) Mit der Funktion Zeiteinstellung ist eine automatische Einstellung der aktuellen Uhrzeit möglich. Im Kontrollgerät werden zwei Zeitquellen zur Zeiteinstellung verwendet: 1) die Systemuhr der Fahrzeugeinheit, 2) der GNSS-Empfänger.

211) Die Zeit der Systemuhr der Fahrzeugeinheit wird automatisch in Abständen von höchstens 12 Stunden neu eingestellt. Wenn diese Frist abgelaufen und kein GNSS-Signal verfügbar ist, erfolgt die Zeiteinstellung, sobald die Fahrzeugeinheit je nach Zustand der Fahrzeugzündung Zugriff auf eine vom GNSS-Empfänger gelieferte gültige Zeit hat. Die Zeitreferenz für die automatische Zeiteinstellung der Systemuhr der Fahrzeugeinheit wird aus dem GNSS-Empfänger abgeleitet. Ein Ereignis Zeitkonflikt wird ausgelöst, wenn die aktuelle Zeit um mehr als eine (1) Minute von der vom GNSS-Empfänger gelieferten Zeitangabe abweicht.

212) In der Betriebsart Kalibrierung ermöglicht es die Funktion Zeiteinstellung ferner, eine Einstellung der aktuellen Uhrzeit auszulösen.

3.24 **Leistungsmerkmale**

213) Die Fahrzeugeinheit muss im Temperaturbereich von – 20 °C bis 70 °C, die externe GNSS-Ausrüstung im Temperaturbereich von – 20 °C bis 70 °C und der Bewegungssensor im Temperaturbereich von – 40 °C bis 135 °C voll einsatzbereit sein; der Inhalt des Massenspeichers muss bis zu Temperaturen von – 40 °C erhalten bleiben.

214) Der Fahrtenschreiber muss bei einer Luftfeuchtigkeit von 10 bis 90 % voll einsatzbereit sein.

215) Die im intelligenten Fahrtenschreiber verwendeten Plombierungen müssen den gleichen Bedingungen standhalten wie sie für die Komponenten des Fahrtenschreibers, an denen sie angebracht sind, gelten.

216) Das Kontrollgerät muss gegen Überspannung, Falschpolung der Stromversorgung und Kurzschluss geschützt sein.

217) Bewegungssensoren müssen entweder

— auf ein Magnetfeld, das die Ermittlung von Fahrzeugbewegungsdaten stört, reagieren — unter diesen Umständen registriert und speichert die Fahrzeugeinheit eine Sensorstörung (Randnummer 88) — oder

— über einen Sensor verfügen, der vor Magnetfeldern geschützt oder dagegen unempfindlich ist.

218) Das Kontrollgerät und die externe GNSS-Ausrüstung müssen der internationalen UN/ECE-Regelung Nr. 10 genügen und gegen elektrostatische Entladungen und Störgrößen geschützt sein.

3.25 **Werkstoffe**

219) Alle Bauteile des Kontrollgeräts müssen aus Werkstoffen mit hinreichender Stabilität und mechanischer Festigkeit sowie genügender elektrischer und magnetischer Unveränderlichkeit bestehen.

220) Zur Gewährleistung normaler Betriebsbedingungen müssen alle Teile des Geräts gegen Feuchtigkeit und Staub geschützt sein.

221) Die Fahrzeugeinheit und die externe GNSS-Ausrüstung müssen den Schutzgrad IP 40 und der Bewegungssensor muss den Schutzgrad IP 64 gemäß Norm IEC 60529:1989 einschließlich A1:1999 und A2:2013 erfüllen.

222) Das Kontrollgerät muss den geltenden technischen Spezifikationen hinsichtlich der ergonomischen Gestaltung genügen.

223) Das Kontrollgerät muss gegen unbeabsichtigte Beschädigungen geschützt sein.

3.26 **Markierungen**

224) Sind am Kontrollgerät Kilometerstand und Geschwindigkeit ablesbar, müssen in der Anzeige folgende Angaben erscheinen:

— in der Nähe der Zahl, die die zurückgelegte Wegstrecke anzeigt, die Maßeinheit der zurückgelegten Wegstrecken mit der Abkürzung „km“,

— in der Nähe der Zahl, die die Geschwindigkeit anzeigt, die Abkürzung „km/h“.

Das Kontrollgerät kann auch auf eine Geschwindigkeitsanzeige in Meilen pro Stunde umgeschaltet werden; in diesem Fall wird als Maßeinheit der Geschwindigkeit die Abkürzung „mph“ angezeigt. Das Kontrollgerät kann auch auf eine Anzeige der zurückgelegten Wegstrecke in Meilen umgeschaltet werden; in diesem Fall wird als Maßeinheit der zurückgelegten Wegstrecke die Abkürzung „mi“ angezeigt.

225) An jeder gesonderten Komponente des Kontrollgeräts ist ein Typenschild mit folgenden Angaben anzubringen:

— Name und Anschrift des Geräteherstellers,

— Teilnummer und Baujahr,

— Seriennummer des Geräts,

— Prüfzeichen des Kontrollgerätetyps.

226) Reicht der Platz nicht für alle vorstehend genannten Angaben aus, muss das Typenschild mindestens folgende Angaben enthalten: Name oder Logo des Herstellers und Nummer des Kontrollgeräteteils.

4 BAUART- UND FUNKTIONSMERKMALE DER FAHRTENSCHREIBERKARTEN

4.1 **Sichtbare Daten**

Die Vorderseite enthält:

227) je nach Kartentyp in Großbuchstaben die Wörter „Fahrerkarte“ oder „Kontrollkarte“ oder „Werkstattkarte“ oder „Unternehmenskarte“ in der Sprache bzw. den Sprachen des ausstellenden Mitgliedstaats;

228) den Namen des Mitgliedstaats, der die Karte ausstellt (optional);

229) das Unterscheidungszeichen des ausstellenden Mitgliedstaats, im Negativdruck in einem blauen Rechteck, umgeben von 12 gelben Sternen. Die Unterscheidungszeichen lauten wie folgt:

B	Belgien	LV	Lettland
BG	Bulgarien	L	Luxemburg
CZ	Tschechische Republik	LT	Litauen
CY	Zypern	M	Malta
DK	Dänemark	NL	Niederlande

D EST	Deutschland Estland	A PL	Österreich Polen
GR	Griechenland	P RO SK SLO	Portugal Rumänien Slowakei Slowenien
E	Spanien	FIN	Finnland
F HR H	Frankreich Kroatien Ungarn	S	Schweden
IRL	Irland	UK	Vereinigtes Königreich
I	Italien		

230) wie folgt nummerierte Angaben zu der ausgestellten Karte:

	Fahrerkarte	Kontrollkarte	Unternehmens- oder Werkstattkarte
1.	Name des Fahrers	Name der Kontrollstelle	Name des Unternehmens oder der Werkstatt
2.	Vorname(n) des Fahrers	Name des Kontrolleurs (falls zutreffend)	Name des Karteninhabers (falls zutreffend)
3.	Geburtsdatum des Fahrers	Vorname(n) des Kontrolleurs (falls zutreffend)	Vorname(n) des Karteninhabers (falls zutreffend)
4.a	Gültig ab		
4.b	Gültig bis		
4.c	Name der ausstellenden Behörde (kann auch auf die Rückseite gedruckt werden)		
4.d	andere Nummer als unter 5 für Verwaltungszwecke (optional)		
5.a	Führerscheinnummer: (am Ausstellungstag der Fahrerkarte)	—	—
5.b	Kartennummer		
6.	Lichtbild des Fahrers	Lichtbild des Kontrolleurs (optional)	Lichtbild des Einbaubetriebs (optional)

	Fahrerkarte	Kontrollkarte	Unternehmens- oder Werkstattkarte
7.	Unterschrift des Inhabers (optional)		
8.	Wohnort oder Anschrift des Inhabers (optional)	Anschrift der Kontrollstelle	Anschrift des Unternehmens oder der Werkstatt

231) Das zu verwendende Datumsformat ist „TT/MM/JJJJ“ oder „TT.MM.JJJJ“ (Tag, Monat, Jahr).

Die Rückseite enthält:

232) eine Erläuterung zu den nummerierten Angaben auf der Vorderseite der Karte,

233) mit ausdrücklicher schriftlicher Zustimmung des Inhabers auch Angaben, die nicht mit der Verwaltung der Fahrerkarte im Zusammenhang stehen; durch derartige Zusätze ändert sich nichts an der Verwendung des Musters als Fahrerkarte.

234) Die Fahrtenschreiberkarten werden mit folgenden Hintergrundfarben gedruckt:

— Fahrerkarte: Weiß,

— Kontrollkarte: Blau,

— Werkstattkarte: Rot,

— Unternehmenskarte: Gelb.

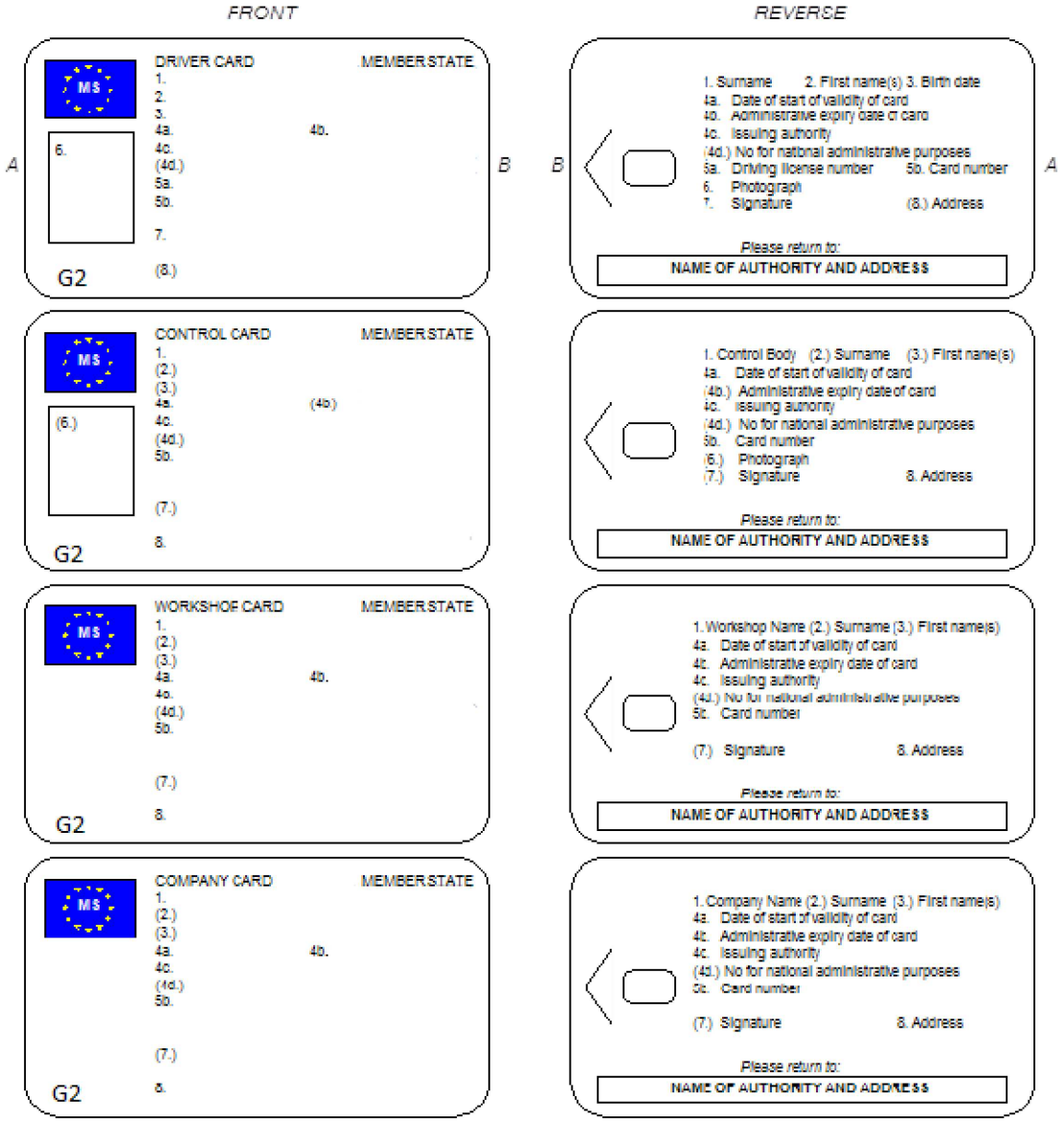
235) Zum Schutz vor Fälschung und unbefugten Änderungen weisen die Fahrtenschreiberkarten mindestens folgende Merkmale auf:

— ein Sicherheitsuntergrunddesign mit feinen Guillochen und Irisdruck,

— im Bereich des Lichtbilds eine Überlappung des Sicherheitsuntergrunddesigns mit dem Lichtbild,

— mindestens eine zweifarbige Mikrodruckzeile.

COMMUNITY MODEL TACHOGRAPH CARDS



236) Die Mitgliedstaaten können nach Beratung mit der Kommission unbeschadet der übrigen Bestimmungen dieses Anhangs Farben oder Markierungen wie Staatssymbole oder Sicherheitsmerkmale hinzufügen.

237) Befristete Karten nach Artikel 26 Absatz 4 der Verordnung (EU) Nr. 165/2014 müssen den Vorschriften dieses Anhangs entsprechen.

4.2 Sicherheit

Ziel der Systemsicherheit ist der Schutz der Integrität und Authentizität der zwischen den Karten und dem Kontrollgerät ausgetauschten Daten und der von den Karten heruntergeladenen Daten, die Zulassung bestimmter Schreibvorgänge auf die Karten nur für das Kontrollgerät, die Entschlüsselung bestimmter Daten, der Ausschluss jeder Möglichkeit einer Fälschung der auf den Karten gespeicherten Daten, die Verhinderung unbefugter Änderungen sowie die Feststellung jeglicher Versuche dieser Art.

238) Zur Gewährleistung der Systemsicherheit müssen die Fahrtenschreiberkarten die Sicherheitsvorgaben gemäß den Anlagen 10 und 11 erfüllen.

239) Fahrtenschreiberkarten müssen mit anderen Geräten, wie z. B. Personalcomputern, lesbar sein.

4.3 **Normen**

240) Die Fahrtenschreiberkarten müssen den folgenden Normen entsprechen:

— ISO/IEC 7810 Identification cards — Physical characteristics,

— ISO/IEC 7816 Identification cards — Integrated circuit cards:

— Teil 1: Physical characteristics,

— Teil 2: Dimensions and position of the contacts (ISO/IEC 7816-2:2007),

— Teil 3: Electrical interface and transmission protocols (ISO/IEC 7816-3:2006),

— Teil 4: Organization, security and commands for interchange)(ISO/IEC 7816-4:2013 + Cor 1:2014),

— Teil 6: Interindustry data elements for interchange (ISO/IEC 7816-6:2004 + Cor 1:2006),

— Teil 8: Commands for security operations (ISO/IEC 7816-8:2004).

— Fahrtenschreiberkarten müssen gemäß ISO/IEC 10373-3:2010 „Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices“ geprüft werden.

4.4 **Spezifikationen für Umgebung und Elektrizität**

241) Fahrtenschreiberkarten müssen unter allen klimatischen Bedingungen, die im Gebiet der Gemeinschaft gewöhnlich anzutreffen sind, ordnungsgemäß funktionieren können, mindestens im Temperaturbereich – 25 °C bis + 70 °C mit gelegentlichen Spitzen bis zu + 85 °C, wobei „gelegentlich“ jeweils nicht mehr als 4 Stunden und nicht mehr als 100mal während der Lebensdauer der Karte bedeutet.

242) Fahrtenschreiberkarten müssen bei einer Luftfeuchtigkeit von 10 bis 90 % ordnungsgemäß funktionieren können.

243) Fahrtenschreiberkarten müssen bei Verwendung gemäß den Spezifikationen für Umgebung und Elektrizität während einer Dauer von fünf Jahren ordnungsgemäß funktionieren können.

244) Während des Betriebs müssen die Fahrtenschreiberkarten hinsichtlich der elektromagnetischen Verträglichkeit der UN/ECE-Regelung Nr. 10 genügen und gegen elektrostatische Entladungen geschützt sein.

4.5 **Datenspeicherung**

Im Sinne dieses Absatzes

— erfolgt die Zeitaufzeichnung auf eine Minute genau, sofern nicht anders angegeben;

— erfolgt die Aufzeichnung des Kilometerstands auf einen Kilometer genau;

— erfolgt die Geschwindigkeitsaufzeichnung auf 1 km/h genau;

— werden Positionen (Längen- und Breitengrade) in Grad und Minuten mit einer Auflösung von 1/10 Minute aufgezeichnet.

Die Funktionen, Befehle und logischen Strukturen der Fahrtenschreiberkarten, die der Erfüllung von Anforderungen zur Datenspeicherung dienen, sind in Anlage 2 spezifiziert.

Sofern nicht anders angegeben muss die Datenspeicherung auf Fahrtenschreiberkarten so erfolgen, dass die jeweils ältesten gespeicherten Daten durch neue Daten ersetzt werden, wenn die für diese Aufzeichnungen vorgesehene Speichergröße erschöpft ist.

245) In diesem Absatz ist die Mindestspeicherkapazität für die verschiedenen Anwendungsdateien festgelegt. Fahrtenschreiberkarten müssen dem Kontrollgerät die tatsächliche Speicherkapazität dieser Dateien anzeigen können.

246) Alle zusätzlichen auf Fahrtenschreiberkarten gespeicherten Daten in Bezug auf andere Anwendungen, für die die Karte möglicherweise vorgesehen ist, müssen in Übereinstimmung mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates und im Einklang mit Artikel 7 der Verordnung (EU) Nr. 165/2014 gespeichert werden.

247) Jede Wurzel-DF (Master File, MF) einer Fahrtenschreiberkarte enthält bis zu fünf Elementardateien (Elementary Files, EF) für die Kartenverwaltung, Anwendungs- und Chipkennungen sowie zwei Verzeichnisse (Dedicated Files, DF):

— DF Tachograph enthält die für Fahrzeugeinheiten der ersten Generation zugängliche Anwendung, die auch in Fahrtenschreiberkarten der ersten Generation enthalten ist,

— DF Tachograph_G2 enthält die nur für Fahrzeugeinheiten der zweiten Generation zugängliche Anwendung, die nur in Fahrtenschreiberkarten der zweiten Generation enthalten ist.

Sämtliche Einzelheiten der Struktur der Fahrtenschreiberkarten sind in Anlage 2 spezifiziert.

4.5.1 *Elementardateien für Kennung und Kartenverwaltung*

4.5.2 *IS-Kartenkennung*

248) Die Fahrtenschreiberkarten müssen die folgenden Chipkartenkenndaten speichern können:

— Clock stop,

— Seriennummer der Karte (einschließlich Fertigungsangaben),

— Typgenehmigungsnummer der Karte

— Kennung der Karten-Personalisierung (ID),

— Kartenhersteller-ID,

— IS-Bezeichner.

4.5.2.1 Chipkennung

249) Die Fahrtenschreiberkarten müssen die folgenden Kenndaten des integrierten Schaltkreises (IS) speichern können:

— IS-Seriennummer,

— IS-Fertigungsangaben.

4.5.2.2 DIR (nur in Fahrtenschreiberkarten der zweiten Generation enthalten)

250) Fahrtenschreiberkarten müssen die in Anlage 2 genannten Datenobjekte zur Anwendungskennung speichern können.

4.5.2.3 ATR-Angaben (eingeschränkt, nur in Fahrtenschreiberkarten der zweiten Generation enthalten)

251) Die Fahrtenschreiberkarten müssen das folgende Datenobjekt mit der erweiterten Längenangabe speichern können:

— falls die Fahrtenschreiberkarte erweiterte Längenfelder unterstützt, das in Anlage 2 spezifizierte Datenobjekt mit der erweiterten Längenangabe.

4.5.2.4 Erweiterte Längenangabe (eingeschränkt, nur in Fahrtenschreiberkarten der zweiten Generation enthalten)

252) Die Fahrtenschreiberkarten müssen die folgenden Datenobjekte mit der erweiterten Längenangabe speichern können:

— falls die Fahrtenschreiberkarte erweiterte Längenfelder unterstützt, die in Anlage 2 spezifizierten Datenobjekte mit der erweiterten Längenangabe.

4.5.3 *Fahrerkarte*

4.5.3.1 Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation)

4.5.3.1.1 Anwendungskennung

253) Die Fahrerkarte muss die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.3.1.2 Schlüssel und Zertifikate

254) Die Fahrtenschreiberkarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil A speichern können.

4.5.3.1.3 Kartenkennung

255) Die Fahrerkarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis.

4.5.3.1.4 Karteninhaberkennung

256) Die Fahrerkarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name des Karteninhabers,

— Vorname(n) des Karteninhabers,

— Geburtsdatum,

— bevorzugte Sprache.

4.5.3.1.5 Herunterladen von der Karte

257) Die Fahrerkarte muss in Bezug auf das Herunterladen von der Karte die folgenden Daten speichern können:

— Datum und Uhrzeit des letzten Herunterladens der Daten von der Karte (zu anderen als Kontrollzwecken).

258) Die Fahrerkarte muss einen derartigen Datensatz gespeichert halten können.

4.5.3.1.6 Führerscheininformationen

259) Die Fahrerkarte muss die folgenden Führerscheindaten speichern können:

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde,

— Führerscheinnummer (am Ausstellungstag der Karte).

4.5.3.1.7 Ereignisdaten

Im Sinne dieses Absatzes erfolgt die Zeitspeicherung auf 1 Sekunde genau.

260) Die Fahrerkarte muss Daten in Bezug auf die folgenden, vom Kontrollgerät bei eingesteckter Karte festgestellten Ereignisse speichern können:

— Zeitüberlappung (wenn die Karte Ursache des Ereignisses ist),

— Einstecken der Karte während des Lenkens (wenn die Karte Gegenstand des Ereignisses ist),

— Letzter Kartenvorgang nicht korrekt abgeschlossen (wenn die Karte Gegenstand des Ereignisses ist),

— Unterbrechung der Stromversorgung,

— Datenfehler Weg und Geschwindigkeit,

— Versuch Sicherheitsverletzung.

261) Die Fahrerkarte muss die folgenden Daten für diese Ereignisse speichern können:

— Ereigniscode,

— Datum und Uhrzeit des Ereignisbeginns (oder des Einsteckens der Karte, wenn das Ereignis zu diesem Zeitpunkt andauerte),

— Datum und Uhrzeit des Ereignisendes (oder der Kartenentnahme, wenn das Ereignis zu diesem Zeitpunkt andauerte),

— amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem das Ereignis eintrat.

Anmerkung: Für das Ereignis „Zeitüberlappung“:

— Datum und Uhrzeit des Ereignisbeginns müssen Datum und Uhrzeit der Kartenentnahme aus dem vorherigen Fahrzeug entsprechen,

— Datum und Uhrzeit des Ereignisendes müssen Datum und Uhrzeit des Einsteckens der Karte in das derzeitige Fahrzeug entsprechen,

— Fahrzeugdaten müssen dem derzeitigen Fahrzeug entsprechen, das das Ereignis auslöst.

Anmerkung: Für das Ereignis „Letzter Kartenvorgang nicht korrekt abgeschlossen“:

— Datum und Uhrzeit des Ereignisbeginns müssen Datum und Uhrzeit des Einsteckens der Karte bei dem nicht korrekt abgeschlossenen Vorgang entsprechen,

— Datum und Uhrzeit des Ereignisendes müssen Datum und Uhrzeit des Einsteckens der Karte bei dem Vorgang entsprechen, während dessen das Ereignis festgestellt wurde (derzeitiger Vorgang),

— Fahrzeugdaten müssen dem Fahrzeug entsprechen, in dem der Vorgang nicht korrekt abgeschlossen wurde.

262) Die Fahrerkarte muss Daten für die sechs jüngsten Ereignisse jeder Art (d. h. 36 Ereignisse) speichern können.

4.5.3.1.8 Störungsdaten

Im Sinne dieses Unterabsatzes erfolgt die Zeitspeicherung auf 1 Sekunde genau.

263) Die Fahrerkarte muss Daten in Bezug auf die folgenden, vom Kontrollgerät bei eingesteckter Karte festgestellten Störungen speichern können:

— Störung Karte (wenn die Karte Gegenstand des Ereignisses ist),

— Störung Kontrollgerät.

264) Die Fahrerkarte muss die folgenden Daten für diese Störungen speichern können:

— Störungscode,

— Datum und Uhrzeit des Störungsbeginns (oder des Einsteckens der Karte, wenn die Störung zu diesem Zeitpunkt andauerte),

— Datum und Uhrzeit des Störungsendes (oder der Kartenentnahme, wenn die Störung zu diesem Zeitpunkt andauerte),

— amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Störung eintrat.

265) Die Fahrerkarte muss Daten für die zwölf jüngsten Störungen jeder Art (d. h. 24 Störungen) speichern können.

4.5.3.1.9 Fahrertätigkeitsdaten

266) Die Fahrerkarte muss für jeden Kalendertag, an dem sie benutzt wurde oder für den der Fahrer manuell Tätigkeiten eingegeben hat, die folgenden Daten speichern können:

— Datum,

— Tagesanwesenheitszähler (wird für jeden dieser Kalendertage um den Wert Eins erhöht),

— vom Fahrer an diesem Tag zurückgelegte Gesamtwegstrecke,

— Fahrerstatus um 0.00 Uhr,

— jedes Mal, wenn der Fahrer die Tätigkeit gewechselt und/oder den Status der Fahrzeugführung verändert und/oder seine Karte eingesteckt oder entnommen hat:

— der Status der Fahrzeugführung (TEAM, EINMANNBETRIEB),

— den Steckplatz (FAHRER, BEIFAHRER),

— den Kartenstatus (EINGESTECKT, NICHT EINGESTECKT),

— die Tätigkeit (LENKEN, BEREITSCHAFT, ARBEIT, UNTERBRECHUNG/RUHE),

— den Zeitpunkt der Veränderung.

267) Der Speicher der Fahrerkarte muss die Fahrertätigkeitsdaten von mindestens 28 Tagen gespeichert halten können (die durchschnittliche Tätigkeit eines Fahrers ist mit 93 Tätigkeitsveränderungen pro Tag definiert).

268) Die in den Randnummern 261, 264 und 266 aufgeführten Daten werden so gespeichert, dass — auch bei zeitlichen Überschneidungen — ein Abrufen der Tätigkeiten in der Reihenfolge ihres Auftretens möglich ist.

4.5.3.1.10 Daten zu gefahrenen Fahrzeugen

269) Die Fahrerkarte muss für jeden Kalendertag, an dem die sie benutzt wurde, sowie für jeden Betriebszeitraum eines Fahrzeugs an diesem Tag (ein Betriebszeitraum umfasst alle aufeinander folgenden Einsteck-/Entnahmevorgänge der Karte in dem Fahrzeug im Hinblick auf diese Karte) die folgenden Daten speichern können:

— Datum und Uhrzeit des ersten Einsatzes des Fahrzeugs (d. h. erstes Karteneinstecken für diesen Betriebszeitraum des Fahrzeugs oder 0.00 Uhr, wenn der Betriebszeitraum zu diesem Zeitpunkt andauert),

— Kilometerstand zu diesem Zeitpunkt,

— Datum und Uhrzeit des letzten Einsatzes des Fahrzeugs (d. h. letzte Kartenentnahme für diesen Betriebszeitraum des Fahrzeugs oder 23.59 Uhr, wenn der Betriebszeitraum zu diesem Zeitpunkt andauert),

— Kilometerstand zu diesem Zeitpunkt,

— amtliches Kennzeichen und zulassender Mitgliedstaat.

270) Die Fahrerkarte muss mindestens 84 derartige Datensätze speichern können.

4.5.3.1.11 Ort des Beginns und/oder des Endes des Arbeitstages

271) Die Fahrerkarte muss die folgenden vom Fahrer eingegebenen Daten zum Ort des Beginns und/oder des Endes des Arbeitstages speichern können:

— Datum und Uhrzeit der Eingabe (oder Datum/Uhrzeit bezogen auf die Eingabe, wenn diese während des manuellen Eingabevorgangs erfolgt),

— Art der Eingabe (Beginn oder Ende, Eingabebedingung),

— eingegebene(s) Land und Region,

— Kilometerstand.

272) Der Speicher der Fahrerkarte muss mindestens 42 derartige Datensatzpaare gespeichert halten können.

4.5.3.1.12 Kartenvorgangsdaten

273) Die Fahrerkarte muss Daten in Bezug auf das Fahrzeug speichern können, in dem der laufende Vorgang eingeleitet wurde:

— Datum und Uhrzeit der Einleitung des Vorgangs (d. h. Einstecken der Karte) auf 1 Sekunde genau,

— amtliches Kennzeichen und zulassender Mitgliedstaat.

4.5.3.1.13 Kontrolltätigkeitsdaten

274) Die Fahrerkarte muss in Bezug auf Kontrolltätigkeiten die folgenden Daten speichern können:

— Datum und Uhrzeit der Kontrolle,

— Kontrollkartennummer und ausstellender Mitgliedstaat,

— Art der Kontrolle (Anzeige und/oder Drucken und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte (siehe Anmerkung)),

— heruntergeladener Zeitraum beim Herunterladen,

— amtliches Kennzeichen und zulassender Mitgliedstaat des kontrollierten Fahrzeugs.

Anmerkung: Ein Herunterladen von der Karte wird nur aufgezeichnet, wenn dies über ein Kontrollgerät erfolgt.

275) Die Fahrerkarte muss einen derartigen Datensatz gespeichert halten können.

4.5.3.1.14 Daten zu spezifischen Bedingungen

276) Die Fahrerkarte muss die folgenden Daten in Bezug auf spezifische Bedingungen speichern können, die bei eingesetzter Karte (ungeachtet des Steckplatzes) eingegeben wurden:

— Datum und Uhrzeit der Eingabe,

— Art der spezifischen Bedingung.

277) Die Fahrerkarte muss mindestens 56 derartige Datensätze speichern können.

4.5.3.2 Fahrtenschreiberanwendung der zweiten Generation (für Fahrzeugeinheiten der ersten Generation nicht zugänglich)

4.5.3.2.1 Anwendungskennung

278) Die Fahrerkarte muss die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.3.2.2 Schlüssel und Zertifikate

279) Die Fahrtenschreiberkarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil B speichern können.

4.5.3.2.3 Kartenkennung

280) Die Fahrerkarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis.

4.5.3.2.4 Karteninhaberkennung

281) Die Fahrerkarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name des Karteninhabers,

— Vorname(n) des Karteninhabers,

— Geburtsdatum,

— bevorzugte Sprache.

4.5.3.2.5 Herunterladen von der Karte

282) Die Fahrerkarte muss in Bezug auf das Herunterladen von der Karte die folgenden Daten speichern können:

— Datum und Uhrzeit des letzten Herunterladens der Daten von der Karte (zu anderen als Kontrollzwecken).

283) Die Fahrerkarte muss einen derartigen Datensatz gespeichert halten können.

4.5.3.2.6 Führerscheininformationen

284) Die Fahrerkarte muss die folgenden Führerscheindaten speichern können:

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde,

— Führerscheinnummer (am Ausstellungstag der Karte).

4.5.3.2.7 Ereignisdaten

Im Sinne dieses Absatzes erfolgt die Zeitspeicherung auf 1 Sekunde genau.

285) Die Fahrerkarte muss Daten in Bezug auf die folgenden, vom Kontrollgerät bei eingesteckter Karte festgestellten Ereignisse speichern können:

— Zeitüberlappung (wenn die Karte Ursache des Ereignisses ist),

— Einstecken der Karte während des Lenkens (wenn die Karte Gegenstand des Ereignisses ist),

— Letzter Kartenvorgang nicht korrekt abgeschlossen (wenn die Karte Gegenstand des Ereignisses ist),

— Unterbrechung der Stromversorgung,

— Kommunikationsfehler mit der Fernkommunikationsausrüstung,

— Ereignis „Fehlen der Positionsdaten vom GNSS-Empfänger“,

— Ereignis „Kommunikationsfehler mit der externen GNSS-Ausrüstung“

— Datenfehler Weg und Geschwindigkeit,

— Datenkonflikt Fahrzeugbewegung,

— Versuch Sicherheitsverletzung,

— Zeitkonflikt.

286) Die Fahrerkarte muss die folgenden Daten für diese Ereignisse speichern können:

— Ereigniscode,

— Datum und Uhrzeit des Ereignisbeginns (oder des Einsteckens der Karte, wenn das Ereignis zu diesem Zeitpunkt andauerte),

— Datum und Uhrzeit des Ereignisendes (oder der Kartenentnahme, wenn das Ereignis zu diesem Zeitpunkt andauerte),

— amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem das Ereignis eintrat.

Anmerkung: Für das Ereignis „Zeitüberlappung“:

— Datum und Uhrzeit des Ereignisbeginns müssen Datum und Uhrzeit der Kartenentnahme aus dem vorherigen Fahrzeug entsprechen,

— Datum und Uhrzeit des Ereignisendes müssen Datum und Uhrzeit des Einsteckens der Karte in das derzeitige Fahrzeug entsprechen,

— Fahrzeugdaten müssen dem derzeitigen Fahrzeug entsprechen, das das Ereignis auslöst.

Anmerkung: Für das Ereignis „Letzter Kartenvorgang nicht korrekt abgeschlossen“:

— Datum und Uhrzeit des Ereignisbeginns müssen Datum und Uhrzeit des Einsteckens der Karte bei dem nicht korrekt abgeschlossenen Vorgang entsprechen,

— Datum und Uhrzeit des Ereignisendes müssen Datum und Uhrzeit des Einsteckens der Karte bei dem Vorgang entsprechen, während dessen das Ereignis festgestellt wurde (derzeitiger Vorgang),

— Fahrzeugdaten müssen dem Fahrzeug entsprechen, in dem der Vorgang nicht korrekt abgeschlossen wurde.

287) Die Fahrerkarte muss Daten für die sechs jüngsten Ereignisse jeder Art (d. h. 66 Ereignisse) speichern können.

4.5.3.2.8 Störungsdaten

Im Sinne dieses Unterabsatzes erfolgt die Zeitspeicherung auf 1 Sekunde genau.

288) Die Fahrerkarte muss Daten in Bezug auf die folgenden, vom Kontrollgerät bei eingesteckter Karte festgestellten Störungen speichern können:

— Störung Karte (wenn die Karte Gegenstand des Ereignisses ist),

— Störung Kontrollgerät.

289) Die Fahrerkarte muss die folgenden Daten für diese Störungen speichern können:

— Störungscode,

— Datum und Uhrzeit des Störungsbeginns (oder des Einsteckens der Karte, wenn die Störung zu diesem Zeitpunkt andauerte),

— Datum und Uhrzeit des Störungsendes (oder der Kartenentnahme, wenn die Störung zu diesem Zeitpunkt andauerte),

— amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Störung eintrat.

290) Die Fahrerkarte muss Daten für die zwölf jüngsten Störungen jeder Art (d. h. 24 Störungen) speichern können.

4.5.3.2.9 Fahrertätigkeitsdaten

291) Die Fahrerkarte muss für jeden Kalendertag, an dem sie benutzt wurde oder für den der Fahrer manuell Tätigkeiten eingegeben hat, die folgenden Daten speichern können:

— Datum,

— Tagesanwesenheitszähler (wird für jeden dieser Kalendertage um den Wert Eins erhöht),

— vom Fahrer an diesem Tag zurückgelegte Gesamtwegstrecke,

— Fahrerstatus um 0.00 Uhr,

— jedes Mal, wenn der Fahrer die Tätigkeit gewechselt und/oder den Status der Fahrzeugführung verändert und/oder seine Karte eingesteckt oder entnommen hat:

— den Status der Fahrzeugführung (TEAM, EINMANNBETRIEB),

— den Steckplatz (FAHRER, BEIFAHRER),

— den Kartenstatus (EINGESTECKT, NICHT EINGESTECKT),

— die Tätigkeit (LENKEN, BEREITSCHAFT, ARBEIT, UNTERBRECHUNG/RUHE).

— Zeitpunkt der Veränderung.

292) Der Speicher der Fahrerkarte muss die Fahrertätigkeitsdaten von mindestens 28 Tagen gespeichert halten können (die durchschnittliche Tätigkeit eines Fahrers ist mit 93 Tätigkeitsveränderungen pro Tag definiert).

293) Die in den Randnummern 286, 289 und 291 aufgeführten Daten werden so gespeichert, dass — auch bei zeitlichen Überschneidungen — ein Abrufen der Tätigkeiten in der Reihenfolge ihres Auftretens möglich ist.

4.5.3.2.10 Daten zu gefahrenen Fahrzeugen

294) Die Fahrerkarte muss für jeden Kalendertag, an dem die sie benutzt wurde, sowie für jeden Betriebszeitraum eines Fahrzeugs an diesem Tag (ein Betriebszeitraum umfasst alle aufeinander folgenden Einsteck-/Entnahmevorgänge der Karte in dem Fahrzeug im Hinblick auf diese Karte) die folgenden Daten speichern können:

— Datum und Uhrzeit des ersten Einsatzes des Fahrzeugs (d. h. erstes Karteneinstecken für diesen Betriebszeitraum des Fahrzeugs oder 0,00 Uhr, wenn der Betriebszeitraum zu diesem Zeitpunkt andauert),

— Kilometerstand zu diesem Zeitpunkt des ersten Einsatzes,

— Datum und Uhrzeit des letzten Einsatzes des Fahrzeugs (d. h. letzte Kartenentnahme für diesen Betriebszeitraum des Fahrzeugs oder 23,59 Uhr, wenn der Betriebszeitraum zu diesem Zeitpunkt andauert),

— Kilometerstand zu diesem Zeitpunkt des letzten Einsatzes,

— amtliches Kennzeichen und zulassender Mitgliedstaat,

— Fahrzeug-Identifizierungsnummer.

295) Die Fahrerkarte muss mindestens 84 derartige Datensätze speichern können.

4.5.3.2.11 Ort und Position des Beginns und/oder des Endes des Arbeitstages

296) Die Fahrerkarte muss die folgenden vom Fahrer eingegebenen Daten zum Ort des Beginns und/oder des Endes des Arbeitstages speichern können:

— Datum und Uhrzeit der Eingabe (oder Datum/Uhrzeit bezogen auf die Eingabe, wenn diese während des manuellen Eingabevorgangs erfolgt),

— Art der Eingabe (Beginn oder Ende, Eingabebedingung),

— eingegebene(s) Land und Region,

— Kilometerstand,

— Position des Fahrzeugs,

— GNSS-Genauigkeit, Datum und Uhrzeit der Feststellung der Position.

297) Der Speicher der Fahrerkarte muss mindestens 84 derartige Datensatzpaare gespeichert halten können.

4.5.3.2.12 Kartenvorgangsdaten

298) Die Fahrerkarte muss Daten in Bezug auf das Fahrzeug speichern können, in dem der laufende Vorgang eingeleitet wurde:

— Datum und Uhrzeit der Einleitung des Vorgangs (d. h. Einstecken der Karte) auf 1 Sekunde genau,

— amtliches Kennzeichen und zulassender Mitgliedstaat.

4.5.3.2.13 Kontrolltätigkeitsdaten

299) Die Fahrerkarte muss in Bezug auf Kontrolltätigkeiten die folgenden Daten speichern können:

— Datum und Uhrzeit der Kontrolle,

— Kontrollkartennummer und ausstellender Mitgliedstaat,

— Art der Kontrolle (Anzeige und/oder Drucken und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte (siehe Anmerkung)),

— heruntergeladener Zeitraum beim Herunterladen,

— amtliches Kennzeichen und zulassender Mitgliedstaat des kontrollierten Fahrzeugs.

Anmerkung: Gemäß Sicherheitsanforderungen wird ein Herunterladen von der Karte nur aufgezeichnet, wenn dies über ein Kontrollgerät erfolgt.

300) Die Fahrerkarte muss einen derartigen Datensatz gespeichert halten können.

4.5.3.2.14 Daten zu spezifischen Bedingungen

301) Die Fahrerkarte muss die folgenden Daten in Bezug auf spezifische Bedingungen speichern können, die bei eingesetzter Karte (ungeachtet des Steckplatzes) eingegeben wurden:

— Datum und Uhrzeit der Eingabe,

— Art der spezifischen Bedingung.

302) Die Fahrerkarte muss mindestens 56 derartige Datensätze speichern können.

4.5.3.2.15 Daten zu den genutzten Fahrzeugeinheiten

303) Die Fahrerkarte muss die folgenden Daten in Bezug auf die verschiedenen Fahrzeugeinheiten, in denen die Karte genutzt wurde, speichern können:

— Datum und Uhrzeit des Beginns des Nutzungszeitraums der Fahrzeugeinheit (d. h. erstes Einstecken der Karte in der Fahrzeugeinheit für den Zeitraum),

— Hersteller der Fahrzeugeinheit,

— Typ der Fahrzeugeinheit,

— Softwareversionsnummer der Fahrzeugeinheit.

304) Die Fahrerkarte muss mindestens 84 derartige Datensätze speichern können.

4.5.3.2.16 Ortsdaten zu drei Stunden ununterbrochener Lenkzeit

305) Die Fahrerkarte muss die folgenden Daten zur Position des Fahrzeugs speichern können, wenn die ununterbrochene Lenkzeit des Fahrer ein Vielfaches von drei Stunden erreicht:

— Datum und Uhrzeit, wenn die ununterbrochene Lenkzeit des Karteninhabers ein Vielfaches von drei Stunden erreicht,

— Position des Fahrzeugs.

— GNSS-Genauigkeit, Datum und Uhrzeit der Feststellung der Position.

306) Die Fahrerkarte muss mindestens 252 derartige Datensätze speichern können.

4.5.4 *Werkstattkarte*

4.5.4.1 Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation)

4.5.4.1.1 Anwendungskennung

307) Die Werkstattkarten müssen die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.4.1.2 Schlüssel und Zertifikate

308) Die Werkstattkarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil A speichern können.

309) Die Werkstattkarte muss einen PIN-Code (Personal Identification Number) speichern können.

4.5.4.1.3 Kartenkennung

310) Die Werkstattkarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis.

4.5.4.1.4 Karteninhaberkennung

311) Die Werkstattkarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name der Werkstatt,

— Anschrift der Werkstatt.

— Name des Karteninhabers,

— Vorname(n) des Karteninhabers,

— bevorzugte Sprache.

4.5.4.1.5 Herunterladen von der Karte

312) Die Werkstattkarte muss einen von der Karte heruntergeladenen Datensatz so speichern können wie eine Fahrerkarte.

4.5.4.1.6 Kalibrierungs- und Zeiteinstellungsdaten

313) Die Werkstattkarte muss Datensätze zu Kalibrierungen und/oder Zeiteinstellungen gespeichert halten können, die ausgeführt werden, während die Karte in einem Kontrollgerät eingesteckt ist.

314) In jedem Kalibrierungsdatensatz müssen folgende Daten enthalten sein:

— Zweck der Kalibrierung (Aktivierung, Ersteinbau, Einbau, regelmäßige Nachprüfung),

— Fahrzeugkennung,

— aktualisierte oder bestätigte Parameter (Wegdrehzahl, Kontrollgerätkonstante, tatsächlicher Reifenumfang, Reifengröße, Einstellung des Geschwindigkeitsbegrenzers, Kilometerstand (alt und neu), Datum und Uhrzeit (alte und neue Werte),

— Kontrollgerätkennung (VU-Teilnummer, VU-Seriennummer, Seriennummer des Bewegungssensors).

315) Die Werkstattkarte muss mindestens 88 derartige Datensätze speichern können.

316) Die Werkstattkarte führt einen Zähler, der die Gesamtzahl der mit der Karte ausgeführten Kalibrierungen angibt.

317) Die Werkstattkarte führt einen Zähler, der die Anzahl der seit dem letzten Herunterladen durchgeführten Kalibrierungen angibt.

4.5.4.1.7 Ereignis- und Störungsdaten

318) Die Werkstattkarte muss Ereignis- und Störungsdaten so speichern können wie eine Fahrerkarte.

319) Die Werkstattkarte muss Daten für die drei jüngsten Ereignisse jeder Art (d. h. 18 Ereignisse) sowie die sechs jüngsten Störungen jeder Art (d. h. 12 Störungen) speichern können.

4.5.4.1.8 Fahrertätigkeitsdaten

320) Die Werkstattkarte muss Fahrertätigkeitsdaten so speichern können wie eine Fahrerkarte.

321) Die Werkstattkarte muss Fahrertätigkeitsdaten für mindestens 1 Tag mit durchschnittlicher Tätigkeit eines Fahrers gespeichert halten können.

4.5.4.1.9 Daten zu gefahrenen Fahrzeugen

322) Die Werkstattkarte muss Datensätze zu gefahrenen Fahrzeugen so speichern können wie eine Fahrerkarte.

323) Die Werkstattkarte muss mindestens 4 derartige Datensätze speichern können.

4.5.4.1.10 Daten zum Beginn und/oder Ende des Arbeitstages

324) Die Werkstattkarte muss Datensätze zum Beginn und/oder Ende des Arbeitstages so speichern können wie eine Fahrerkarte.

325) Die Werkstattkarte muss mindestens 3 derartige Datensatzpaare gespeichert halten können.

4.5.4.1.11 Kartenvorgangsdaten

326) Die Werkstattkarte muss einen Kartenvorgang so speichern können wie eine Fahrerkarte.

4.5.4.1.12 Kontrolltätigkeitsdaten

327) Die Werkstattkarte muss einen Kontrolltätigkeitsdatensatz so speichern können wie eine Fahrerkarte.

4.5.4.1.13 Daten zu spezifischen Bedingungen

328) Die Werkstattkarte muss Daten in Bezug auf spezifische Bedingungen so wie die Fahrerkarte speichern können.

329) Die Werkstattkarte muss mindestens 2 derartige Datensätze speichern können.

4.5.4.2 Fahrtenschreiberanwendung der zweiten Generation (für Fahrzeugeinheiten der ersten Generation nicht zugänglich)

4.5.4.2.1 Anwendungskennung

330) Die Werkstattkarten müssen die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.4.2.2 Schlüssel und Zertifikate

331) Die Werkstattkarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil A speichern können.

332) Die Werkstattkarte muss einen PIN-Code (Personal Identification Number) speichern können.

4.5.4.2.3 Kartenkennung

333) Die Werkstattkarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis.

4.5.4.2.4 Karteninhaberkennung

334) Die Werkstattkarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name der Werkstatt,

— Anschrift der Werkstatt.

— Name des Karteninhabers,

— Vorname(n) des Karteninhabers,

— bevorzugte Sprache.

4.5.4.2.5 Herunterladen von der Karte

335) Die Werkstattkarte muss einen von der Karte heruntergeladenen Datensatz so speichern können wie eine Fahrerkarte.

4.5.4.2.6 Kalibrierungs- und Zeiteinstellungsdaten

336) Die Werkstattkarte muss Datensätze zu Kalibrierungen und/oder Zeiteinstellungen gespeichert halten können, die ausgeführt werden, während die Karte in einem Kontrollgerät eingesteckt ist.

337) In jedem Kalibrierungsdatensatz müssen folgende Daten enthalten sein:

— Zweck der Kalibrierung (Aktivierung, Ersteinbau, Einbau, regelmäßige Nachprüfung),

— Fahrzeugkennung,

— aktualisierte oder bestätigte Parameter (Wegdrehzahl, Kontrollgerätkonstante, tatsächlicher Reifenumfang, Reifengröße, Einstellung des Geschwindigkeitsbegrenzers, Kilometerstand (alt und neu), Datum und Uhrzeit (alte und neue Werte),

— Kontrollgerätkennung (VU-Teilnummer, VU-Seriennummer, Seriennummer des Bewegungssensors, Seriennummer der Fernkommunikationsausrüstung und Seriennummer der externen GNSS-Ausrüstung, falls zutreffend),

— Typ und Kennung aller vorhandenen Plombierungen,

— Fähigkeit der Fahrzeugeinheit, aktivierte oder nicht aktivierte Fahrtenschreiberkarten der ersten Generation zu nutzen.

338) Die Werkstattkarte muss mindestens 88 derartige Datensätze speichern können.

339) Die Werkstattkarte führt einen Zähler, der die Gesamtzahl der mit der Karte ausgeführten Kalibrierungen angibt.

340) Die Werkstattkarte führt einen Zähler, der die Anzahl der seit dem letzten Herunterladen durchgeführten Kalibrierungen angibt.

4.5.4.2.7 Ereignis- und Störungsdaten

341) Die Werkstattkarte muss Ereignis- und Störungsdaten so speichern können wie eine Fahrerkarte.

342) Die Werkstattkarte muss Daten für die drei jüngsten Ereignisse jeder Art (d. h. 33 Ereignisse) sowie die sechs jüngsten Störungen jeder Art (d. h. 12 Störungen) speichern können.

4.5.4.2.8 Fahrertätigkeitsdaten

343) Die Werkstattkarte muss Fahrertätigkeitsdaten so speichern können wie eine Fahrerkarte.

344) Die Werkstattkarte muss Fahrertätigkeitsdaten für mindestens 1 Tag mit durchschnittlicher Tätigkeit eines Fahrers gespeichert halten können.

4.5.4.2.9 Daten zu gefahrenen Fahrzeugen

345) Die Werkstattkarte muss Datensätze zu gefahrenen Fahrzeugen so speichern können wie eine Fahrerkarte.

346) Die Werkstattkarte muss mindestens 4 derartige Datensätze speichern können.

4.5.4.2.10 Daten zum Beginn und/oder Ende des Arbeitstages

347) Die Werkstattkarte muss Datensätze zum Beginn und/oder Ende des Arbeitstages so speichern können wie eine Fahrerkarte.

348) Die Werkstattkarte muss mindestens 3 derartige Datensatzpaare gespeichert halten können.

4.5.4.2.11 Kartenvorgangsdaten

349) Die Werkstattkarte muss einen Kartenvorgang so speichern können wie eine Fahrerkarte.

4.5.4.2.12 Kontrolltätigkeitsdaten

350) Die Werkstattkarte muss einen Kontrolltätigkeitsdatensatz so speichern können wie eine Fahrerkarte.

4.5.4.2.13 Daten zu den genutzten Fahrzeugeinheiten

351) Die Werkstattkarte muss die folgenden Daten in Bezug auf die verschiedenen Fahrzeugeinheiten, in denen die Karte genutzt wurde, speichern können:

— Datum und Uhrzeit des Beginns des Nutzungszeitraums der Fahrzeugeinheit (d. h. erstes Einstecken der Karte in der Fahrzeugeinheit für den Zeitraum),

— Hersteller der Fahrzeugeinheit,

— Typ der Fahrzeugeinheit,

— Softwareversionsnummer der Fahrzeugeinheit.

352) Die Werkstattkarte muss mindestens 4 derartige Datensätze speichern können.

4.5.4.2.14 Ortsdaten zu drei Stunden ununterbrochener Lenkzeit

353) Die Werkstattkarte muss die folgenden Daten zur Position des Fahrzeugs speichern können, wenn die ununterbrochene Lenkzeit des Fahrer ein Vielfaches von drei Stunden erreicht:

— Datum und Uhrzeit, wenn die ununterbrochene Lenkzeit des Karteninhabers ein Vielfaches von drei Stunden erreicht,

— Position des Fahrzeugs,

— GNSS-Genauigkeit, Datum und Uhrzeit der Feststellung der Position.

354) Die Werkstattkarte muss mindestens 18 derartige Datensätze speichern können.

4.5.4.2.15 Daten zu spezifischen Bedingungen

355) Die Werkstattkarte muss Daten in Bezug auf spezifische Bedingungen so wie die Fahrerkarte speichern können.

356) Die Werkstattkarte muss mindestens 2 derartige Datensätze speichern können.

4.5.5 *Kontrollkarte*

4.5.5.1 Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation)

4.5.5.1.1 Anwendungskennung

357) Die Kontrollkarte muss die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.5.1.2 Schlüssel und Zertifikate

358) Die Kontrollkarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil A speichern können.

4.5.5.1.3 Kartenkennung

359) Die Kontrollkarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis (wenn zutreffend).

4.5.5.1.4 Karteninhaberkennung

360) Die Kontrollkarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name der Kontrollstelle,

— Anschrift der Kontrollstelle,

— Name des Karteninhabers,

— Vorname(n) des Karteninhabers,

— bevorzugte Sprache.

4.5.5.1.5 Kontrolltätigkeitsdaten

361) Die Kontrollkarte muss die folgenden Daten in Bezug auf Kontrolltätigkeiten speichern können:

— Datum und Uhrzeit der Kontrolle,

— Art der Kontrolle (Anzeige und/oder Drucken und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte und/oder straßenseitige Kalibrierprüfung),

— heruntergeladener Zeitraum (wenn zutreffend),

— amtliches Kennzeichen und zulassender Mitgliedstaat des kontrollierten Fahrzeugs,

— Kartennummer und ausstellender Mitgliedstaat der kontrollierten Fahrerkarte.

362) Die Kontrollkarte muss mindestens 230 derartige Datensätze gespeichert halten können.

4.5.5.2 Fahrtenschreiberanwendung G2 (für Fahrzeugeinheiten der ersten Generation nicht zugänglich)

4.5.5.2.1 Anwendungskennung

363) Die Kontrollkarte muss die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.5.2.2 Schlüssel und Zertifikate

364) Die Kontrollkarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil B speichern können.

4.5.5.2.3 Kartenkennung

365) Die Kontrollkarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis (wenn zutreffend).

4.5.5.2.4 Karteninhaberkennung

366) Die Kontrollkarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name der Kontrollstelle,

— Anschrift der Kontrollstelle,

— Name des Karteninhabers,

— Vorname(n) des Karteninhabers,

— bevorzugte Sprache.

4.5.5.2.5 Kontrolltätigkeitsdaten

367) Die Kontrollkarte muss die folgenden Daten in Bezug auf Kontrolltätigkeiten speichern können:

— Datum und Uhrzeit der Kontrolle,

— Art der Kontrolle (Anzeige und/oder Drucken und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte und/oder straßenseitige Kalibrierprüfung),

— heruntergeladener Zeitraum (wenn zutreffend),

— amtliches Kennzeichen und zulassender Mitgliedstaat des kontrollierten Fahrzeugs,

— Kartennummer und ausstellender Mitgliedstaat der kontrollierten Fahrerkarte.

368) Die Kontrollkarte muss mindestens 230 derartige Datensätze gespeichert halten können.

4.5.6 *Unternehmenskarte*

4.5.6.1 Fahrtenschreiberanwendung (zugänglich für Fahrzeugeinheiten der ersten und zweiten Generation)

4.5.6.1.1 Anwendungskennung

369) Die Unternehmenskarte muss die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.6.1.2 Schlüssel und Zertifikate

370) Die Unternehmenskarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil A speichern können.

4.5.6.1.3 Kartenkennung

371) Die Unternehmenskarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis (wenn zutreffend).

4.5.6.1.4 Karteninhaberkennung

372) Die Unternehmenskarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name des Unternehmens,

— Anschrift des Unternehmens.

4.5.6.1.5 Unternehmensaktivitätsdaten

373) Die Unternehmenskarte muss die folgenden Daten in Bezug auf Unternehmensaktivitäten speichern können:

— Datum und Uhrzeit der Aktivität,

— Art der Aktivität (Sperren/Entsperren der Fahrzeugeinheit und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte),

— heruntergeladener Zeitraum (wenn zutreffend),

— amtliches Kennzeichen und Zulassungsbehörde des Mitgliedstaates des Fahrzeugs,

— Kartennummer und ausstellender Mitgliedstaat (beim Herunterladen von der Karte).

374) Die Unternehmenskarte muss mindestens 230 derartige Datensätze gespeichert halten können.

4.5.6.2 Fahrtenschreiberanwendung G2 (für Fahrzeugeinheiten der ersten Generation nicht zugänglich)

4.5.6.2.1 Anwendungskennung

375) Die Unternehmenskarte muss die folgenden Anwendungskenndaten speichern können:

— Kennnummer der Fahrtenschreiberanwendung,

— Art der Fahrtenschreiberkartenkennung.

4.5.6.2.2 Schlüssel und Zertifikate

376) Die Unternehmenskarte muss eine Reihe kryptografischer Schlüssel und Zertifikate gemäß Anlage 11 Teil B speichern können.

4.5.6.2.3 Kartenkennung

377) Die Unternehmenskarte muss die folgenden Kartenkenndaten speichern können:

— Kartennummer,

— ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum,

— gültig ab, gültig bis (wenn zutreffend).

4.5.6.2.4 Karteninhaberkennung

378) Die Unternehmenskarte muss die folgenden Karteninhaberkenndaten speichern können:

— Name des Unternehmens,

— Anschrift des Unternehmens.

4.5.6.2.5 Unternehmensaktivitätsdaten

379) Die Unternehmenskarte muss die folgenden Daten in Bezug auf Unternehmensaktivitäten speichern können:

— Datum und Uhrzeit der Aktivität,

— Art der Aktivität (Sperren/Entsperren der Fahrzeugeinheit und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte),

— heruntergeladener Zeitraum (wenn zutreffend),

— amtliches Kennzeichen und Zulassungsbehörde des Mitgliedstaates des Fahrzeugs,

— Kartennummer und ausstellender Mitgliedstaat (beim Herunterladen von der Karte).

380) Die Unternehmenskarte muss mindestens 230 derartige Datensätze gespeichert halten können.

5 EINBAU EINES KONTROLLGERÄTS

5.1 **Einbau**

381) Neue Kontrollgeräte werden in nicht aktiviertem Zustand an Einbaubetriebe oder Fahrzeughersteller geliefert, wobei alle in Kapitel 3.21 aufgeführten Kalibrierungsparameter auf geeignete und gültige Standardwerte eingestellt sind. Liegt kein bestimmter Wert vor, sind Buchstaben-Parameter auf Strings mit „?“ und numerische Parameter auf „0“zu setzen. Die Auslieferung sicherheitsrelevanter Teile des Kontrollgeräts kann erforderlichenfalls während der Sicherheitszertifizierung eingeschränkt werden.

382) Vor seiner Aktivierung muss das Kontrollgerät den Zugang zur Kalibrierfunktion gewähren, auch wenn es sich nicht in der Betriebsart Kalibrierung befindet.

383) Vor seiner Aktivierung darf das Kontrollgerät die in 3.12.3, 3.12.9 sowie 3.12.12 bis 3.12.15 genannten Daten weder aufzeichnen noch speichern.

384) Während des Einbaus werden alle bekannten Parameter vom Fahrzeughersteller voreingestellt.

385) Der Fahrzeughersteller oder Einbaubetrieb aktiviert das eingebaute Kontrollgerät spätestens, bevor das Fahrzeug im Anwendungsbereich der Verordnung (EG) Nr. 561/2006 betrieben wird.

386) Die Aktivierung des Kontrollgeräts wird durch das erstmalige Einstecken einer gültigen Werkstattkarte in eine der beiden Kartenschnittstellen automatisch ausgelöst.

387) Gegebenenfalls erforderliche spezifische Koppelungsoperationen zwischen dem Bewegungssensor und der Fahrzeugeinheit müssen automatisch vor oder während der Aktivierung stattfinden.

388) Ebenso müssen gegebenenfalls erforderliche spezifische Kopplungsoperationen zwischen der externen GNSS-Ausrüstung und der Fahrzeugeinheit automatisch vor oder während der Aktivierung stattfinden.

389) Nach seiner Aktivierung sorgt das Kontrollgerät für die vollständige Anwendung aller Funktionen und Datenzugriffsrechte.

390) Nach seiner Aktivierung kommuniziert das Kontrollgerät der Fernkommunikationsausrüstung die gesicherten Daten, die für die Zwecke der gezielten Straßenkontrollen erforderlich sind.

391) Die Aufzeichnungs- und Speicherfunktion des Kontrollgeräts muss nach seiner Aktivierung voll wirksam sein.

392) Nach dem Einbau erfolgt eine Kalibrierung. Bei der Erstkalibrierung wird das amtliche Kennzeichen des Fahrzeugs (VRN) nicht notwendigerweise eingegeben, wenn es der mit der Kalibrierung beauftragten zugelassenen Werkstatt nicht bekannt ist. Unter diesen Umständen und nur zu diesem Zeitpunkt muss der Fahrzeugeigentümer die Möglichkeit haben, unter Verwendung seiner Unternehmenskarte das amtliche Kennzeichen des Fahrzeugs einzugeben (beispielsweise mittels Befehlen in einer geeigneten Menüstruktur der Mensch-Maschine-Schnittstelle der Fahrzeugeinheit), bevor das Fahrzeug im Geltungsbereich der Verordnung (EG) Nr. 561/2006 betrieben wird [1]. Eine Aktualisierung oder Bestätigung dieser Eingabe ist nur unter Verwendung einer Werkstattkarte möglich.

393) Der Einbau einer externen GNSS-Ausrüstung erfordert die Kopplung mit der Fahrzeugeinheit und die nachträgliche Überprüfung der GNSS-Positionsdaten.

394) Das Kontrollgerät ist im Fahrzeug so anzubringen, dass für den Fahrer alle notwendigen Funktionen vom Fahrersitz aus zugänglich sind.

[1] ABl. L 102 vom 11.4.2006, S. 1.

5.2 **Einbauplakette**

395) Nach der Einbauprüfung beim Ersteinbau wird auf dem Kontrollgerät deutlich sichtbar und leicht zugänglich eine eingravierte oder dauerhaft aufgedruckte Einbauplakette angebracht. Falls dies nicht möglich ist, wird die Plakette deutlich sichtbar an der B-Säule des Fahrzeugs angebracht. Bei Fahrzeugen ohne B-Säule sollte die Einbauplakette am Türrahmen der Fahrerseite des Fahrzeugs angebracht werden und in jedem Fall deutlich sichtbar sein.

Nach jedem Eingriff eines zugelassenen Einbaubetriebs oder einer zugelassenen Werkstatt ist die Einbauplakette durch eine neue Plakette zu ersetzen.

396) Die Einbauplakette muss mindestens die nachstehenden Angaben enthalten:

— Name, Anschrift oder Firmenzeichen des zugelassenen Einbaubetriebs oder der zugelassenen Werkstatt,

— Wegdrehzahl des Kraftfahrzeugs in der Form „w = … imp/km“,

— Konstante des Kontrollgeräts in der Form „k = … imp/km“,

— tatsächlicher Reifenumfang in der Form „l = … mm“,

— Reifengröße,

— Datum der Messung der Wegdrehzahl des Kraftfahrzeugs und des tatsächlichen Reifenumfangs,

— Fahrzeugidentifizierungsnummer,

— Vorhandensein oder Nichtvorhandensein einer externen GNSS-Ausrüstung,

— Seriennummer der externen GNSS-Ausrüstung,

— Seriennummer der Fernkommunikationsausrüstung,

— Seriennummer aller vorhandenen Plombierungen,

— Fahrzeugteil, in dem der Adapter gegebenenfalls eingebaut wird,

— Fahrzeugteil, in dem der Bewegungssensor eingebaut wird, wenn er nicht an das Getriebe angeschlossen ist oder kein Adapter verwendet wird,

— Farbe des Kabels zwischen dem Adapter und diesem Fahrzeugteil, das seine Eingangsimpulse bereitstellt,

— Seriennummer des eingebetteten Bewegungssensors des Adapters.

397) Nur bei Fahrzeugen der Klassen M1 und N1, die gemäß der Verordnung (EG) Nr. 68/2009 der Kommission [1] in der zuletzt geänderten Fassung mit einem Adapter ausgestattet sind und bei denen nicht alle nötigen Informationen nach Randnummer 396 aufgenommen werden können, kann eine zweite, zusätzliche Einbauplakette verwendet werden. In diesen Fällen muss die zusätzliche Plakette mindestens die letzten vier in Randnummer 396 aufgeführten Spiegelstriche enthalten.

Falls diese zweite, zusätzliche Plakette verwendet wird, ist sie an oder neben der ersten, in Randnummer 396 beschriebenen Hauptplakette anzubringen; sie muss das gleiche Schutzniveau haben. Daneben muss die zweite Plakette ebenfalls Name, Anschrift oder Firmenzeichen des zugelassenen Einbaubetriebs oder der zugelassenen Werkstatt, der bzw. die den Einbau vorgenommen hat, sowie das Datum des Einbaus tragen.

[1] Verordnung (EG) Nr. 68/2009 der Kommission vom 23. Januar 2009 zur neunten Anpassung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr an den technischen Fortschritt (ABl. L 21 vom 24.1.2009, S. 3).

5.3 **Plombierung**

398) Folgende Geräteteile müssen plombiert werden:

— jeder Anschluss, sofern es bei einer Trennung der Verbindung zu nicht nachweisbaren Änderungen oder nicht feststellbaren Datenverlusten kommen würde (dies kann beispielsweise für den Einbau des Bewegungssensors am Getriebe, den Adapter für Fahrzeuge der Klassen M1/N1, die externe GNSS-Verbindung oder die Fahrzeugeinheit gelten);

— die Einbauplakette, es sei denn, sie ist so angebracht, dass sie sich nicht ohne Vernichtung der Angaben entfernen lässt.

399) Die genannten Plombierungen dürfen entfernt werden:

— in Notfällen,

— um einen Geschwindigkeitsbegrenzer oder ein anderes der Sicherheit im Straßenverkehr dienendes Gerät einzubauen, zu justieren oder zu reparieren, sofern das Kontrollgerät auch dann noch zuverlässig und ordnungsgemäß arbeitet und von einem zugelassenen Einbaubetrieb oder einer zugelassenen Werkstatt (gemäß Kapitel 6) unmittelbar nach dem Einbau des Geschwindigkeitsbegrenzers bzw. eines anderen der Sicherheit im Straßenverkehr dienenden Gerätes oder andernfalls spätestens nach sieben Tagen wieder plombiert wird.

400) Jede Verletzung der Plombierung muss Gegenstand einer schriftlichen Begründung sein, die der zuständigen Behörde zur Verfügung zu halten ist.

401) Die Plombierungen müssen eine von ihrem Hersteller zugeteilte Kennnummer tragen. Diese Nummer ist einmalig und unterscheidet sich von allen anderen Plombierungsnummern, die von anderen Herstellern zugeteilt wurden.

Diese einmalige Nummer setzt sich wie folgt zusammen: MM NNNNNN als nicht entfernbare Angaben, dabei ist MM das einmalige Herstellerzeichen (die Registrierung in der Datenbank ist von der Europäischen Kommission zu verwalten) und NNNNNN die im Bereich des Herstellers einmalige alphanumerische Nummer der Plombierung.

402) Die Plombierungen müssen über eine freie Stelle verfügen, an der zugelassene Einbaubetriebe, Werkstätten oder Fahrzeughersteller ein besonderes Zeichen gemäß Artikel 22 Absatz 3 der Verordnung (EU) Nr. 165/2014 anbringen können.

Dieses Zeichen darf die Kennnummer der Plombierung nicht überdecken.

403) Die Hersteller der Plombierungen werden in einer speziellen Datenbank registriert und veröffentlichen die Nummern ihrer Plombierungen nach einem von der Europäischen Kommission festzulegenden Verfahren.

404) Die zugelassenen Werkstätten und Fahrzeughersteller verwenden im Rahmen der Verordnung (EU) Nr. 165/2014 nur Plombierungen von Herstellern, die in der vorstehend genannten Datenbank registriert sind.

405) Die Hersteller der Plombierungen und ihre Händler führen umfassende Aufzeichnungen zur Rückverfolgbarkeit der zur Verwendung im Rahmen der Verordnung (EU) Nr. 165/2014 verkauften Plombierungen und müssen bereit sein, diese den zuständigen nationalen Behörden erforderlichenfalls vorzulegen.

406) Die einmaligen Identifikationsnummern der Plombierungen müssen auf der Einbauplakette sichtbar sein.

6 EINBAUPRÜFUNGEN, NACHPRÜFUNGEN UND REPARATUREN

Die in Artikel 22 Absatz 5 der Verordnung (EU) Nr. 165/2014 genannten Umstände, unter denen die Plombierungen entfernt werden dürfen, sind in Kapitel 5.3 dieses Anhangs festgelegt.

6.1 **Zulassung der Einbaubetriebe, Werkstätten und Fahrzeughersteller**

Die Mitgliedstaaten übernehmen die Zulassung, regelmäßige Kontrolle und Zertifizierung der Stellen, die

— den Einbau,

— Einbauprüfungen,

— Nachprüfungen und

— Reparaturen vornehmen.

Werkstattkarten werden, sofern keine entsprechende Begründung erfolgt, nur an für die Aktivierung und/oder Kalibrierung des Kontrollgeräts gemäß diesem Anhang zugelassene Einbaubetriebe und/oder Werkstätten ausgegeben,

— die keinen Anspruch auf eine Unternehmenskarte haben

— und deren sonstige unternehmerische Tätigkeit keine potenzielle Gefährdung der Gesamtsicherheit des Systems nach Anlage 10 darstellt.

6.2 **Prüfung neuer oder reparierter Geräte**

407) Für jedes neue oder reparierte Einzelgerät werden die ordnungsgemäße Arbeitsweise und die Genauigkeit der Anzeigen und Aufzeichnungen innerhalb der in den Kapiteln 3.2.1, 3.2.2, 3.2.3 und 3.3 festgelegten Grenzen durch die in Kapitel 5.3 vorgesehene Plombierung sowie durch Kalibrierung geprüft.

6.3 **Einbauprüfung**

408) Beim Einbau in ein Fahrzeug muss die Gesamtanlage (einschließlich des Kontrollgeräts) den Vorschriften über die in den Kapiteln 3.2.1, 3.2.2, 3.2.3 und 3.3 festgelegten zulässigen Fehlergrenzen entsprechen.

6.4 **Regelmäßige Nachprüfungen**

409) Regelmäßige Nachprüfungen der im Kraftfahrzeug eingebauten Ausrüstung erfolgen nach jeder Reparatur der Ausrüstung, jeder Änderung der Wegdrehzahl oder des tatsächlichen Reifenumfangs, wenn die UTC-Zeit von der korrekten Zeit um mehr als 20 Minuten abweicht oder wenn sich das amtliche Kennzeichen geändert hat, und mindestens einmal innerhalb von zwei Jahren (24 Monaten) seit der letzten Nachprüfung.

410) Überprüft wird zumindest:

— die ordnungsgemäße Arbeitsweise des Kontrollgeräts, einschließlich der Funktion Datenspeicherung auf Fahrtenschreiberkarten und der Kommunikation mit Fernabfragegeräten,

— die Einhaltung der Bestimmungen von Kapitel 3.2.1 und 3.2.2 über die zulässigen Fehlergrenzen des Geräts in eingebautem Zustand,

— die Einhaltung der Bestimmungen von Kapitel 3.2.3 und 3.3,

— das Vorhandensein des Typgenehmigungszeichens auf dem Kontrollgerät,

— das Vorhandensein der Einbauplakette gemäß Randnummer 396 sowie des Typenschilds gemäß Randnummer 225,

— die Reifengröße und der tatsächliche Umfang der Radreifen.

— dass keine Manipulationsgeräte am Kontrollgerät angebracht sind,

— dass die Plombierungen ordnungsgemäß angebracht sind, sich in einem guten Zustand befinden, ihre Kennnummern gültig sind (Hersteller der Plombierungen in der Datenbank der Europäischen Kommission verzeichnet) und ihre Kennnummern den Angaben auf der Einbauplakette (siehe Randnummer 401) entsprechen.

411) Falls sich erweist, dass seit der letzten Nachprüfung eines der in Kapitel 3.9 (Feststellung von Ereignissen und Störungen) aufgeführten Ereignisse aufgetreten ist, das von den Herstellern von Fahrtenschreibern und/oder nationalen Behörden als potenzielle Bedrohung der Sicherheit des Geräts betrachtet wird, so trifft die Werkstatt folgende Maßnahmen:

a. Vergleich zwischen den Kenndaten des an das Getriebe angeschlossenen Bewegungssensors und jenen des gekoppelten und in der Fahrzeugeinheit registrierten Bewegungssensors,

b. Überprüfung der Übereinstimmung der Informationen auf der Einbauplakette mit den in den Aufzeichnungen der Fahrzeugeinheit enthaltenen Informationen,

c. Vergleich der Seriennummer und der Genehmigungsnummer des Bewegungssensors, sofern auf dessen Gehäuse aufgedruckt, auf Übereinstimmung mit den im Massenspeicher des Kontrollgeräts gespeicherten Informationen.

d. Vergleich der Kenndaten auf dem Typenschild der externen GNSS-Ausrüstung, falls vorhanden, mit den im Massenspeicher der Fahrzeugeinheit gespeicherten Daten.

412) Die Werkstätten halten etwaige Erkenntnisse in Bezug auf aufgebrochene Plombierungen oder Manipulationsgeräte in ihren Nachprüfungsberichten fest. Die Werkstätten bewahren diese Berichte mindestens 2 Jahre lang auf und stellen sie der zuständigen Behörde auf Wunsch zur Verfügung.

413) Diese Nachprüfungen umfassen eine Kalibrierung und einen vorbeugenden Austausch der Plombierungen, für deren Einbau die Werkstätten verantwortlich sind..

6.5 **Messung der Anzeigefehler**

414) Die Messung der Anzeigefehler beim Einbau und während der Benutzung wird unter folgenden Bedingungen durchgeführt, die als normale Prüfbedingungen anzusehen sind:

— unbeladenes Fahrzeug in fahrbereitem Zustand,

— Reifendruck gemäß den Angaben des Herstellers,

— Reifenabnutzung innerhalb der nach den nationalen Rechtsvorschriften zulässigen Grenzen,

— Bewegungen des Fahrzeugs:

— Das Fahrzeug muss sich mit eigener Motorkraft geradlinig auf ebenem Gelände und mit einer Geschwindigkeit von 50 ± 5 km/h fortbewegen. Die Messstrecke muss mindestens 1 000 m betragen;

— die Prüfung kann auch mit anderen Methoden, so auf einem geeigneten Prüfstand, durchgeführt werden, sofern eine vergleichbare Genauigkeit gewährleistet ist.

6.6 **Reparaturen**

415) Die Werkstätten müssen Daten vom Kontrollgerät herunterladen können, um die Daten dem entsprechenden Transportunternehmen zu übergeben.

416) Die zugelassenen Werkstätten stellen den Transportunternehmen eine Bescheinigung über die Unmöglichkeit des Herunterladens der Daten aus, wenn das Herunterladen von aufgezeichneten Daten aufgrund eines Defekts des Kontrollgeräts auch nach der Reparatur durch diese Werkstätten nicht möglich ist. Eine Kopie jeder ausgestellten Bescheinigung ist von den Werkstätten mindestens 2 Jahre lang aufzubewahren.

7 KARTENAUSGABE

Die von den Mitgliedstaaten eingerichteten Kartenausgabeverfahren müssen folgenden Vorschriften entsprechen:

417) Die Kartennummer der Erstausgabe einer Fahrtenschreiberkarte an einen Antragsteller hat einen fortlaufenden Index (wenn zutreffend) sowie einen Ersatzindex und einen auf „0“ gesetzten Erneuerungsindex.

418) Die Kartennummern aller an dieselbe Kontrollstelle oder dieselbe Werkstatt oder dasselbe Transportunternehmen ausgegebenen nicht personengebundenen Fahrtenschreiberkarten weisen die gleichen ersten 13 Stellen sowie einen unterschiedlichen laufenden Index auf.

419) Eine als Ersatz für eine vorhandene Fahrtenschreiberkarte ausgegebene Fahrtenschreiberkarte weist die gleiche Kartennummer auf wie die ersetzte Karte, wobei jedoch der Ersatzindex um „1“ (in der Reihenfolge 0, … , 9, A, … , Z) erhöht ist.

420) Eine als Ersatz für eine vorhandene Fahrtenschreiberkarte ausgegebene Fahrtenschreiberkarte weist das gleiche Datum für den Ablauf der Gültigkeit auf wie die ersetzte Karte.

421) Eine zur Erneuerung einer vorhandenen Fahrtenschreiberkarte ausgegebene Fahrtenschreiberkarte trägt die gleiche Kartennummer wie die erneuerte Karte, wobei jedoch der Ersatzindex auf „0" zurückgesetzt und der Erneuerungsindex um „1" erhöht ist (in der Reihenfolge 0, … , 9, A, … , Z).

422) Der Austausch einer vorhandenen Fahrtenschreiberkarte zwecks Änderung von Verwaltungsdaten richtet sich bei Erneuerung innerhalb desselben Mitgliedstaates nach den Vorschriften für die Erneuerung und bei Ausführung durch einen anderen Mitgliedstaat nach den Vorschriften für die Erstausgabe.

423) In der Rubrik „Name des Karteninhabers" bei nicht personengebundenen Werkstatt- oder Kontrollkarten wird der Name der Werkstatt bzw. der Kontrollstelle oder des Einbaubetriebs oder der Name des Kontrolleurs angegeben, falls die Mitgliedstaaten dies beschließen.

424) Die Mitgliedstaaten tauschen Daten auf elektronischem Weg aus, um die Einzigkeit der von ihnen ausgestellten Fahrerkarten gemäß Artikel 31 der Verordnung (EU) Nr. 165/2014 zu gewährleisten.

8 TYPGENEHMIGUNG VON KONTROLLGERÄTEN UND FAHRTENSCHREIBERKARTEN

8.1 **Allgemeines**

Im Sinne dieses Kapitels ist unter dem Ausdruck „Kontrollgerät" das „Kontrollgerät oder seine Komponenten" zu verstehen. Für das/die Verbindungskabel zwischen dem Bewegungssensor und der Fahrzeugeinheit, der externen GNSS-Ausrüstung und der Fahrzeugeinheit oder der Fernkommunikationsausrüstung und der Fahrzeugeinheit ist keine Typgenehmigung erforderlich. Das zur Verwendung durch das Kontrollgerät bestimmte Papier ist als Komponente des Kontrollgeräts zu betrachten.

Jeder Hersteller kann für Komponenten des Kontrollgeräts in Kombination mit einem Bewegungssensor, einer externen GNSS-Ausrüstung –und umgekehrt — die Typgenehmigung beantragen, sofern jede Komponente den Vorschriften dieses Anhangs entspricht. Alternativ kann der Hersteller auch die Typgenehmigung für das Kontrollgerät beantragen.

425) Kontrollgeräte sind zusammen mit allen integrierten Zusatzgeräten zur Typgenehmigung vorzulegen.

426) Die Typgenehmigung von Kontrollgeräten und Fahrtenschreiberkarten beinhaltet Sicherheitsprüfungen, Funktionsprüfungen und Interoperabilitätsprüfungen. Die positiven Ergebnisse der einzelnen Prüfungen werden in einem geeigneten Zertifikat ausgewiesen.

427) Die Typgenehmigungsbehörden der Mitgliedstaaten erteilen nur dann eine Typgenehmigung, wenn ihnen

— ein Sicherheitszertifikat,

— ein Funktionszertifikat und

— ein Interoperabilitätszertifikat

für das Kontrollgerät oder die Fahrtenschreiberkarte, für die die Typgenehmigung beantragt wurde, vorliegen.

428) Änderungen an der Software oder Hardware des Geräts oder an den für seine Herstellung verwendeten Werkstoffen sind vor ihrer Umsetzung der Behörde zu melden, die die Typgenehmigung für das Gerät erteilt hat. Diese Behörde bestätigt dem Hersteller die Erweiterung der Typgenehmigung oder verlangt eine Aktualisierung oder Bestätigung des entsprechenden Funktions-, Sicherheits- und/oder Interoperabilitätszertifikats.

429) Verfahren zur Versionsaufrüstung der Software bereits eingebauter Kontrollgeräte sind von der Behörde zu genehmigen, die die Typgenehmigung für das Kontrollgerät erteilt hat. Durch die Softwareaufrüstung dürfen im Kontrollgerät gespeicherte Fahrertätigkeitsdaten nicht verändert oder gelöscht werden. Die Softwareaufrüstung darf nur unter der Verantwortung des Geräteherstellers erfolgen.

430) Die Typgenehmigung von Softwareänderungen zur Aufrüstung eines zuvor typgenehmigten Kontrollgeräts darf nicht verweigert werden, wenn derartige Änderungen nur für nicht in diesem Anhang aufgeführte Funktionen gelten. Die Softwareaufrüstung eines Kontrollgeräts kann die Einführung neuer Zeichensätze ausschließen, wenn dies technisch nicht machbar ist.

8.2 **Sicherheitszertifikat**

431) Das Sicherheitszertifikat wird gemäß den Bestimmungen von Anlage 10 dieses Anhangs erteilt. Die zu zertifizierenden Komponenten des Kontrollgeräts sind Fahrzeugeinheit, Bewegungssensor, externe GNSS-Ausrüstung und Fahrtenschreiberkarten.

432) Falls die für die Sicherheitszertifizierung zuständigen Behörden die Zertifizierung eines neuen Geräts ausnahmsweise wegen überholter Sicherheitsmechanismen verweigern, wird die Typgenehmigung in diesem bestimmten Ausnahmefall weiterhin erteilt, falls keine der Verordnung entsprechende Alternativlösung besteht.

433) In diesem Fall unterrichtet der betreffende Mitgliedstaat unverzüglich die Europäische Kommission, die innerhalb von zwölf Kalendermonaten nach Erteilung der Typgenehmigung ein Verfahren einleitet, um zu gewährleisten, dass das ursprüngliche Sicherheitsniveau wiederhergestellt wird.

8.3 **Funktionszertifikat**

434) Jeder Antragsteller einer Typgenehmigung legt der Typgenehmigungsbehörde des Mitgliedstaats sämtliche Materialien und Unterlagen vor, die die Behörde für notwendig erachtet.

435) Die Hersteller stellen die entsprechenden Muster der Produkte, für die eine Typgenehmigung beantragt wird, sowie die zugehörigen Unterlagen, die die mit der Durchführung von Funktionsprüfungen beauftragten Labors benötigen, innerhalb eines Monats nach diesbezüglichem Ersuchen zur Verfügung. Die aus diesem Ersuchen erwachsenden Kosten trägt die ersuchende Stelle. Die Labors behandeln sämtliche sensiblen Geschäftsinformationen vertraulich.

436) Ein Funktionszertifikat ist dem Hersteller erst zu erteilen, nachdem mindestens alle Funktionsprüfungen nach Anlage 9 erfolgreich bestanden wurden.

437) Das Funktionszertifikat wird von der Typgenehmigungsbehörde erteilt. Auf diesem Zertifikat ist neben dem Namen des Empfängers und der Modellkennung eine ausführliche Liste der durchgeführten Prüfungen und der erzielten Ergebnisse anzuführen.

438) Im Funktionszertifikat für eine Komponente eines Kontrollgeräts sind auch die Typgenehmigungsnummern sämtlicher anderen typgenehmigten kompatiblen Kontrollgerätkomponenten anzugeben.

439) Im Funktionszertifikat für eine Komponente eines Kontrollgeräts ist auch die ISO- oder CEN-Norm anzugeben, anhand deren die Funktionale Schnittstelle zertifiziert worden ist.

8.4 **Interoperabilitätszertifikat**

440) Interoperabilitätsprüfungen werden von einer einzigen Prüfstelle durchgeführt, die der Europäischen Kommission untersteht und sich in ihrer Verantwortung befindet.

441) Die Prüfstelle registriert von den Herstellern gestellte Anträge auf Interoperabilitätsprüfungen in der Reihenfolge ihres Eintreffens.

442) Anträge werden nur dann amtlich registriert, wenn der Prüfstelle folgende Unterlagen vorliegen:

— sämtliche Materialien und Dokumente, die für diese Interoperabilitätsprüfungen erforderlich sind,

— das entsprechende Sicherheitszertifikat,

— das entsprechende Funktionszertifikat.

Das Registrierungsdatum des Antrags wird dem Hersteller mitgeteilt.

443) Für ein Kontrollgerät oder eine Fahrtenschreiberkarte, für die kein Sicherheitszertifikat und kein Funktionszertifikat erteilt wurde, werden vom Labor keine Interoperabilitätsprüfungen durchgeführt, außer in dem in Randnummer 432 genannten Ausnahmefall.

444) Jeder Hersteller, der Interoperabilitätsprüfungen beantragt, verpflichtet sich, der damit beauftragten Prüfstelle sämtliche Materialien und Dokumente zu überlassen, die er für die Durchführung der Prüfungen bereitgestellt hat.

445) Die Interoperabilitätsprüfungen werden gemäß den Bestimmungen von Anlage 9 dieses Anhangs für jeweils alle Modelle von Kontrollgeräten oder Fahrtenschreiberkarten durchgeführt,

— deren Typgenehmigung noch gültig ist oder

— für die eine Typgenehmigung beantragt wurde und die ein gültiges Interoperabilitätszertifikat besitzen.

446) Die Interoperabilitätsprüfungen erstrecken sich auf alle Generationen von Kontrollgeräten oder Fahrtenschreiberkarten, die noch verwendet werden.

447) Das Interoperabilitätszertifikat wird dem Hersteller von der Prüfstelle erst erteilt, nachdem alle erforderlichen Interoperabilitätsprüfungen erfolgreich bestanden wurden.

448) Sind die Interoperabilitätsprüfungen bei einem oder mehreren Kontrollgeräten oder bei einer oder mehreren Fahrtenschreiberkarten nicht erfolgreich, wird das Interoperabilitätszertifikat erst dann erteilt, wenn der antragstellende Hersteller die erforderlichen Änderungen vorgenommen und die Interoperabilitätsprüfungen bestanden hat. Die Prüfstelle stellt mit Hilfe des von diesem Interoperabilitätsfehler betroffenen Herstellers die Ursache des Problems fest und bemüht sich, den antragstellenden Hersteller bei der Suche nach einer technischen Lösung zu unterstützen. Hat der Hersteller sein Produkt verändert, muss er sich bei den zuständigen Behörden vergewissern, dass das Sicherheitszertifikat und die Funktionszertifikate noch gültig sind.

449) Das Interoperabilitätszertifikat ist sechs Monate gültig. Hat der Hersteller bei Ablauf dieser Frist keine entsprechende Typgenehmigungsbogen erhalten, wird es ihm wieder entzogen. Das Interoperabilitätszertifikat wird vom Hersteller an die Typgenehmigungsbehörde des Mitgliedstaats weitergeleitet, die das Funktionszertifikat erteilt hat.

450) Ein Element, das möglicherweise einem Interoperabilitätsfehler zugrunde liegt, darf nicht gewinnbringend oder zur Errichtung einer beherrschenden Stellung verwendet werden.

8.5 Typgenehmigungsbogen

451) Die Typgenehmigungsbehörde des Mitgliedstaates darf den Typgenehmigungsbogen ausstellen, sobald ihr die drei benötigten Zertifikate vorliegen.

452) Auf dem Typgenehmigungsbogen für eine Komponente eines Kontrollgeräts sind auch die Typgenehmigungsnummern des anderen typgenehmigten interoperablen Kontrollgeräts anzugeben.

453) Bei der Erteilung der Typgenehmigung an den Hersteller fertigt die Typgenehmigungsbehörde eine Kopie des Typgenehmigungsbogens für die mit den Interoperabilitätsprüfungen betraute Prüfstelle an.

454) Die für Interoperabilitätsprüfungen zuständige Prüfstelle unterhält eine öffentliche Website mit einer aktuellen Liste der Modelle von Kontrollgeräten und Fahrtenschreiberkarten,

— für die ein Antrag auf Interoperabilitätsprüfungen registriert wurde,

— für die ein Interoperabilitätszertifikat (auch ein vorläufiges Interoperabilitätszertifikat) erteilt wurde,

— für die ein Typgenehmigungsbogen ausgestellt wurde.

8.6 **Ausnahmeverfahren: für die ersten Interoperabilitätszertifikate für Kontrollgeräte und Fahrtenschreiberkarten der zweiten Generation**

455) Während eines Zeitraums von vier Monaten, nachdem ein erster Satz von Kontrollgeräten der zweiten Generation und Fahrtenschreiberkarten der zweiten Generation (Fahrer-, Werkstatt-, Kontroll- und Unternehmenskarten) als interoperabel zertifiziert wurden, gilt jedes Interoperabilitätszertifikat (auch die ersten), das in diesem Zeitraum auf entsprechenden Antrag ausgestellt wird, als vorläufig.

456) Sind am Ende dieses Zeitraums sämtliche betreffenden Produkte interoperabel, erhalten sämtliche entsprechenden Interoperabilitätszertifikate endgültigen Charakter.

457) Werden in diesem Zeitraum Interoperabilitätsfehler festgestellt, ermittelt die mit den Interoperabilitätsprüfungen betraute Prüfstelle die Ursachen der Probleme mit Hilfe aller beteiligten Hersteller und fordert diese auf, die erforderlichen Änderungen vorzunehmen.

458) Liegen am Ende dieses Zeitraums weiterhin Interoperabilitätsprobleme vor, ermittelt die mit den Interoperabilitätsprüfungen betraute Prüfstelle in Zusammenarbeit mit den betreffenden Herstellern und mit den Typgenehmigungsbehörden, die die entsprechenden Funktionszertifikate erteilt haben, die Ursachen der Interoperabilitätsfehler und gibt an, welche Änderungen von den einzelnen betroffenen Herstellern vorzunehmen sind. Die Suche nach technischen Lösungen dauert maximal zwei Monate; ist nach Ablauf dieses Zeitraums keine gemeinsame Lösung gefunden worden, entscheidet die Kommission nach Rücksprache mit der mit den Interoperabilitätsprüfungen betrauten Prüfstelle unter Angabe von Gründen, welchen Geräten und Karten ein endgültiges Interoperabilitätszertifikat erteilt wird.

459) Anträge auf Interoperabilitätsprüfungen, die von der Prüfstelle zwischen dem Ende der Viermonatsfrist nach Erteilung des ersten vorläufigen Interoperabilitätszertifikats und dem Datum der in Randnummer 455 genannten Entscheidung der Kommission registriert werden, sind bis zur Lösung der ursprünglichen Interoperabilitätsprobleme zurückzustellen. Anschließend werden diese Anträge in der Reihenfolge ihrer Registrierung bearbeitet.

Anlage 1

DATENGLOSSAR

INHALTSVERZEICHNIS

1. EINLEITUNG 88
1.1. Grundlage für die Definition von Datentypen 88
1.2. Referenzdokumente 88
2. DATENTYPDEFINITIONEN 89
2.1. ActivityChangeInfo 89
2.2. Address 90
2.3. AESKey 91
2.4. AES128Key 91
2.5. AES192Key 91
2.6. AES256Key 92
2.7. BCDString 92
2.8. CalibrationPurpose 92
2.9. CardActivityDailyRecord 93
2.10. CardActivityLengthRange 93
2.11. CardApprovalNumber 93
2.12. CardCertificate 94
2.13. CardChipIdentification 94
2.14. CardConsecutiveIndex 94
2.15. CardControlActivityDataRecord 94
2.16. CardCurrentUse 95
2.17. CardDriverActivity 95
2.18. CardDrivingLicenceInformation 95
2.19. CardEventData 96
2.20. CardEventRecord 96
2.21. CardFaultData 96
2.22. CardFaultRecord 97
2.23. CardIccIdentification 97
2.24. CardIdentification 97
2.25. CardMACertificate 98
2.26. CardNumber 98
2.27. CardPlaceDailyWorkPeriod 99
2.28. CardPrivateKey 99

2.29. CardPublicKey 99
2.30. CardRenewalIndex 99
2.31. CardReplacementIndex 99
2.32. CardSignCertificate 100
2.33. CardSlotNumber 100
2.34. CardSlotsStatus 100
2.35. CardSlotsStatusRecordArray 100
2.36. CardStructureVersion 101
2.37. CardVehicleRecord 101
2.38. CardVehiclesUsed 102
2.39. CardVehicleUnitRecord 102
2.40. CardVehicleUnitsUsed 102
2.41. Certificate 103
2.42. CertificateContent 103
2.43. CertificateHolderAuthorisation 104
2.44. CertificateRequestID 104
2.45. CertificationAuthorityKID 104
2.46. CompanyActivityData 105
2.47. CompanyActivityType 106
2.48. CompanyCardApplicationIdentification 106
2.49. CompanyCardHolderIdentification 106
2.50. ControlCardApplicationIdentification 106
2.51. ControlCardControlActivityData 107
2.52. ControlCardHolderIdentification 107
2.53. ControlType 108
2.54. CurrentDateTime 109
2.55. CurrentDateTimeRecordArray 109
2.56. DailyPresenceCounter 109
2.57. Datef 109
2.58. DateOfDayDownloaded 110
2.59. DateOfDayDownloadedRecordArray 110
2.60. Distance 110
2.61. DriverCardApplicationIdentification 110
2.62. DriverCardHolderIdentification 111
2.63. DSRCSecurityData 112
2.64. EGFCertificate 112
2.65. EmbedderIcAssemblerId 112

2.66. EntryTypeDailyWorkPeriod 113
2.67. EquipmentType 113
2.68. EuropeanPublicKey 114
2.69. EventFaultRecordPurpose 114
2.70. EventFaultType 114
2.71. ExtendedSealIdentifier 115
2.72. ExtendedSerialNumber 116
2.73. FullCardNumber 116
2.74. FullCardNumberAndGeneration 117
2.75. Generation 117
2.76. GeoCoordinates 117
2.77. GNSSAccuracy 118
2.78. GNSSContinuousDriving 118
2.79. GNSSContinuousDrivingRecord 118
2.80. GNSSPlaceRecord 118
2.81. HighResOdometer 119
2.82. HighResTripDistance 119
2.83. HolderName 119
2.84. InternalGNSSReceiver 119
2.85. K-ConstantOfRecordingEquipment 119
2.86. KeyIdentifier 120
2.87. KMWCKey 120
2.88. Language 120
2.89. LastCardDownload 120
2.90. LinkCertificate 120
2.91. L-TyreCircumference 121
2.92. MAC 121
2.93. ManualInputFlag 121
2.94. ManufacturerCode 121
2.95. ManufacturerSpecificEventFaultData 121
2.96. MemberStateCertificate 122
2.97. MemberStateCertificateRecordArray 122
2.98. MemberStatePublicKey 122
2.99. Name 122
2.100. NationAlpha 123
2.101. NationNumeric 123
2.102. NoOfCalibrationRecords 123

2.103. NoOfCalibrationsSinceDownload 123
2.104. NoOfCardPlaceRecords 123
2.105. NoOfCardVehicleRecords 124
2.106. NoOfCardVehicleUnitRecords 124
2.107. NoOfCompanyActivityRecords 124
2.108. NoOfControlActivityRecords 124
2.109. NoOfEventsPerType 124
2.110. NoOfFaultsPerType 124
2.111. NoOfGNSSCDRecords 124
2.112. NoOfSpecificConditionRecords 125
2.113. OdometerShort 125
2.114. OdometerValueMidnight 125
2.115. OdometerValueMidnightRecordArray 125
2.116. OverspeedNumber 125
2.117. PlaceRecord 126
2.118. PreviousVehicleInfo 126
2.119. PublicKey 127
2.120. RecordType 127
2.121. RegionAlpha 128
2.122. RegionNumeric 128
2.123. RemoteCommunicationModuleSerialNumber 129
2.124. RSAKeyModulus 129
2.125. RSAKeyPrivateExponent 129
2.126. RSAKeyPublicExponent 129
2.127. RtmData 129
2.128. SealDataCard 129
2.129. SealDataVu 130
2.130. SealRecord 130
2.131. SensorApprovalNumber 130
2.132. SensorExternalGNSSApprovalNumber 131
2.133. SensorExternalGNSSCoupledRecord 131
2.134. SensorExternalGNSSIdentification 131
2.135. SensorExternalGNSSInstallation 132
2.136. SensorExternalGNSSOSIdentifier 132
2.137. SensorExternalGNSSSCIdentifier 132
2.138. SensorGNSSCouplingDate 133

2.139. SensorGNSSSerialNumber 133
2.140. SensorIdentification 133
2.141. SensorInstallation 133
2.142. SensorInstallationSecData 134
2.143. SensorOSIdentifier 134
2.144. SensorPaired 134
2.145. SensorPairedRecord 135
2.146. SensorPairingDate 135
2.147. SensorSCIdentifier 135
2.148. SensorSerialNumber 135
2.149. Signature 135
2.150. SignatureRecordArray 136
2.151. SimilarEventsNumber 136
2.152. SpecificConditionRecord 136
2.153. SpecificConditions 136
2.154. SpecificConditionType 137
2.155. Speed 137
2.156. SpeedAuthorised 137
2.157. SpeedAverage 138
2.158. SpeedMax 138
2.159. TachographPayload 138
2.160. TachographPayloadEncrypted 138
2.161. TDesSessionKey 138
2.162. TimeReal 139
2.163. TyreSize 139
2.164. VehicleIdentificationNumber 139
2.165. VehicleIdentificationNumberRecordArray 139
2.166. VehicleRegistrationIdentification 139
2.167. VehicleRegistrationNumber 140
2.168. VehicleRegistrationNumberRecordArray 140
2.169. VuAbility 140
2.170. VuActivityDailyData 141
2.171. VuActivityDailyRecordArray 141
2.172. VuApprovalNumber 141
2.173. VuCalibrationData 142
2.174. VuCalibrationRecord 142
2.175. VuCalibrationRecordArray 143

2.176. VuCardIWData 144
2.177. VuCardIWRecord 144
2.178. VuCardIWRecordArray 145
2.179. VuCardRecord 145
2.180. VuCardRecordArray 146
2.181. VuCertificate 146
2.182. VuCertificateRecordArray 146
2.183. VuCompanyLocksData 147
2.184. VuCompanyLocksRecord 147
2.185. VuCompanyLocksRecordArray 148
2.186. VuControlActivityData 148
2.187. VuControlActivityRecord 148
2.188. VuControlActivityRecordArray 149
2.189. VuDataBlockCounter 149
2.190. VuDetailedSpeedBlock 149
2.191. VuDetailedSpeedBlockRecordArray 150
2.192. VuDetailedSpeedData 150
2.193. VuDownloadablePeriod 150
2.194. VuDownloadablePeriodRecordArray 151
2.195. VuDownloadActivityData 151
2.196. VuDownloadActivityDataRecordArray 151
2.197. VuEventData 152
2.198. VuEventRecord 152
2.199. VuEventRecordArray 153
2.200. VuFaultData 154
2.201. VuFaultRecord 154
2.202. VuFaultRecordArray 155
2.203. VuGNSSCDRecord 155
2.204. VuGNSSCDRecordArray 156
2.205. VuIdentification 156
2.206. VuIdentificationRecordArray 157
2.207. VuITSConsentRecord 157
2.208. VuITSConsentRecordArray 158
2.209. VuManufacturerAddress 158
2.210. VuManufacturerName 158
2.211. VuManufacturingDate 158

2.212. VuOverSpeedingControlData 159
2.213. VuOverSpeedingControlDataRecordArray 159
2.214. VuOverSpeedingEventData 159
2.215. VuOverSpeedingEventRecord 159
2.216. VuOverSpeedingEventRecordArray 160
2.217. VuPartNumber 161
2.218. VuPlaceDailyWorkPeriodData 161
2.219. VuPlaceDailyWorkPeriodRecord 161
2.220. VuPlaceDailyWorkPeriodRecordArray 162
2.221. VuPrivateKey 162
2.222. VuPublicKey 162
2.223. VuSerialNumber 162
2.224. VuSoftInstallationDate 162
2.225. VuSoftwareIdentification 163
2.226. VuSoftwareVersion 163
2.227. VuSpecificConditionData 163
2.228. VuSpecificConditionRecordArray 163
2.229. VuTimeAdjustmentData 164
2.230. VuTimeAdjustmentGNSSRecord 164
2.231. VuTimeAdjustmentGNSSRecordArray 164
2.232. VuTimeAdjustmentRecord 165
2.233. VuTimeAdjustmentRecordArray 165
2.234. WorkshopCardApplicationIdentification 166
2.235. WorkshopCardCalibrationData 166
2.236. WorkshopCardCalibrationRecord 167
2.237. WorkshopCardHolderIdentification 168
2.238. WorkshopCardPIN 168
2.239. W-VehicleCharacteristicConstant 169
2.240. VuPowerSupplyInterruptionRecord 169
2.241. VuPowerSupplyInterruptionRecordArray 169
2.242. VuSensorExternalGNSSCoupledRecordArray 170
2.243. VuSensorPairedRecordArray 170
3. DEFINITIONEN FÜR WERT- UND GRÖSSENBEREICHE 171
4. ZEICHENSÄTZE 171
5. KODIERUNG 171
6. OBJEKTKENNUNGEN UND ANWENDUNGSBEZEICHNER 171
6.1. Objektkennungen 171
6.2. Anwendungskennungen 172

1. EINLEITUNG

Diese Anlage enthält die Spezifizierung der zur Verwendung im Kontrollgerät und auf den Fahrtenschreiberkarten vorgesehenen Datenformate, -elemente und -strukturen.

1.1. Grundlage für die Definition von Datentypen

Die Definition der Datentypen in dieser Anlage beruht auf der Abstract Syntax Notation One (ASN.1), da es auf diese Weise möglich ist, einfache und strukturierte Daten ohne Implizierung einer spezifischen, anwendungs- und umgebungsabhängigen Transfersyntax (Kodierungsregeln) festzulegen.

Die ASN.1-Typbenennungskonventionen werden gemäß ISO/IEC 8824-1 verwendet. Das heißt:

— In den gewählten Benennungen ist soweit möglich die Bedeutung des Datentyps implizit erkennbar.

— Handelt es sich bei einem Datentyp um eine Zusammensetzung aus anderen Datentypen, ist die Datentypbenennung zwar weiterhin eine Folge von alphabetischen Zeichen, die mit einem Großbuchstaben beginnen, doch werden innerhalb der Benennung Großbuchstaben verwendet, um die entsprechende Bedeutung zu vermitteln.

— Generell stehen die Datentypbenennungen in Beziehung zu den Benennungen der Datentypen, aus denen sie aufgebaut sind, zu dem Gerät, in denen die Daten gespeichert werden, und zu der mit den Daten verbundenen Funktion.

Ist ein ASN.1-Typ bereits im Rahmen einer anderen Norm definiert und für den Gebrauch im Kontrollgerät von Bedeutung, wird dieser ASN.1-Typ in dieser Anlage definiert.

Um mehrere Arten von Kodierungsregeln zu ermöglichen, sind einige ASN.1-Typen dieser Anlage mit Wertbereichsbezeichnern versehen, die in Abschnitt 3 und Anlage 2 definiert sind.

1.2. Referenzdokumente

In dieser Anlage werden folgende Referenzdokumente herangezogen:

ISO 639	Code for the representation of names of languages. First Edition: 1988.
ISO 3166	Codes for the representation of names of countries and their subdivisions — Part 1: Country codes, 2013.
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. 2009.
ISO/IEC 7816-5	Identification cards — Integrated circuit cards — Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. 2003.

ISO 16844-3 Road vehicles — Tachograph systems — Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006.

TR-03110-3 BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token — Part 3 Common Specifications, Version 2.20, 3. Februar 2015.

2. DATENTYPDEFINITIONEN

Bei allen folgenden Datentypen besteht der Standardwert für einen „unbekannten“ oder einen „nicht zutreffenden“ Inhalt in der Ausfüllung des Datenelements mit „FF“-Bytes.

Sofern nicht anders angegeben, werden alle Datentypen für Anwendungen der 1. Generation und 2. Generation verwendet.

2.1. **ActivityChangeInfo**

Mit diesem Datentyp ist es möglich, den Steckplatz- und Fahrerstatus um 0.00 Uhr und für einen Fahrer oder einen Beifahrer Tätigkeitsänderungen und/oder Veränderungen des Status der Fahrzeugführung und/oder Veränderungen des Kartenstatus innerhalb eines Zwei-Byte-Wortes zu kodieren. Dieser Datentyp bezieht sich auf Anhang 1C Randnummern 105, 266, 291, 320, 321, 343 und 344.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Wertzuweisung — Oktettanordnung: ‘scpaatttttttttt’B (16 Bit)

Für Aufzeichnungen im Massenspeicher (oder den Steckplatz-Status):

‘s’B Slot:

‘0’B: FAHRER,

‘1’B: BEIFAHRER,

‘c’B Status der Fahrzeugführung:

‘0’B: EINMANNBETRIEB,

‘1’B: TEAM,

‘p’B Status der Fahrerkarte (oder Werkstattkarte) im entsprechenden Steckplatz:

‘0’B: EINGESTECKT, eine Karte ist eingesteckt,

‘1’B: NICHT EINGESTECKT, keine Karte eingesteckt (oder Karte entnommen),

‘aa’B Tätigkeit:

‘00’B: UNTERBRECHUNG/RUHE,

‘01’B: BEREITSCHAFT,

‘10’B: ARBEIT,

‘11’B: LENKEN,

‘ttttttttttt’B Zeitpunkt der Veränderung: Anzahl der Minuten seit 0.00 Uhr an diesem Tag.

Für Aufzeichnungen auf der Fahrerkarte (oder Werkstattkarte) (und den Fahrerstatus):

's'B	Steckplatz (nicht von Belang, wenn 'p' = 1. Ausnahmebedingung siehe Anmerkung):
	'0'B: FAHRER,
	'1'B: BEIFAHRER,
'c'B	Status der Fahrzeugführung (Fall 'p' = 0) oder
	Status der Folgetätigkeit (Fall 'p' = 1):
	'0'B: EINMANNBETRIEB,
	'0'B: UNBEKANNT
	'1'B: TEAM,
	'1'B: BEKANNT (= manuell eingegeben)
'p'B	Kartenstatus:
	'0'B: EINGESTECKT, Karte ist in ein Kontrollgerät eingesteckt,
	'1'B: NICHT EINGESTECKT, keine Karte eingesteckt (oder Karte entnommen),
'aa'B	Tätigkeit (nicht von Belang, wenn 'p' = 1 und 'c' = 0. Ausnahmebedingung siehe Anmerkung):
	'00'B: UNTERBRECHUNG/RUHE,
	'01'B: BEREITSCHAFT,
	'10'B: ARBEIT,
	'11'B: LENKEN,
'ttttttttttt'B	Zeitpunkt der Veränderung: Anzahl der Minuten seit 0.00 Uhr an diesem Tag.

Anmerkung für den Fall „Kartenentnahme":

Wenn die Karte entnommen wurde, gilt Folgendes:

— 's' ist relevant und gibt den Steckplatz an, aus dem die Karte entnommen wurde,

— 'c' muss auf 0 gesetzt sein,

— 'p' muss auf 1 gesetzt sein,

— 'aa' muss die zu dieser Zeit gewählte laufende Tätigkeit kodieren.

Infolge eines manuellen Eintrags können die (auf der Karte gespeicherten) Bits 'c' und 'aa' des Worts später zur Berücksichtigung des Eintrags überschrieben werden.

2.2. **Address**

Eine Adresse.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage gibt einen in Kapitel 4 definierten Zeichensatz an,

address ist eine mit dem angegebenen Zeichensatz kodierte Adresse.

2.3. **AESKey**

2. Generation:

Ein AES-Schlüssel mit einer Länge von 128, 192 oder 256 Bit.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Wertzuweisung: nicht näher spezifiziert.

2.4. **AES128Key**

2. Generation:

Ein AES128-Schlüssel.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length bezeichnet die Länge des AES128-Schlüssel in Oktetten.

aes128Key ist ein AES-Schlüssel mit einer Länge von 128 Bit.

Wertzuweisung:

Der Wert für die Länge beträgt 16.

2.5. **AES192Key**

2. Generation:

Ein AES192-Schlüssel.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length bezeichnet die Länge des AES192-Schlüssel in Oktetten.

aes192Key ist ein AES-Schlüssel mit einer Länge von 192 Bit.

Wertzuweisung:

Der Wert für die Länge beträgt 24.

2.6. **AES256Key**

2. Generation:

Ein AES256-Schlüssel.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length bezeichnet die Länge des AES256-Schlüssel in Oktetten.

aes256Key ist ein AES-Schlüssel mit einer Länge von 256 Bit.

Wertzuweisung:

Der Wert für die Länge beträgt 32.

2.7. **BCDString**

BCDString wird für die Darstellung von binär kodierten Dezimalzahlen (BCD) angewendet. Dieser Datentyp dient der Darstellung einer Dezimalziffer in einer 4-Bit-Gruppe. BCDString basiert auf „CharacterStringType“ der ISO/IEC 8824-1.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString verwendet eine „hstring“-Notation. Die äußerste linke Hexadezimalziffer ist die höchstwertige 4-Bit-Gruppe des ersten Oktetts. Um ein Vielfaches der Oktette zu erhalten, werden nach Bedarf von der Position der äußersten linken 4-Bit-Gruppe im ersten Oktett 4-Bit-Gruppen mit rechtsstehenden Nullen eingefügt.

Zulässige Ziffern: 0, 1, … 9.

2.8. **CalibrationPurpose**

Code zur Erläuterung, warum ein bestimmter Satz von Kalibierungsparametern aufgezeichnet wurde. Dieser Datentyp bezieht sich auf Anhang 1B Randnummern 097 und 098 und Anhang 1C Randnummer 119.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Wertzuweisung:

1. Generation:

‘00’H	reservierter Wert,
‘01’H	Aktivierung: Aufzeichnung von bekannten Kalibrierungsparametern zum Zeitpunkt der VU-Aktivierung,
‘02’H	Ersteinbau: Erste Kalibrierung der VU nach ihrer Aktivierung,
‘03’H	Einbau: Erste Kalibrierung der VU im derzeitigen Fahrzeug,
‘04’H	Regelmäßige Nachprüfung

2. Generation:

Zusätzlich zur 1. Generation werden folgende Werte genutzt:

‘05’H Eingabe des amtlichen Kennzeichens nach Unternehmen,

‘06’H Zeitanpassung ohne Kalibrierung,

‘07’H bis ‘7F’H RFU,

‘80’H bis ‘FF’H Herstellerspezifisch.

2.9. **CardActivityDailyRecord**

Auf einer Karte gespeicherte Informationen zu den Fahrertätigkeiten an einem bestimmten Kalendertag. Dieser Datentyp bezieht sich auf Anhang 1C Randnummern 266, 291, 320 und 343.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength — Gesamtlänge des vorherigen Tagesdatensatzes in Byte. Der Höchstwert wird durch die Länge des OCTET STRING angegeben, der diese Datensätze enthält (siehe CardActivityLengthRange, Anlage 2 Abschnitt 4). Ist dieser Datensatz der älteste Tagesdatensatz, muss der Wert von activityPreviousRecordLength auf 0 gesetzt werden.

activityRecordLength — Gesamtlänge dieses Datensatzes in Byte. Der Höchstwert wird durch die Länge des OCTET STRING angegeben, der diese Datensätze enthält.

activityRecordDate — Datum des Datensatzes.

activityDailyPresenceCounter –Tagesanwesenheitszähler für die Karte an diesem Tag.

activityDayDistance — die an diesem Tag zurückgelegte Gesamtwegstrecke.

activityChangeInfo –Menge der ActivityChangeInfo-Daten für den Fahrer an diesem Tag. Kann maximal 1440 Werte enthalten (1 Tätigkeitsänderung je Minute). Dieser Datensatz enthält stets auch den ActivityChangeInfo-Wert für den Fahrerstatus um 0.00 Uhr.

2.10. **CardActivityLengthRange**

Anzahl der Bytes auf einer Fahrer- oder Werkstattkarte, die für die Speicherung von Datensätzen zur Fahrertätigkeit zur Verfügung stehen.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.11. **CardApprovalNumber**

Typgenehmigungsnummer der Karte.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Wertzuweisung:

Die Genehmigungsnummer muss derjenigen entsprechen, die auf der zugehörigen Website der Europäischen Kommission veröffentlicht ist, und beispielsweise etwaige Bindestriche berücksichtigen. Die Genehmigungsnummer muss linksbündig ausgerichtet sein.

2.12. **CardCertificate**

1. Generation:

Zertifikat des öffentlichen Schlüssels einer Karte.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Auf einer Karte gespeicherte Information zur Identifizierung des integrierten Schaltkreises (IS) der Karte (Anhang 1C Randnummer 249). Anhand der icSerialNumber gemeinsam mit den icManufacturingReferences wird der Kartenchip eindeutig identifiziert. Mit der icSerialNumber allein ist eine eindeutige Identifizierung des Kartenchips nicht möglich.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber ist die IS-Seriennummer.

icManufacturingReferences ist der spezifische IS-Herstellerbezeichner.

2.14. **CardConsecutiveIndex**

Fortlaufender Kartenindex (Begriffsbestimmung h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Wertzuweisung: (siehe Anlage 1C Kapitel 7)

Reihenfolge für die Erhöhung: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information über die letzte Kontrolle, welcher der Fahrer unterzogen wurde (Anhang 1C Randnummern 274, 299, 327 und 350).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType — Art der Kontrolle.

controlTime — Datum und Uhrzeit der Kontrolle.

controlCardNumber — FullCardNumber des ausführenden Kontrolleurs.

controlVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Kontrolle stattfand.

controlDownloadPeriodBegin und **controlDownloadPeriodEnd** — übertragener Zeitraum bei Übertragungen.

2.16. CardCurrentUse

Information über die aktuelle Benutzung der Karte (Anhang 1C Randnummern 273, 298, 326 und 349).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime — Uhrzeit, zu der die Karte für die aktuelle Benutzung eingesteckt wird. Bei Kartenentnahme wird dieses Element auf null gesetzt.

sessionOpenVehicle — Kennung des derzeit gefahrenen Fahrzeugs, gesetzt beim Einstecken der Karte. Bei Kartenentnahme wird dieses Element auf null gesetzt.

2.17. CardDriverActivity

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information über die Tätigkeiten des Fahrers (Anhang 1C Randnummern 267, 268, 292, 293, 321 und 344).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord — Angabe des Beginns des Speicherortes (Anzahl der Bytes vom Anfang des Strings) des ältesten vollständigen Tagesdatensatzes im String activityDailyRecords. Der Höchstwert ist durch die Länge des Strings gegeben.

activityPointerNewestRecord — Angabe des Beginns des Speicherortes (Anzahl der Bytes vom Anfang des Strings) des jüngsten vollständigen Tagesdatensatzes im String activityDailyRecords. Der Höchstwert ist durch die Länge des Strings gegeben.

activityDailyRecords — der für die Fahrertätigkeitsdaten zur Verfügung stehende Speicherplatz (Datenstruktur: CardActivityDailyRecord) für jeden Kalendertag, an dem die Karte benutzt wurde.

Wertzuweisung: Dieser Oktettstring wird zyklisch mit CardActivityDailyRecord-Datensätzen gefüllt. Bei der ersten Benutzung beginnt die Speicherung beim ersten Byte des Strings. Alle neuen Datensätze werden am Ende des vorigen angefügt. Ist der String voll, wird die Speicherung am ersten Byte des Strings unabhängig davon fortgesetzt, ob es innerhalb eines Datenelements zu einem Bruch kommt. Bevor (zur Vergrößerung des aktuellen activityDailyRecord oder zum Einsetzen eines neuen activityDailyRecord) neue Tätigkeitsdaten in den String gesetzt werden, die ältere Tätigkeitsdaten ersetzen, muss activityPointerOldestDayRecord aktualisiert werden, um den neuen Platz des ältesten vollständigen Tagesdatensatzes auszuweisen, und activityPreviousRecordLength dieses (neuen) ältesten vollständigen Tagesdatensatzes muss auf 0 zurückgesetzt werden.

2.18. CardDrivingLicenceInformation

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Führerscheindaten des Karteninhabers (Anhang 1C Randnummern 259 und 284).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority — die für die Ausstellung des Führerscheins zuständige Behörde.

drivingLicenceIssuingNation — Nationalität der Ausstellungsbehörde des Führerscheins.

drivingLicenceNumber — Nummer des Führerscheins.

2.19. **CardEventData**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Ereignissen im Zusammenhang mit dem Karteninhaber (Anhang 1C Randnummern 260, 285, 318 und 341).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData — eine nach absteigendem Wert von EventFaultType geordnete Folge von cardEventRecords (mit Ausnahme von Versuchen der Sicherheitsverletzung, die in der letzten Gruppe der Folge zusammengefasst sind).

cardEventRecords — Ereignisdatensätze einer bestimmten Ereignisart (oder Kategorie bei Ereignissen Versuch Sicherheitsverletzung).

2.20. **CardEventRecord**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu einem Ereignis im Zusammenhang mit dem Karteninhaber (Anhang 1C Randnummern 261, 286, 318 und 341).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType — Art des Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

eventVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem das Ereignis eingetreten ist.

2.21. **CardFaultData**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Störungen im Zusammenhang mit dem Karteninhaber (Anhang 1C Randnummern 263, 288, 318 und 341).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData — eine Folge von Datensätzen mit Kontrollgerätstörungen, gefolgt von Datensätzen mit Kartenfehlfunktionen.

cardFaultRecords — Störungsdatensätze einer bestimmten Störungskategorie (Kontrollgerät oder Karte).

2.22. **CardFaultRecord**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu einer Störung im Zusammenhang mit dem Karteninhaber (Anhang 1C Randnummern 264, 289, 318 und 341).

```
CardFaultRecord ::= SEQUENCE {
   faultType                        EventFaultType,
   faultBeginTime                   TimeReal,
   faultEndTime                     TimeReal,
   faultVehicleRegistration         VehicleRegistrationIdentification
}
```

faultType — Art der Störung.

faultBeginTime — Datum und Uhrzeit des Störungsbeginns.

faultEndTime — Datum und Uhrzeit des Störungsendes.

faultVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Störung auftrat.

2.23. **CardIccIdentification**

Auf einer Karte gespeicherte Information zur Identifizierung der Karte des integrierten Schaltkreises (IS) (Anhang 1C Randnummer 248).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                        OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber         ExtendedSerialNumber,
   cardApprovalNumber               CardApprovalNumber,
   cardPersonaliserID               ManufacturerCode,
   embedderIcAssemblerId            EmbedderIcAssemblerId,
   icIdentifier                     OCTET STRING (SIZE(2))
}
```

clockStop — Clockstop-Modus laut Definition in Anlage 2.

cardExtendedSerialNumber — eindeutige Seriennummer der IS-Karte gemäß weiterer Spezifikation durch den Datentyp ExtendedSerialNumber.

cardApprovalNumber –Typgenehmigungsnummer der Karte.

cardPersonaliserID — Karten-Personaliser-ID kodiert als ManufacturerCode.

embedderIcAssemblerId — enthält Informationen zum Kartenhersteller/IS-Assembler.

icIdentifier — Bezeichner des IS auf der Karte und des IS-Herstellers laut Definition in ISO/IEC 7816-6.

2.24. **CardIdentification**

Auf der Karte gespeicherte Information zur Identifikation der Karte (Anhang 1C Randnummern 255, 280, 310, 333, 359, 365, 371 und 377).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState — Code des Mitgliedstaates, der die Karte ausgestellt hat.

cardNumber — Kartennummer.

cardIssuingAuthorityName — Name der Behörde, die die Karte ausgestellt hat.

cardIssueDate — Datum der Ausstellung der Karte an den derzeitigen Inhaber.

cardValidityBegin — Datum, an dem die Gültigkeit der Karte beginnt.

cardExpiryDate — Datum, an dem die Gültigkeit der Karte abläuft.

2.25. CardMACertificate

2. Generation:

Zertifikat des öffentlichen Schlüssels der Karte zur gegenseitigen Authentisierung mit einer VU. Die Struktur dieses Zertifikats ist in Anlage 11 spezifiziert.

```
CardMACertificate ::= Certificate
```

2.26. CardNumber

Kartennummer nach Begriffsbestimmung g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification — eindeutige Kennung eines Fahrers in einem Mitgliedstaat.

ownerIdentification — eindeutige Kennung eines Unternehmens oder einer Werkstatt oder einer Kontrollstelle in einem Mitgliedstaat.

cardConsecutiveIndex — fortlaufender Kartenindex.

cardReplacementIndex — Kartenersatzindex.

cardRenewalIndex — Kartenerneuerungsindex.

Die erste Folge der Auswahl eignet sich zur Kodierung einer Fahrerkartennummer, die zweite Folge zur Kodierung der Werkstatt-, Kontroll- und Unternehmenskartennummer.

2.27. **CardPlaceDailyWorkPeriod**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zum Ort des Beginns und/oder des Endes des Arbeitstages (Anhang 1C Randnummern 272, 297, 325 und 348).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord — Index des zuletzt aktualisierten Ortsdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Ortsdatensatzes entspricht, beginnend mit '0' für das erste Auftreten der Ortsdatensätze in der Struktur.

placeRecords — Datensätze mit Informationen zu den eingegebenen Orten.

2.28. **CardPrivateKey**

1. Generation:

Der private Schlüssel einer Karte.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Der öffentliche Schlüssel einer Karte.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Ein Kartenerneuerungsindex (Begriffsbestimmung i)).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Wertzuweisung: (siehe Kapitel VII in diesem Anhang).

'0' Erstausstellung.

Reihenfolge für die Erhöhung: '0, …, 9, A, …, Z'

2.31. **CardReplacementIndex**

Ein Kartenersatzindex (Begriffsbestimmung j)).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Wertzuweisung: (siehe Kapitel VII in diesem Anhang).

'0' Originalkarte.

Reihenfolge für die Erhöhung: '0, …, 9, A, …, Z'

2.32. **CardSignCertificate**

2. Generation:

Zertifikat des öffentlichen Schlüssels einer Karte zur Signatur. Die Struktur dieses Zertifikats ist in Anlage 11 spezifiziert.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Code zur Unterscheidung der beiden Steckplätze einer Fahrzeugeinheit.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Wertzuweisung: nicht näher spezifiziert.

2.34. **CardSlotsStatus**

Code zur Angabe der in den beiden Steckplätzen der Fahrzeugeinheit eingesteckten Kartenarten.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Wertzuweisung — Oktettanordnung: 'ccccdddd'B

'cccc'B Identifizierung der im Steckplatz Beifahrer befindlichen Kartenart,

'dddd'B Identifizierung der im Steckplatz Fahrer befindlichen Kartenart,

mit folgenden Codes:

'0000'B keine Karte eingesteckt,

'0001'B Fahrerkarte eingesteckt,

'0010'B Werkstattkarte eingesteckt,

'0011'B Kontrollkarte eingesteckt,

'0100'B Unternehmenskarte eingesteckt.

2.35. **CardSlotsStatusRecordArray**

2. Generation:

CardSlotsStatus und im Download-Protokoll verwendete Metadaten.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType — Art des Datensatzes (CardSlotsStatus). **Wertzuweisung**: siehe RecordType

recordSize — die Größe des CardSlotsStatus in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der CardSlotsStatus-Datensätze.

2.36. **CardStructureVersion**

Code zur Angabe der Version der auf einer Fahrtenschreiberkarte implementierten Struktur.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Wertzuweisung: 'aabb'H:

'aa'H Index für Änderungen der Struktur.

'00'H für Anwendungen der 1. Generation

'01'H für Anwendungen der 2. Generation

'bb'H Index für Änderungen im Zusammenhang mit dem Gebrauch der Datenelemente, die für die vom oberen Byte gegebenen Struktur definiert sind.

'00'H für diese Version der Anwendungen der 1. Generation

'00'H für diese Version der Anwendungen der 2. Generation

2.37. **CardVehicleRecord**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zur Einsatzzeit eines Fahrzeugs an einem Kalendertag (Anhang 1C Randnummern 269, 294, 322 und 345).

1. Generation:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin — Kilometerstand zu Beginn der Einsatzzeit des Fahrzeugs.

vehicleOdometerEnd — Kilometerstand am Ende der Einsatzzeit des Fahrzeugs.

vehicleFirstUse — Datum und Uhrzeit des Beginns der Einsatzzeit des Fahrzeugs.

vehicleLastUse — Datum und Uhrzeit des Endes der Einsatzzeit des Fahrzeugs.

vehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs.

vuDataBlockCounter — Wert des VuDataBlockCounter beim letzten Auszug der Einsatzzeit des Fahrzeugs.

2. Generation:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Zusätzlich zur 1. Generation wird folgendes Datenelement verwendet:

VehicleIdentificationNumber — die Fahrzeugidentifizierungsnummer mit Bezug auf das Fahrzeug insgesamt.

2.38. **CardVehiclesUsed**

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den vom Karteninhaber gefahrenen Fahrzeugen (Anhang 1C Randnummern 270, 295, 323 und 346).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord — Index des zuletzt aktualisierten Fahrzeugdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Fahrzeugdatensatzes entspricht, beginnend mit '0' für das erste Auftreten der Fahrzeugdatensätze in der Struktur.

cardVehicleRecords — Datensätze mit Informationen zu den gefahrenen Fahrzeugen.

2.39. **CardVehicleUnitRecord**

2. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu der verwendeten Fahrzeugeinheit (Anhang 1C Randnummern 303 und 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp — Beginn der Einsatzzeit der Fahrzeugeinheit (d. h. erstes Karteneinstecken in die Fahrzeugeinheit für diesen Zeitraum).

manufacturerCode — Name des Herstellers der Fahrzeugeinheit.

deviceID — Identifizierung des Typs der Fahrzeugeinheit eines Herstellers. Der Wert ist herstellerspezifisch.

vuSoftwareVersion — Softwareversionsnummer der Fahrzeugeinheit.

2.40. **CardVehicleUnitsUsed**

2. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den vom Karteninhaber gefahrenen Fahrzeugeinheiten (Anhang 1C Randnummern 306 und 352).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord — Index des zuletzt aktualisierten Datensatzes für die Fahrzeugeinheit.

Wertzuweisung: Zahl, die dem Zähler des Datensatzes der Fahrzeugeinheit entspricht, beginnend mit '0' für das erste Auftreten der Datensätze der Fahrzeugeinheit in der Struktur.

cardVehicleUnitRecords — Datensätze mit Informationen zu den genutzten Fahrzeugeinheiten.

2.41. Certificate

Das von einer Zertifizierungsstelle ausgestellte Zertifikat eines öffentlichen Schlüssels.

1. Generation:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Wertzuweisung: digitale Signatur mit teilweiser Wiederherstellung eines CertificateContent gemäß Anlage 11 „Gemeinsame Sicherheitsmechanismen": Signature (128 Byte) || Public Key remainder (58 Byte) || Certification Authority Reference (8 Byte).

2. Generation:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Wertzuweisung: siehe Anlage 11

2.42. CertificateContent

1. Generation:

Der (Klartext-) Inhalt des Zertifikats eines öffentlichen Schlüssels gemäß Anlage 11 „Gemeinsame Sicherheitsmechanismen".

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier — Version des entsprechenden Zertifikats.

Wertzuweisung: '01h' für diese Version.

certificationAuthorityReference identifiziert die das Zertifikat ausstellende Zertifizierungsstelle. und enthält darüber hinaus einen Verweis auf den öffentlichen Schlüssel dieser Zertifizierungsstelle.

certificateHolderAuthorisation identifiziert die Rechte des Zertifikatsinhabers.

certificateEndOfValidity — Datum, an dem die Gültigkeit des Zertifikats administrativ endet.

certificateHolderReference identifiziert den Zertifikatsinhaber. und enthält zugleich einen Verweis auf dessen öffentlichen Schlüssel.

publicKey — der öffentliche Schlüssel, der durch dieses Zertifikat zertifiziert wird.

2.43. **CertificateHolderAuthorisation**

Identifizierung der Rechte eines Zertifikatsinhabers.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

1. Generation:

tachographApplicationID — Anwendungsbezeichner für die Kontrollgerätanwendung.

Wertzuweisung: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Dieser AID ist ein proprietärer nichtregistrierter Anwendungsbezeichner gemäß ISO/IEC 7816-5.

equipmentType ist die Kennung des Gerätetyps, für den das Zertifikat bestimmt ist.

Wertzuweisung: entsprechend dem Datentyp EquipmentType. **0**, wenn es sich um ein Zertifikat eines Mitgliedstaates handelt.

2. Generation:

tachographApplicationID bezeichnet die 6 höchstwertigen Bytes des zugehörigen Anwendungsbezeichners (Application Identifier, AID) der Fahrtenschreiberkarte der 2. Generation. Der AID für die Fahrtenschreiberkartenanwendung ist in Kapitel 6.2 spezifiziert.

Wertzuweisung: 'FF 53 4D 52 44 54'.

equipmentType — ist die Kennung des für die 2. Generation angegebenen Gerätetyps, für den das Zertifikat bestimmt ist.

Wertzuweisung: entsprechend dem Datentyp EquipmentType.

2.44. **CertificateRequestID**

Eindeutige Kennung eines Zertifikatsantrags. Kann auch als Bezeichner des öffentlichen Schlüssels einer Fahrzeugeinheit verwendet werden, wenn die Seriennummer der Fahrzeugeinheit, für die der Schlüssel bestimmt ist, zum Zeitpunkt der Erzeugung des Zertifikats nicht bekannt ist.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber — einmalige Seriennummer des Zertifikatsantrags für den im Folgenden angegebenen Hersteller und Monat.

requestMonthYear — Kennung für den Monat und das Jahr des Zertifikatsantrags.

Wertzuweisung: BCD-Kodierung des Monats (zwei Stellen) und des Jahres (die beiden letzten Stellen).

crIdentifier — Bezeichner zur Unterscheidung eines Zertifikatsantrags von einer erweiterten Seriennummer.

Wertzuweisung: 'FFh'.

manufacturerCode — numerischer Code des Herstellers, der das Zertifikat beantragt.

2.45. **CertificationAuthorityKID**

Bezeichner des öffentlichen Schlüssels einer Zertifizierungsstelle (Mitgliedstaatliche Stelle oder Europäische Zertifizierungsstelle).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric — numerischer Landescode der Zertifizierungsstelle.

nationAlpha — alphanumerischer Landescode der Zertifizierungsstelle.

keySerialNumber — eine Seriennummer zur Unterscheidung der verschiedenen Schlüssel der Zertifizierungsstelle für den Fall des Wechsels von Schlüsseln.

additionalInfo — 2-Byte-Feld für Zusatzkodierung (je nach Zertifizierungsstelle).

caIdentifier — Bezeichner zur Unterscheidung des Schlüsselbezeichners einer Zertifizierungsstelle von anderen Schlüsselbezeichnern.

Wertzuweisung: '01h'.

2.46. **CompanyActivityData**

Auf einer Unternehmenskarte gespeicherte Information zu den mit der Karte ausgeführten Tätigkeiten (Anhang 1C Randnummern 373 und 379).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord         INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords             SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord              SEQUENCE {
     companyActivityType                CompanyActivityType,
     companyActivityTime                TimeReal,
     cardNumberInformation              FullCardNumber,
     vehicleRegistrationInformation     VehicleRegistrationIdentification,
     downloadPeriodBegin                TimeReal,
     downloadPeriodEnd                  TimeReal
    }
}
```

companyPointerNewestRecord — Index des zuletzt aktualisierten companyActivityRecord.

Wertzuweisung: Zahl, die dem Zähler des Unternehmenstätigkeitsdatensatzes entspricht, beginnend mit '0' für das erste Auftreten des Unternehmenstätigkeitsdatensatzes in der Struktur.

companyActivityRecords — sämtliche Unternehmenstätigkeitsdatensätze.

companyActivityRecord — Folge von Informationen zu einer Unternehmenstätigkeit.

companyActivityType — Art der Unternehmenstätigkeit.

companyActivityTime — Datum und Uhrzeit der Unternehmenstätigkeit.

cardNumberInformation — gegebenenfalls Kartennummer und ausstellender Mitgliedstaat der heruntergeladenen Karte.

vehicleRegistrationInformation — amtliches Kennzeichen und zulassender Mitgliedstaat des heruntergeladenen bzw. des gesperrten oder entsperrten Fahrzeugs.

downloadPeriodBegin und **downloadPeriodEnd** — gegebenenfalls der von der VU heruntergeladene Zeitraum.

2.47. **CompanyActivityType**

Code für die von einem Unternehmen unter Nutzung seiner Unternehmenskarte ausgeführte Tätigkeit.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Auf einer Unternehmenskarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Anhang 1C Randnummern 369 und 375).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion gibt die Version der auf der Karte implementierten Struktur an.

noOfCompanyActivityRecords Anzahl der Unternehmenstätigkeitsdatensätze, die die Karte speichern kann.

2.49. **CompanyCardHolderIdentification**

Auf einer Unternehmenskarte gespeicherte Information zur Identifizierung des Karteninhabers (Anhang 1C Randnummern 372 und 378).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName — Name des Unternehmens, dem die Karte gehört.

companyAddress — Anschrift des Unternehmens, dem die Karte gehört.

cardHolderPreferredLanguage — bevorzugte Sprache des Karteninhabers.

2.50. **ControlCardApplicationIdentification**

Auf einer Kontrollkarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Anhang 1C Randnummern 357 und 363).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion — gibt die Version der auf der Karte implementierten Version der Struktur an.

noOfControlActivityRecords — Anzahl der Kontrolltätigkeitsdatensätze, die die Karte speichern kann.

2.51. **ControlCardControlActivityData**

Auf einer Kontrollkarte gespeicherte Information zur mit der Karte durchgeführten Kontrolltätigkeit (Anhang 1C Randnummern 361 und 367).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
     controlType                       ControlType,
     controlTime                       TimeReal,
     controlledCardNumber              FullCardNumber,
     controlledVehicleRegistration     VehicleRegistrationIdentification,
     controlDownloadPeriodBegin        TimeReal,
     controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord — Index des zuletzt aktualisierten Kontrolltätigkeitsdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Kontrolltätigkeitsdatensatzes entspricht, beginnend mit '0' für das erste Auftreten des Kontrolltätigkeitsdatensatzes in der Struktur.

controlActivityRecords — sämtliche Kontrolltätigkeitsdatensätze.

controlActivityRecord — Folge von Informationen zu einer Kontrolle.

controlType — Art der Kontrolle.

controlTime — Datum und Uhrzeit der Kontrolle.

controlledCardNumber — Kartennummer und ausstellender Mitgliedstaat der kontrollierten Karte.

controlledVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Kontrolle stattfand.

controlDownloadPeriodBegin und **controlDownloadPeriodEnd** — heruntergeladener Zeitraum.

2.52. **ControlCardHolderIdentification**

Auf einer Kontrollkarte gespeicherte Information zur Identifizierung des Karteninhabers (Anhang 1C Randnummern 360 und 366).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                   Name,
   controlBodyAddress                Address,
   cardHolderName                    HolderName,
   cardHolderPreferredLanguage       Language
}
```

controlBodyName — Name der Kontrollstelle des Karteninhabers.

controlBodyAddress — Anschrift der Kontrollstelle des Karteninhabers.

cardHolderName — Name und Vorname(n) des Inhabers der Kontrollkarte.

cardHolderPreferredLanguage — bevorzugte Sprache des Karteninhabers.

2.53. **ControlType**

Code zur Angabe der bei einer Kontrolle ausgeführten Aktivitäten. Dieser Datentyp bezieht sich auf Anhang 1C Randnummern 126, 274, 299, 327 und 350.

```
ControlType ::= OCTET STRING (SIZE(1))
```

1. Generation:

Wertzuweisung — Oktettanordnung: 'cvpdxxxx'B (8 Bit)

'c'B Herunterladen der Karte:

'0'B: Karte bei dieser Kontrollaktivität nicht heruntergeladen,

'1'B: Karte bei dieser Kontrollaktivität heruntergeladen

'v'B Herunterladen der VU:

'0'B: VU bei dieser Kontrollaktivität nicht heruntergeladen,

'1'B: VU bei dieser Kontrollaktivität heruntergeladen

'p'B Drucken:

'0'B: kein Drucken bei dieser Kontrollaktivität,

'1'B: Drucken bei dieser Kontrollaktivität

'd'B Anzeige:

'0'B: keine Anzeige bei dieser Kontrollaktivität verwendet,

'1'B: Anzeige bei dieser Kontrollaktivität verwendet

'xxxx'B Nichtverwendung.

2. Generation:

Wertzuweisung — Oktettanordnung: 'cvpdexxx'B (8 Bit)

'c'B Herunterladen der Karte:

'0'B: Karte bei dieser Kontrollaktivität nicht heruntergeladen,

'1'B: Karte bei dieser Kontrollaktivität heruntergeladen

'v'B Herunterladen der VU:

'0'B: VU bei dieser Kontrollaktivität nicht heruntergeladen,

'1'B: VU bei dieser Kontrollaktivität heruntergeladen

'p'B Drucken:

'0'B: kein Drucken bei dieser Kontrollaktivität,

'1'B: Drucken bei dieser Kontrollaktivität

'd'B Anzeige:

'0'B: keine Anzeige bei dieser Kontrollaktivität verwendet,

'1'B: Anzeige bei dieser Kontrollaktivität verwendet

'e'B	Kalibrierungskontrolle unterwegs:
	'0'B: Kalibrierungsparameter bei dieser Kontrollaktivität nicht überprüft,
	'1'B: Kalibrierungsparameter bei dieser Kontrollaktivität überprüft
'xxx'B	RFU.

2.54. **CurrentDateTime**

Aktuelles Datum und aktuelle Uhrzeit des Kontrollgeräts.

```
CurrentDateTime ::= TimeReal
```

Wertzuweisung: nicht näher spezifiziert.

2.55. **CurrentDateTimeRecordArray**

2. Generation:

Datum und Uhrzeit plus im Download-Protokoll verwendete Metadaten.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType — Art des Datensatzes (CurrentDateTime). **Wertzuweisung**: siehe RecordType

recordSize — die Größe des CurrentDateTime in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –.Menge der aktuellen Datums- und Uhrzeit-Datensätze.

2.56. **DailyPresenceCounter**

Auf einer Fahrer- oder Werkstattkarte gespeicherter Zähler, der für jeden Kalendertag, an dem die Karte in eine VU eingesteckt wurde, um eins erhöht wird. Dieser Datentyp bezieht sich auf Anhang 1C Randnummern 266, 299, 320 und 343.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Wertzuweisung: Laufende Nummer mit Höchstwert = 9999, danach wieder bei 0 beginnend. Zum Zeitpunkt des ersten Einsteckens der Karte ist die Zahl auf 0 gesetzt.

2.57. **Datef**

Datum in einem leicht ausdruckbaren numerischen Format.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Wertzuweisung:

yyyy	Jahr
mm	Monat
dd	Tag
'00000000'H	bezeichnet explizit kein Datum.

2.58. **DateOfDayDownloaded**

2. Generation:

Datum und Uhrzeit des Downloads.

```
DateOfDayDownloaded ::= TimeReal
```

Wertzuweisung: nicht näher spezifiziert.

2.59. **DateOfDayDownloadedRecordArray**

2. Generation:

Datum und Uhrzeit des Herunterladens plus im Download-Protokoll verwendete Metadaten.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType — Art des Datensatzes (DateOfDayDownloaded). **Wertzuweisung**: siehe RecordType

recordSize — die Größe des CurrentDateTime in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der Download-Datensätze von Datum und Uhrzeit.

2.60. **Distance**

Eine zurückgelegte Wegstrecke (Ergebnis der Differenz von zwei Kilometerständen des Fahrzeugs).

```
Distance ::= INTEGER(0..2^16-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in km im Betriebsbereich 0 bis 9 999 km.

2.61. **DriverCardApplicationIdentification**

Auf einer Fahrerkarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Anhang 1C Randnummern 253 und 278).

1. Generation:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion gibt die Version der auf der Karte implementierten Struktur an.

noOfEventsPerType — Anzahl der Ereignisse je Ereignisart, die die Karte speichern kann.

noOfFaultsPerType — Anzahl der Störungen je Störungsart, die die Karte speichern kann.

activityStructureLength — gibt die Zahl der Bytes an, die für die Speicherung von Tätigkeitsdatensätzen zur Verfügung stehen.

noOfCardVehicleRecords — Anzahl der Fahrzeugdatensätze, die die Karte enthalten kann.

noOfCardPlaceRecords — Anzahl der Orte, die die Karte aufzeichnen kann.

2. Generation:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Zusätzlich zur 1. Generation werden folgende Datenelementeverwendet:

noOfGNSSCDRecords — Anzahl der ununterbrochenen GNSS-Lenkzeitendatensätze, die die Karte speichern kann.

noOfSpecificConditionRecords — Anzahl der Datensätze mit Bezug auf spezifische Bedingungen, die die Karte speichern kann.

2.62. DriverCardHolderIdentification

Auf einer Fahrerkarte gespeicherte Information zur Identifizierung des Karteninhabers (Anhang 1C Randnummern 256 und 281).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName — Name und Vorname(n) des Inhabers der Fahrerkarte.

cardHolderBirthDate — Geburtsdatum des Inhabers der Fahrerkarte.

cardHolderPreferredLanguage — bevorzugte Sprache des Karteninhabers.

2.63. **DSRCSecurityData**

2. Generation:

Die Klartextinformationen sowie der MAC, die per dedizierter Nahbereichskommunikation (DSRC) vom Kontrollgerät an die Fernabfrageeinrichtung (Remote Interrogator, RI) übertragen werden, Einzelheiten siehe Anlage 11 Teil B Kapitel 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength — Teil der DER-TLV-Kodierung; der Wert ist auf '81 10' zu setzen (siehe Anlage 11 Teil B Kapitel 13).

currentDateTime — aktuelles Datum und aktuelle Uhrzeit der Fahrzeugeinheit.

counter — Anzahl der Nachrichten der Fahrtenschreiberfernüberwachung (Remote Tachograph Monitoring, RTM).

vuSerialNumber — Seriennummer der Fahrzeugeinheit.

dSRCMKVersionNumber — Versionsnummer des DSRC-Hauptschlüssels, von dem die VU-spezifischen DSRC-Schlüssel abgeleitet wurden.

tagLengthMac — Tag und Länge des MAC-Datenobjekts als Teil der DER-TLV-Kodierung. Der Tag muss '8E' lauten, während die Länge des MAC in Oktetten kodiert wird (siehe Anlage 11 Teil B Kapitel 13).

mac — das mithilfe RTM-Nachricht berechnete MAC (siehe Anlage 11 Teil B Kapitel 13).

2.64. **EGFCertificate**

2. Generation:

Zertifikat des öffentlichen Schlüssels der externen GNSS-Ausrüstung zur gegenseitigen Authentisierung mit einer VU. Die Struktur dieses Zertifikats ist in Anlage 11 spezifiziert.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Enthält Informationen zum Chipkartenhersteller.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode — der Zweibuchstabencode des Modulintegrators gemäß ISO 3166.

moduleEmbedder — Kennung des Modulintegrators.

manufacturerInformation — zum internen Gebrauch beim Hersteller.

2.66. **EntryTypeDailyWorkPeriod**

Code zur Unterscheidung zwischen Beginn und Ende des Eintrags eines Arbeitstages und Eingabebedingung.

1. Generation

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Wertzuweisung: gemäß ISO/IEC 8824-1.

2. Generation

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Wertzuweisung: gemäß ISO/IEC 8824-1.

2.67. **EquipmentType**

Code zur Unterscheidung verschiedener Gerätetypen für die Fahrtenschreiberanwendung.

```
EquipmentType ::= INTEGER(0..255)
```

1. Generation:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Wertzuweisung: gemäß ISO/IEC 8824-1.

Der Wert 0 ist für die Angabe des Mitgliedstaats oder Europas im CHA-Feld der Zertifikate reserviert.

2. Generation:

Die Werte der 1. Generation werden um Folgendes ergänzt:

```
--GNSS Facility                          (8),
--Remote Communication Module            (9),
--ITS interface module                   (10),
--Plaque                                 (11), -- may be used in SealRecord
--M1/N1 Adapter                          (12), -- may be used in SealRecord
--European Root CA (ERCA)                (13),
--Member State CA (MSCA)                 (14),
--External GNSS connection               (15), -- may be used in SealRecord
--Unused                                 (16), -- used in SealDataVu
--RFU                                    (17..255)
```

Hinweis: Die Werte der 2. Generation für Einbauplakette, Adapter und externen GNSS-Anschluss sowie die Werte der 1. Generation für Fahrzeugeinheit und Bewegungssensor können gegebenenfalls in SealRecord verwendet werden.

2.68. **EuropeanPublicKey**

1. Generation:

Der europäische öffentliche Schlüssel.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Code, der erläutert, warum ein Ereignis oder eine Störung aufgezeichnet wurde.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Wertzuweisung:

'00'H	eines der 10 jüngsten Ereignisse oder Störungen
'01'H	das längste Ereignis an einem der letzten 10 Tage des Auftretens
'02'H	eines der 5 längsten Ereignisse in den letzten 365 Tagen
'03'H	das letzte Ereignis an einem der letzten 10 Tage des Auftretens
'04'H	das schwerwiegendste Ereignis an einem der letzten 10 Tage des Auftretens
'05'H	eines der 5 schwerwiegendsten Ereignisse in den letzten 365 Tagen
'06'H	das erste Ereignis oder die erste Störung nach der letzten Kalibrierung
'07'H	ein aktives Ereignis oder eine andauernde Störung
'08'H to '7F'H	RFU
'80'H to 'FF'H	herstellerspezifisch

2.70. **EventFaultType**

Code zur näheren Beschreibung eines Ereignisses oder einer Störung.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Wertzuweisung:

1. Generation:

'0x'H	Allgemeine Ereignisse,
'00'H	Keine weiteren Angaben,
'01'H	Einstecken einer ungültigen Karte,
'02'H	Kartenkonflikt,
'03'H	Zeitüberlappung,
'04'H	Lenken ohne geeignete Karte,
'05'H	Einstecken der Karte während des Lenkens,
'06'H	Letzter Vorgang nicht korrekt abgeschlossen,
'07'H	Geschwindigkeitsüberschreitung,
'08'H	Unterbrechung der Stromversorgung,
'09'H	DatenfehlerBewegung,
'0A'H	Datenkonflikt Fahrzeugbewegung,
'0B' to '0F'H	RFU,

	„Versuch Sicherheitsverletzung“ an der Fahrzeugeinheit,
‘1x’H	Keine weiteren Angaben,
‘10’H	Fehlgeschlagene Authentisierung des Bewegungssensors,
‘11’H	Authentisierungsfehler der Fahrtenschreiberkarte,
‘12’H	Unbefugte Veränderung des Bewegungssensors,
‘13’H	Integritätsfehler der Kartendateneingabedaten
‘14’H	Integritätsfehler der gespeicherten Benutzerdaten,
‘15’H	Interner Datenübertragungsfehler,
‘16’H	Unberechtigtes Öffnen des Gehäuses,
‘17’H	Hardwaremanipulation,
‘18’H	RFU,
‘19’H to ‘1F’H	
‘2x’H	„Versuch Sicherheitsverletzung“ Bewegungssensor,
‘20’H	Keine weiteren Angaben,
‘21’H	Fehlgeschlagene Authentisierung,
‘22’H	Integritätsfehler der gespeicherten Daten,
‘23’H	Interner Datenübertragungsfehler,
‘24’H	Unberechtigtes Öffnen des Gehäuses,
‘25’H	Hardwaremanipulation,
‘26’H to ‘2F’H	RFU,
‘3x’H	Störungen Kontrollgerät,
‘30’H	Keine weiteren Angaben,
‘31’H	Interne Störung VU,
‘32’H	Druckerstörung,
‘33’H	Anzeigestörung,
‘34’H	Störung beim Herunterladen,
‘35’H	Sensorstörung,
‘36’H to ‘3F’H	RFU,
‘4x’H	Kartenstörungen,
‘40’H	Keine weiteren Angaben,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	Herstellerspezifisch.

2. Generation:

Die Werte der 1. Generation werden um Folgendes ergänzt:

‘0B’H	Zeitkonflikt (zwischen GNSS und Systemuhr der VU),
‘0C’ to ‘0F’H	RFU,
‘5x’H	Störungen im Zusammenhang mit dem GNSS,
‘50’H	Keine weiteren Angaben,
‘51’H	Störung des internen GNSS-Empfängers,
‘52’H	Störung des externen GNSS-Empfängers,
‘53’H	Kommunikationsstörung des externen GNSS,
‘54’H	Fehlende GNSS-Positionsdaten,
‘55’H	Manipulationserkennung beim GNSS,
‘56’H	Abgelaufenes Zertifikat der externen GNSS-Ausrüstung,
‘57’H to ‘5F’H	RFU,
‘6x’H	Störungen im Zusammenhang mit dem Fernkommunikationsmodul,
‘60’H	Keine weiteren Angaben,
‘61’H	Störung des Fernkommunikationsmoduls,
‘62’H	Kommunikationsstörung des Fernkommunikationsmoduls,
‘63’H to ‘6F’H	RFU,
‘7x’H	ITS-Schnittstellenmodul,
‘70’H	Keine weiteren Angaben,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

2. Generation:

Der erweiterte Plombenbezeichner dient der eindeutigen Identifizierung von Plomben (Anhang 1C Randnummer 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode — ein Code des Plombenherstellers.

sealIdentifier — ein Bezeichner für die Plombe, der für den Hersteller eindeutig sein muss.

2.72. **ExtendedSerialNumber**

Eindeutige Kennung eines Geräts. Kann auch als Bezeichner des öffentlichen Schlüssels eines Geräts verwendet werden.

1. Generation:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber — einmalige Seriennummer des Geräts in Bezug auf den Hersteller, den Gerätetyp sowie den Monat und das Jahr (im Folgenden angegeben).

monthYear — Kennung für den Monat und das Jahr der Herstellung (oder der Zuweisung der Seriennummer).

Wertzuweisung: BCD-Kodierung des Monats (zwei Stellen) und des Jahres (die beiden letzten Stellen).

type — Bezeichner des Gerätetyps.

Wertzuweisung — herstellerspezifisch, mit reserviertem Wert 'FFh'.

manufacturerCode — numerischer Code des Herstellers eines typgenehmigten Geräts.

2. Generation:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber — siehe 1. Generation

monthYear — siehe 1. Generation

type — Angabe des Gerätetyps

manufacturerCode — siehe 1. Generation

2.73. **FullCardNumber**

Code zur vollständigen Identifizierung einer Karte.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType — Art der Fahrtenschreiberkarte.

cardIssuingMemberState — Code des Mitgliedstaates, der die Karte ausgegeben hat.

cardNumber — Kartennummer.

2.74. **FullCardNumberAndGeneration**

2. Generation:

Code zur vollständigen Identifizierung einer Karte und ihrer Generation.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber — Bezeichner der Fahrtenschreiberkarte.

generation — Angabe der Generation der verwendeten Fahrtenschreiberkarte.

2.75. **Generation**

2. Generation:

Generation des verwendeten Fahrtenschreibers.

```
Generation ::= INTEGER(0..255)
```

Wertzuweisung:

'00'H	RFU
'01'H	1. Generation
'02'H	2. Generation
'03'H … 'FF'H	RFU

2.76. **GeoCoordinates**

2. Generation:

Die Geokoordinaten sind als Integer kodiert. Bei diesen Integern handelt es sich um Vielfache der Kodierungen ±DDMM.M für die Breite und ±DDDMM.M für die Länge. Hier geben ±DD beziehungsweise ±DDD die Grade an, MM.M die Minuten.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude — kodiert als Vielfaches (Faktor 10) der Darstellung ±DDMM.M.

longitude — kodiert als Vielfaches (Faktor 10) der Darstellung ±DDDMM.M.

2.77. **GNSSAccuracy**

2. Generation:

Die Genauigkeit der GNSS-Positionsdaten (Begriffsbestimmung eee)). Diese Genauigkeit ist als Integer kodiert, bei dem es sich um ein Vielfaches (Faktor 10) des durch den GSA-NMEA-Datensatz bereitgestellten X.Y-Wertes handelt.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

2. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Informationen im Zusammenhang mit der GNSS-Position des Fahrzeugs, wenn die ununterbrochene Lenkzeit des Fahrers ein Vielfaches von drei Stunden erreicht (Anhang 1C Randnummern 306 und 354).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord — Index des zuletzt aktualisierten ununterbrochenen GNSS-Lenkzeitendatensatzes.

Wertzuweisung: Zahl, die dem Zähler des ununterbrochenen GNSS-Lenkzeitendatensatzes entspricht, beginnend mit '0' für das erste Auftreten des ununterbrochenen GNSS-Lenkzeitendatensatzes in der Struktur.

gnssContinuousDrivingRecords — Datensätze mit Datum und Uhrzeit, wann die ununterbrochene Lenkzeit ein Vielfaches von drei Stunden erreicht, sowie Informationen zur Position des Fahrzeugs.

2.79. **GNSSContinuousDrivingRecord**

2. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Informationen im Zusammenhang mit der GNSS-Position des Fahrzeugs, wenn die ununterbrochene Lenkzeit des Fahrers ein Vielfaches von drei Stunden erreicht (Anhang 1C Randnummern 305 und 353).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp — Datum und Uhrzeit, wann die ununterbrochene Lenkzeit des Karteninhabers ein Vielfaches von drei Stunden erreicht.

gnssPlaceRecord — Informationen zur Position des Fahrzeugs.

2.80. **GNSSPlaceRecord**

2. Generation:

Informationen zur GNSS-Position des Fahrzeugs (Anhang 1C Randnummern 108, 109, 110, 296, 305, 347 und 353).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp — Datum und Uhrzeit, wann die GNSS-Position des Fahrzeugs bestimmt wurde.

gnssAccuracy — Genauigkeit der GNSS-Positionsdaten.

geoCoordinates — der mittels GNSS aufgezeichnete Standort.

2.81. **HighResOdometer**

Kilometerstand des Fahrzeugs: Vom Fahrzeug während des Betriebs insgesamt zurückgelegte Wegstrecke.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in 1/200 km im Betriebsbereich 0 bis 21 055 406 km.

2.82. **HighResTripDistance**

Während einer Fahrt oder eines Teils einer Fahrt zurückgelegte Wegstrecke.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in 1/200 km im Betriebsbereich 0 bis 21 055 406 km.

2.83. **HolderName**

Familienname und Vorname(n) eines Karteninhabers.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname — Familienname des Inhabers. Ohne Titel.

Wertzuweisung: Handelt es sich nicht um eine auf eine bestimmte Person ausgestellte Karte, so enthält holderSurname die gleichen Informationen wie companyName oder workshopName oder controlBodyName.

holderFirstNames — Vorname(n) und Initialen des Inhabers.

2.84. **InternalGNSSReceiver**

2. Generation:

Information, ob es sich beim GNSS-Empfänger der VU um ein internes oder externes Gerät handelt. „True“ bedeutet, dass es sich um einen VU-internen GNSS-Empfänger handelt. „False“ bedeutet, dass der GNSS-Empfänger extern ist.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Kontrollgerätkonstante (Begriffsbestimmung m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Wertzuweisung: Impulse je Kilometer im Betriebsbereich 0 bis 64 255 Imp/km.

2.86. **KeyIdentifier**

Eindeutiger Bezeichner eines öffentlichen Schlüssels zur Herstellung eines Verweises auf den Schlüssel und für dessen Auswahl. Identifiziert zugleich den Inhaber des Schlüssels.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

Die erste Auswahlmöglichkeit eignet sich zum Verweis auf den öffentlichen Schlüssel einer Fahrzeugeinheit oder einer Fahrtenschreiberkarte.

Die zweite Auswahlmöglichkeit eignet sich zum Verweis auf den öffentlichen Schlüssel einer Fahrzeugeinheit (falls die Seriennummer der Fahrzeugeinheit zum Zeitpunkt der Generierung des Zertifikats nicht bekannt ist).

Die dritte Auswahlmöglichkeit eignet sich zum Verweis auf den öffentlichen Schlüssel eines Mitgliedstaates.

2.87. **KMWCKey**

2. Generation:

AES-Schlüssel und zugehörige Schlüsselversion, die für die Kopplung VU–Bewegungssensor verwendet wird. Zu den Einzelheiten siehe Anlage 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey — Länge des AES-Schlüssels, verkettet mit dem Schlüssel, der für die Kopplung VU–Bewegungssensor verwendet wird.

keyVersion — Schlüsselversion des AES-Schlüssels.

2.88. **Language**

Code zur Identifizierung einer Sprache.

```
Language ::= IA5String(SIZE(2))
```

Wertzuweisung: Kodierung aus zwei Kleinbuchstaben gemäß ISO 639.

2.89. **LastCardDownload**

Auf der Fahrerkarte gespeicherte(s) Datum und Uhrzeit des letzten Herunterladens der Daten von der Karte (zu anderen als Kontrollzwecken) — Anhang 1C Randnummern 257 und 282. Diese Datumsangabe kann mit einer beliebigen VU oder einem Kartenlesegerät geändert werden.

```
LastCardDownload ::= TimeReal
```

Wertzuweisung: nicht näher spezifiziert.

2.90. **LinkCertificate**

2. Generation:

Das Linkzertifikat zwischen Schlüsselpaaren der European Root CA.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Tatsächlicher Umfang der Fahrzeugreifen (Begriffsbestimmung u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl, Wert in 1/8 mm im Betriebsbereich 0 bis 8 031 mm.

2.92. **MAC**

2. Generation:

Kryptografische Prüfsumme mit einer Länge von 8, 12 oder 16 Byte, entsprechend den in Anlage 11 spezifizierten Cipher Suites.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Code, der angibt, ob ein Karteninhaber beim Einstecken der Karte Fahrertätigkeiten manuell eingegeben hat oder nicht (Anhang 1B Randnummer 081 und Anhang 1C Randnummer 102).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Wertzuweisung: nicht näher spezifiziert.

2.94. **ManufacturerCode**

Code zur Identifizierung des Herstellers typgenehmigter Geräte.

```
ManufacturerCode ::= INTEGER(0..255)
```

Das für Interoperabilitätsprüfungen zuständige Labor führt die Liste der Herstellercodes und veröffentlicht sie auf seiner Internetseite (Anhang 1C Randnummer 454).

ManufacturerCodes werden den Entwicklern von Fahrtenschreibergeräten auf Antrag beim für Interoperabilitätsprüfungen zuständigen Labor vorläufig zugeteilt.

2.95. **ManufacturerSpecificEventFaultData**

2. Generation:

Herstellerspezifische Fehlercodes vereinfachen die Fehleranalyse sowie die Instandhaltung von Fahrzeugeinheiten.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode — Name des Herstellers der Fahrzeugeinheit.

manufacturerSpecificErrorCode — ein für den Hersteller spezifischer Fehlercode.

2.96. **MemberStateCertificate**

Zertifikat des öffentlichen Schlüssels eines Mitgliedstaates, ausgestellt von der europäischen Zertifizierungsstelle.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

2. Generation:

Zertifikat des Mitgliedstaats und im Download-Protokoll verwendete Metadaten.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType — Art des Datensatzes (MemberStateCertificate). **Wertzuweisung**: siehe RecordType

recordSize — die Größe des MemberStateCertificate in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze. Der Wert muss auf 1 gesetzt werden, da die Zertifikate verschieden lang sein können.

records –der Satz der Mitgliedstaatzertifikate.

2.98. **MemberStatePublicKey**

1. Generation:

Der öffentliche Schlüssel eines Mitgliedstaates.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Ein Name.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage gibt einen in Kapitel 4 definierten Zeichensatz an,

name ist ein unter Verwendung des spezifizierten Zeichensatzes kodierter Name.

2.100. **NationAlpha**

Die alphabetische Bezeichnung eines Staats erfolgt im Einklang mit den auf Fahrzeugen im grenzüberschreitenden Verkehr gemäß dem Wiener Übereinkommen über den Straßenverkehr (Vereinte Nationen, 1968) verwendeten Unterscheidungszeichen.

```
NationAlpha ::= IA5String(SIZE(3))
```

Die Codes NationAlpha und NationNumeric sind in einer Liste aufgeführt, die von dem gemäß Anhang 1C Randnummer 440 mit der Durchführung der Interoperabilitätsprüfungen beauftragten Labor auf dessen Internetseite geführt wird.

2.101. **NationNumeric**

Numerische Bezeichnung eines Landes.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Wertzuweisung: siehe Datentyp 2.100 (NationAlpha).

Jegliche Änderung oder Aktualisierung der Spezifikationen NationAlpha oder NationNumeric darf von dem beauftragten Labor nur nach Einholung von Stellungnahmen der Hersteller typgenehmigter digitaler und intelligenter Fahrtenschreiber-Fahrzeugeinheiten vorgenommen werden.

2.102. **NoOfCalibrationRecords**

Anzahl der Kalibrierungsdatensätze, die eine Werkstattkarte speichern kann.

1. Generation:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Wertzuweisung: siehe Anlage 2.

2. Generation:

$$\texttt{NoOfCalibrationRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Wertzuweisung: siehe Anlage 2.

2.103. **NoOfCalibrationsSinceDownload**

Zähler zur Angabe der mit einer Werkstattkarte seit dem letzten Herunterladen durchgeführten Kalibrierungen (Anhang 1C Randnummern 317 und 340).

$$\texttt{NoOfCalibrationsSinceDownload ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Wertzuweisung: nicht näher spezifiziert.

2.104. **NoOfCardPlaceRecords**

Anzahl der Ortsdatensätze, die eine Fahrer- oder Werkstattkarte speichern kann.

1. Generation:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Wertzuweisung: siehe Anlage 2.

2. Generation:

$$\texttt{NoOfCardPlaceRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Wertzuweisung: siehe Anlage 2.

2.105. **NoOfCardVehicleRecords**

Anzahl der Angaben zu den gefahrenen Fahrzeugen enthaltenden Datensätze, die eine Fahrer- oder Werkstattkarte speichern kann.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.106. **NoOfCardVehicleUnitRecords**

2. Generation:

Anzahl der Angaben zu dengenutzten Fahrzeugeinheiten enthaltenden Datensätze, die eine Fahrer- oder Werkstattkarte speichern kann.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.107. **NoOfCompanyActivityRecords**

Anzahl der Unternehmenstätigkeitsdatensätze, die eine Unternehmenskarte speichern kann.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.108. **NoOfControlActivityRecords**

Anzahl der Kontrollaktivitätsdatensätze, die eine Kontrollkarte speichern kann.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.109. **NoOfEventsPerType**

Anzahl der Ereignisse je Ereignisart, die eine Karte speichern kann.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Wertzuweisung: siehe Anlage 2.

2.110. **NoOfFaultsPerType**

Anzahl der Störungen je Störungsart, die eine Karte speichern kann.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Wertzuweisung: siehe Anlage 2.

2.111. **NoOfGNSSCDRecords**

2. Generation:

Anzahl der ununterbrochenen GNSS-Lenkzeitendatensätze, die die Karte speichern kann.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.112. **NoOfSpecificConditionRecords**

2. Generation:

Anzahl der Datensätze mit Bezug auf spezifische Bedingungen, die eine Karte speichern kann.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Wertzuweisung: siehe Anlage 2.

2.113. **OdometerShort**

Kilometerstand des Fahrzeugs in Kurzform.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in km im Betriebsbereich 0 bis 9 999 999 km.

2.114. **OdometerValueMidnight**

Kilometerstand des Fahrzeugs um Mitternacht am jeweiligen Tag (Anhang 1B Randnummer 090 und Anhang 1C Randnummer 113).

```
OdometerValueMidnight ::= OdometerShort
```

Wertzuweisung: nicht näher spezifiziert.

2.115. **OdometerValueMidnightRecordArray**

2. Generation:

OdometerValueMidnight und im Download-Protokoll verwendete Metadaten.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType — Art des Datensatzes (OdometerValueMidnight). **Wertzuweisung**: siehe RecordType

recordSize — die Größe des OdometerValueMidnight in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der OdometerValueMidnight-Datensätze.

2.116. **OverspeedNumber**

Anzahl der Geschwindigkeitsüberschreitungen seit der letzten Kontrolle Geschwindigkeitsüberschreitung.

```
OverspeedNumber ::= INTEGER(0..255)
```

Wertzuweisung: 0 bedeutet, dass seit der letzten Kontrolle Geschwindigkeitsüberschreitung kein Ereignis Geschwindigkeitsüberschreitung aufgetreten ist, 1 bedeutet, dass 1 derartiges Ereignis seit der letzten entsprechenden Kontrolle aufgetreten ist, … 255 bedeutet, dass 255 oder mehr derartige Ereignisse seit der letzten entsprechenden Kontrolle aufgetreten sind.

2.117. **PlaceRecord**

Informationen zum Ort des Beginns oder Endes des Arbeitstages (Anhang 1C Randnummern 108, 271, 296, 324 und 347).

1. Generation:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime — auf die Eingabe bezogene Datums- und Zeitangabe.

entryTypeDailyWorkPeriod — Art der Eingabe.

dailyWorkPeriodCountry — eingegebenes Land.

dailyWorkPeriodRegion — eingegebene Region.

vehicleOdometerValue — Kilometerstand zum Zeitpunkt und am Ort der Eingabe.

2. Generation:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

Zusätzlich zur 1. Generation wird folgende Komponente genutzt:

entryGNSSPlaceRecord — die aufgezeichneten Standort- und Zeitangaben.

2.118. **PreviousVehicleInfo**

Information zum zuvor von einem Fahrer gefahrenen Fahrzeug beim Einstecken seiner Karte in eine Fahrzeugeinheit (Anhang 1B Randnummer 081 und Anhang 1C Randnummer 102).

1. Generation:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs.

cardWithdrawalTime — Datum und Uhrzeit der Kartenentnahme.

2. Generation:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Zusätzlich zur 1. Generation wird folgendes Datenelement verwendet:

vuGeneration — Kennzeichnung für die Generation der Fahrzeugeinheit.

2.119. **PublicKey**

1. Generation:

Ein öffentlicher RSA-Schlüssel.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus — Modulus des Schlüsselpaares.

rsaKeyPublicExponent — öffentlicher Exponent des Schlüsselpaares.

2.120. **RecordType**

2. Generation:

Bezeichnung eines Datensatztyps. Dieser Datentyp wird in RecordArrays verwendet.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Wertzuweisung:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	Herstellerspezifisch.

2.121. **RegionAlpha**

Alphabetische Angabe einer Region innerhalb eines bestimmten Landes.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

1. Generation:

Wertzuweisung:

```
‘   ’         No information available,
Spain:
‘AN ’         Andalucía,
‘AR ’         Aragón,
‘AST’         Asturias,
‘C  ’         Cantabria,
‘CAT’         Cataluña,
‘CL ’         Castilla-León,
‘CM ’         Castilla-La-Mancha,
‘CV’          Valencia,
‘EXT’         Extremadura,
‘G  ’         Galicia,
‘IB ’         Baleares,
‘IC ’         Canarias,
‘LR ’         La Rioja,
‘M  ’         Madrid,
‘MU ’         Murcia,
‘NA ’         Navarra,
‘PV ’         País Vasco
```

2. Generation:

Die RegionAlpha-Codes sind in einer Liste aufgeführt, die von dem mit der Durchführung der Interoperabilitätsprüfungen beauftragten Labor auf dessen Internetseite geführt wird.

2.122. **RegionNumeric**

Numerische Angabe einer Region innerhalb eines bestimmten Landes.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

1. Generation:

Wertzuweisung:

```
‘00’H         No information available,
Spain:
‘01’H         Andalucía,
‘02’H         Aragón,
‘03’H         Asturias,
‘04’H         Cantabria,
‘05’H         Cataluña,
‘06’H         Castilla-León,
‘07’H         Castilla-La-Mancha,
‘08’H         Valencia,
‘09’H         Extremadura,
‘0A’H         Galicia,
‘0B’H         Baleares,
‘0C’H         Canarias,
‘0D’H         La Rioja,
‘0E’H         Madrid,
‘0F’H         Murcia,
‘10’H         Navarra,
‘11’H         País Vasco
```

2. Generation:

Die RegionNumeric-Codes sind in einer Liste aufgeführt, die von dem mit der Durchführung der Interoperabilitätsprüfungen beauftragten Labor auf dessen Internetseite geführt wird.

2.123. **RemoteCommunicationModuleSerialNumber**

2. Generation:

Seriennummer des Fernkommunikationsmoduls.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

1. Generation:

Der Modulus eines RSA-Schlüsselpaares.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Wertzuweisung: nicht spezifiziert.

2.125. **RSAKeyPrivateExponent**

1. Generation:

Privater Exponent eines RSA-Schlüsselpaares.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Wertzuweisung: nicht spezifiziert.

2.126. **RSAKeyPublicExponent**

1. Generation:

Öffentlicher Exponent eines RSA-Schlüsselpaares.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Wertzuweisung: nicht spezifiziert.

2.127. **RtmData**

2. Generation:

Bezüglich der Definition dieses Datentyps siehe Anlage 14.

2.128. **SealDataCard**

2. Generation:

Dieser Datentyp speichert Informationen über die an den verschiedenen Komponenten eines Fahrzeugs angebrachten Plomben und dient der Speicherung auf einer Karte. Dieser Datentyp bezieht sich auf Anhang 1C Randnummer 337.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords — Anzahl der in der Menge sealRecords aufgeführten Datensätze.

sealRecords — Plombendatensatz.

2.129. **SealDataVu**

2. Generation:

Dieser Datentyp speichert Informationen über die an den verschiedenen Komponenten eines Fahrzeugs angebrachten Plomben und dient der Speicherung in einer Fahrzeugeinheit.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords — Plombendatensatz. Sind weniger als 5 Plomben verfügbar, wird der Wert EquipmentType in allen unbenutzten sealRecords auf 16, d. h. unbenutzt, gesetzt.

2.130. **SealRecord**

2. Generation:

Dieser Datentyp speichert Informationen zur an einer Komponente angebrachten Plombe. Dieser Datentyp bezieht sich auf Anhang 1C Randnummer 337.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType — identifiziert den Gerätetyp, an dem die Plombe angebracht ist.

extendedSealIdentifier — bezeichnet die am Gerät angebrachte Plombe.

2.131. **SensorApprovalNumber**

Typgenehmigungsnummer desBewegungssensors.

1. Generation:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Wertzuweisung: nicht spezifiziert.

2. Generation:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Wertzuweisung:

Die Genehmigungsnummer muss derjenigen entsprechen, die auf der zugehörigen Website der Europäischen Kommission veröffentlicht ist, und beispielsweise etwaige Bindestriche berücksichtigen. Die Genehmigungsnummer muss linksbündig ausgerichtet sein.

2.132. **SensorExternalGNSSApprovalNumber**

2. Generation:

Typgenehmigungsnummer der externen GNSS-Ausrüstung.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Wertzuweisung:

Die Genehmigungsnummer muss derjenigen entsprechen, die auf der zugehörigen Website der Europäischen Kommission veröffentlicht ist, und beispielsweise etwaige Bindestriche berücksichtigen. Die Genehmigungsnummer muss linksbündig ausgerichtet sein.

2.133. **SensorExternalGNSSCoupledRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zur Identifizierung der mit der Fahrzeugeinheit gekoppelten externen GNSS-Ausrüstung (Anhang 1C Randnummer 100).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber — Seriennummer der mit der Fahrzeugeinheit gekoppelten externen GNSS-Ausrüstung.

sensorApprovalNumber –Typgenehmigungsnummer dieser externen GNSS-Ausrüstung.

sensorCouplingDate — Datum der Kopplung dieser externen GNSS-Ausrüstung mit der Fahrzeugeinheit.

2.134. **SensorExternalGNSSIdentification**

2. Generation:

Informationen zur Identifizierung der externen GNSS-Ausrüstung (Anhang 1C Randnummer 98).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber — erweiterte Seriennummer der externen GNSS-Ausrüstung.

sensorApprovalNumber –Typgenehmigungsnummer der externen GNSS-Ausrüstung.

sensorSCIdentifier — Bezeichner der Sicherheitskomponente der externen GNSS-Ausrüstung.

sensorOSIdentifier — Bezeichner des Betriebssystems der externen GNSS-Ausrüstung.

2.135. **SensorExternalGNSSInstallation**

2. Generation:

In einer externen GNSS-Ausrüstung gespeicherte Informationen zur Installation der externen GNSS-Ausrüstung (Anhang 1C Randnummer 123).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst — Datum der ersten Kopplung der externen GNSS-Ausrüstung mit einer Fahrzeugeinheit.

firstVuApprovalNumber –Typgenehmigungsnummer der ersten mit der externen GNSS-Ausrüstung gekoppelten Fahrzeugeinheit.

firstVuSerialNumber — Seriennummer der ersten mit der externen GNSS-Ausrüstung gekoppelten Fahrzeugeinheit.

sensorCouplingDateCurrent — Datum der aktuellen Kopplung der externen GNSS-Ausrüstung mit einer Fahrzeugeinheit.

currentVuApprovalNumber –Typgenehmigungsnummer der derzeit mit der externen GNSS-Ausrüstung gekoppelten Fahrzeugeinheit.

currentVuSerienNumber — Seriennummer der derzeit mit der externen GNSS-Ausrüstung gekoppelten Fahrzeugeinheit.

2.136. **SensorExternalGNSSOSIdentifier**

2. Generation:

Bezeichner des Betriebssystems der externen GNSS-Ausrüstung.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Wertzuweisung: herstellerspezifisch.

2.137. **SensorExternalGNSSSCIdentifier**

2. Generation:

Dieser Typ dient beispielsweise der Identifizierung des kryptografischen Moduls der externen GNSS-Ausrüstung.

Bezeichner der Sicherheitskomponente der externen GNSS-Ausrüstung.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Wertzuweisung: Komponente herstellerspezifisch.

2.138. **SensorGNSSCouplingDate**

2. Generation:

Datum einer Kopplung der externen GNSS-Ausrüstung mit einer Fahrzeugeinheit.

```
SensorGNSSCouplingDate ::= TimeReal
```

Wertzuweisung: nicht spezifiziert.

2.139. **SensorGNSSSerialNumber**

2. Generation:

Dieser Typ dient der Speicherung der Seriennummer des GNSS-Empfängers sowohl innerhalb als auch außerhalb der VU.

Seriennummer des GNSS-Empfängers.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

In einem Bewegungssensor gespeicherte Information zur Identifizierung des Bewegungssensors (Anhang 1B Randnummer 077 und Anhang 1C Randnummer 95).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorSCIdentifier                SensorSCIdentifier,
   sensorOSIdentifier                SensorOSIdentifier
}
```

sensorSerialNumber — erweiterte Seriennummer des Bewegungssensors (umfasst Teilnummer und Herstellercode)

sensorApprovalNumber –Typgenehmigungsnummer des Bewegungssensors.

sensorSCIdentifier — Bezeichner der Sicherheitskomponente des Bewegungssensors.

sensorOSIdentifier — Bezeichner des Betriebssystems des Bewegungssensors.

2.141. **SensorInstallation**

In einem Bewegungssensor gespeicherte Information zur Installation des Bewegungssensors (Anhang 1B Randnummer 099 und Anhang 1C Randnummer 122).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst            SensorPairingDate,
   firstVuApprovalNumber             VuApprovalNumber,
   firstVuSerialNumber               VuSerialNumber,
   sensorPairingDateCurrent          SensorPairingDate,
   currentVuApprovalNumber           VuApprovalNumber,
   currentVUSerialNumber             VuSerialNumber
}
```

sensorPairingDateFirst — Datum der ersten Koppelung des Bewegungssensors mit einer Fahrzeugeinheit.

firstVuApprovalNumber –Typgenehmigungsnummer der ersten mit dem Bewegungssensor gekoppelten Fahrzeugeinheit.

firstVuSerialNumber — Seriennummer der ersten mit dem Bewegungssensor gekoppelten Fahrzeugeinheit.

sensorPairingDateCurrent — Datum der derzeitigen Koppelung des Bewegungssensors mit der Fahrzeugeinheit.

currentVuApprovalNumber –Typgenehmigungsnummer der derzeit mit dem Bewegungssensor gekoppelten Fahrzeugeinheit.

currentVUSerialNumber — Seriennummer der derzeit mit dem Bewegungssensor gekoppelten Fahrzeugeinheit.

2.142. **SensorInstallationSecData**

Auf einer Werkstattkarte gespeicherte Information zu den für die Koppelung von Bewegungssensoren und Fahrzeugeinheiten benötigten Sicherheitsdaten (Anhang 1C Randnummern 308 und 331).

1. Generation:

```
SensorInstallationSecData ::= TdesSessionKey
```

Wertzuweisung: gemäß ISO 16844-3.

2. Generation:

Wie in Anlage 11 beschrieben, muss eine Werkstattkarte bis zu drei Schlüssel für die Kopplung VU–Bewegungssensor speichern können, die unterschiedliche Schlüsselversionen haben.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                          KMWCKey,
   kMWCKey2                          KMWCKey OPTIONAL,
   kMWCKey3                          KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Bezeichner des Betriebssystems des Bewegungssensors.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Wertzuweisung: herstellerspezifisch.

2.144. **SensorPaired**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zur Identifizierung des mit der Fahrzeugeinheit gekoppelten Bewegungssensors (Anhang 1B Randnummer 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorPairingDateFirst            SensorPairingDate
}
```

sensorSerialNumber — Seriennummer des derzeit mit der Fahrzeugeinheit gekoppelten Bewegungssensors.

sensorApprovalNumber –Typgenehmigungsnummer des derzeit mit der Fahrzeugeinheit gekoppelten Bewegungssensors.

sensorPairingDateFirst — Datum der ersten Koppelung des derzeit mit der Fahrzeugeinheit gekoppelten Bewegungssensors mit einer Fahrzeugeinheit.

2.145. **SensorPairedRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zur Identifizierung eines mit der Fahrzeugeinheit gekoppelten Bewegungssensors (Anhang 1C Randnummer 97).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber — Seriennummer eines mit der Fahrzeugeinheit gekoppelten Bewegungssensors.

sensorApprovalNumber –Typgenehmigungsnummer dieses Bewegungssensors.

sensorPairingDate — Datum der Koppelung dieses Bewegungssensors mit der Fahrzeugeinheit.

2.146. **SensorPairingDate**

Datum einer Koppelung des Bewegungssensors mit einer Fahrzeugeinheit.

```
SensorPairingDate ::= TimeReal
```

Wertzuweisung: nicht spezifiziert.

2.147. **SensorSCIdentifier**

Bezeichner der Sicherheitskomponente des Bewegungssensors.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Wertzuweisung: Komponente herstellerspezifisch.

2.148. **SensorSerialNumber**

Seriennummer des Bewegungssensors.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Eine digitale Signatur.

1. Generation:

```
Signature ::= OCTET STRING (SIZE(128))
```

Wertzuweisung: gemäß Anlage 11, Gemeinsame Sicherheitsmechanismen.

2. Generation:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Wertzuweisung: gemäß Anlage 11, Gemeinsame Sicherheitsmechanismen.

2.150. **SignatureRecordArray**

2. Generation:

Satz von Signaturen plus im Download-Protokoll verwendete Metadaten.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType — Art des Datensatzes (Signatur). **Wertzuweisung**: siehe RecordType

recordSize — die Größe der Signatur in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze. Der Wert muss auf 1 gesetzt werden, da die Signaturen verschieden lang sein können.

records — der Satz von Signaturen.

2.151. **SimilarEventsNumber**

Anzahl ähnlicher Ereignisse an einem bestimmten Tag (Anhang 1B Randnummer 094 und Anhang 1C Randnummer 117).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Wertzuweisung: 0 wird nicht verwendet, 1 bedeutet, dass an diesem Tag nur ein Ereignis dieser Art aufgetreten und gespeichert wurde, 2 bedeutet, dass 2 Ereignisse dieser Art an diesem Tag aufgetreten sind (nur eines wurde gespeichert), … 255 bedeutet, dass 255 oder mehr Ereignisse dieser Art an diesem Tag aufgetreten sind.

2.152. **SpecificConditionRecord**

Auf einer Fahrerkarte, einer Werkstattkarte oder in einer Fahrzeugeinheit gespeicherte Information zu einer spezifischen Bedingung (Anhang 1C Randnummern 130, 276, 301, 328 und 355).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime — Datum und Uhrzeit der Eingabe.

specificConditionType — Code zur Identifizierung der spezifischen Bedingung.

2.153. **SpecificConditions**

Auf einer Fahrerkarte, einer Werkstattkarte oder in einer Fahrzeugeinheit gespeicherte Information zu einer spezifischen Bedingung (Anhang 1C Randnummern 131, 277, 302, 329 und 356).

2. Generation:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord — Index des zuletzt aktualisierten Datensatzes mit Bezug auf spezifische Bedingungen.

Wertzuweisung: Zahl, die dem Zähler des Datensatzes mit Bezug auf spezifische Bedingungen entspricht, beginnend mit '0' für das erste Auftreten des Datensatzes mit Bezug auf spezifische Bedingungen in der Struktur.

specificConditionRecords — Datensätze mit Informationen zu den aufgezeichneten spezifischen Bedingungen.

2.154. **SpecificConditionType**

Code zur Identifizierung einer spezifischen Bedingung (Anhang 1B Randnummern 050b, 105a, 212a und 230a sowie Anhang 1C Randnummer 62).

```
SpecificConditionType ::= INTEGER(0..255)
```

1. Generation:

Wertzuweisung:

'00'H	RFU
'01'H	Kontrollgerät nicht erforderlich — Anfang
'02'H	Kontrollgerät nicht erforderlich — Ende
'03'H	Fährüberfahrt/Zugfahrt
'04'H … 'FF'H	RFU

2. Generation:

Wertzuweisung:

'00'H	RFU
'01'H	Kontrollgerät nicht erforderlich — Anfang
'02'H	Kontrollgerät nicht erforderlich — Ende
'03'H	Fährüberfahrt/Zugfahrt — Anfang
'04'H	Fährüberfahrt/Zugfahrt — Ende
'05'H … 'FF'H	RFU

2.155. **Speed**

Fahrzeuggeschwindigkeit (km/h).

```
Speed ::= INTEGER(0..255)
```

Wertzuweisung: Kilometer pro Stunde im Betriebsbereich 0 bis 220 km/h.

2.156. **SpeedAuthorised**

Zulässige Höchstgeschwindigkeit des Fahrzeugs (Begriffsbestimmung hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Durchschnittsgeschwindigkeit in einem vorher festgelegten Zeitraum (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Höchstgeschwindigkeit in einem vorher festgelegten Zeitraum.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

2. Generation:

Zur Definition dieses Datentyps siehe Anlage 14.

2.160. **TachographPayloadEncrypted**

2. Generation:

DER-TLV-verschlüsselte Fahrtenschreibernutzlast, d. h. die verschlüsselt in der RTM-Nachricht gesendeten Daten. Zur Verschlüsselung siehe Anlage 11 Teil B Kapitel 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag — Teil der DER-TLV-Kodierung; der Wert ist auf '87' zu setzen (siehe Anlage 11 Teil B Kapitel 13).

length — Teil der DER-TLV-Kodierung, der die Länge des folgenden paddingContentIndicatorByte und der encryptedData kodiert.

paddingContentIndicatorByte — auf '00' zu setzen.

encryptedData — verschlüsselte tachographPayload gemäß Anlage 11 Teil B Kapitel 13. Die Länge dieser Daten in Oktetten beträgt immer ein Vielfaches von 16.

2.161. **TDesSessionKey**

1. Generation:

Ein Triple-DES-Sitzungsschlüssel.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Wertzuweisung: nicht näher spezifiziert.

2.162. **TimeReal**

Code für ein kombiniertes Datum/Uhrzeit-Feld, in dem Datum und Uhrzeit als Sekunden nach dem 1. Januar 1970 00h.00m.00s. GMT ausgedrückt sind.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Wertzuweisung — **Oktettanordnung**: Anzahl der Sekunden seit dem 1. Januar 1970, 0.00 Uhr GMT.

Höchstmögliche(s) Datum/Uhrzeit ist im Jahr 2106.

2.163. **TyreSize**

Bezeichnung der Reifenabmessungen.

```
TyreSize ::= IA5String(SIZE(15))
```

Wertzuweisung: gemäß Richtlinie 92/23/EWG vom 31.3.1992, ABl. L 129, S.95.

2.164. **VehicleIdentificationNumber**

Fahrzeugidentifizierungsnummer (VIN) mit Bezug auf das Fahrzeug insgesamt, in der Regel Fahrgestellnummer oder Rahmennummer.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Wertzuweisung: laut Definition in ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

2. Generation:

Fahrzeugidentifizierungsnummer plus im Download-Protokoll verwendete Metadaten.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType — Art des Datensatzes (VehicleIdentificationNumber). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VehicleIdentificationNumber in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — der Satz von Fahrzeugidentifizierungsnummern.

2.166. **VehicleRegistrationIdentification**

Für Europa eindeutige Identifizierung eines Fahrzeugs (amtliches Kennzeichen und Mitgliedstaat).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation — Land, in dem das Fahrzeug zugelassen ist.

vehicleRegistrationNumber — amtliches Kennzeichen des Fahrzeugs (VRN).

2.167. **VehicleRegistrationNumber**

Amtliches Kennzeichen des Fahrzeugs (VRN). Das amtliche Kennzeichen wird von der Fahrzeugzulassungsstelle zugewiesen.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage gibt einen in Kapitel 4 definierten Zeichensatz an,

vehicleRegNumber ein unter Verwendung des spezifizierten Zeichensatzes kodiertes amtliches Kennzeichen.

Wertzuweisung: länderspezifisch.

2.168. **VehicleRegistrationNumberRecordArray**

2. Generation:

Amtliches Kennzeichen des Fahrzeugs plus im Download-Protokoll verwendete Metadaten.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType — Art des Datensatzes (VehicleRegistrationNumber). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VehicleRegistrationNumber in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — der Satz amtlicher Kennzeichen.

2.169. **VuAbility**

2. Generation:

In einer VU gespeicherte Information darüber, ob bei der VU die Nutzung von Fahrtenschreiberkarten der ersten Generation möglich ist (Anhang 1C Randnummer 121).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Wertzuweisung — Oktettanordnung: 'xxxxxxxa'B (8 Bit)

Zur möglichen Unterstützung der 1. Generation:

'a'B	Möglichkeit der Unterstützung von Fahrtenschreiberkarten der 1. Generation:
	'0' B 1. Generation unterstützt,
	'1'B 1. Generation nicht unterstützt,
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

1. Generation:

In einer FE gespeicherte Information zu Tätigkeitsänderungen und/oder Veränderungen des Status der Fahrzeugführung und/oder Veränderungen des Kartenstatus für einen bestimmten Kalendertag (Anhang 1B Randnummer 084 und Anhang 1C Randnummer 105, 106, 107) und des Steckplatzstatus an diesem Tag um 0.00 Uhr.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                INTEGER SIZE(0..1440),
   activityChangeInfos                SET SIZE(noOfActivityChanges) OF
                                      ActivityChangeInfo
}
```

noOfActivityChanges — Anzahl der ActivityChangeInfo-Wörter in der activityChangeInfos-Menge.

activityChangeInfos — Datensatz der in der VU für den Tag gespeicherten ActivityChangeInfo-Wörter. Er enthält stets zwei ActivityChangeInfo-Wörter für den Status der beiden Steckplätze an diesem Tag um 0.00 Uhr.

2.171. **VuActivityDailyRecordArray**

2. Generation:

In einer VU gespeicherte Information zu Tätigkeitsänderungen und/oder Veränderungen des Status der Fahrzeugführung und/oder Veränderungen des Kartenstatus für einen bestimmten Kalendertag (Anhang 1C Randnummer 105, 106, 107) und des Steckplatzstatus an diesem Tag um 0.00 Uhr.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType — Art des Datensatzes (ActivityChangeInfo). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von ActivityChangeInfo in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Datensatz der in der VU für den Tag gespeicherten ActivityChangeInfo-Wörter. Er enthält stets zwei ActivityChangeInfo-Wörter für den Status der beiden Steckplätze an diesem Tag um 0.00 Uhr.

2.172. **VuApprovalNumber**

Typgenehmigungsnummer der Fahrzeugeinheit.

1. Generation:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Wertzuweisung: nicht spezifiziert.

2. Generation:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Wertzuweisung:

Die Genehmigungsnummer muss derjenigen entsprechen, die auf der zugehörigen Website der Europäischen Kommission veröffentlicht ist, und beispielsweise etwaige Bindestriche berücksichtigen. Die Genehmigungsnummer muss linksbündig ausgerichtet sein.

2.173. **VuCalibrationData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu den Kalibrierungen des Kontrollgeräts (Anhang 1B Randnummer 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords — Anzahl der in der vuCalibrationRecords-Menge enthaltenen Datensätze.

vuCalibrationRecords –Menge der Kalibrierungsdatensätze.

2.174. **VuCalibrationRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einer Kalibrierung des Kontrollgeräts (Anhang 1B Randnummer 098 sowie Anhang 1C Randnummern 119 und 120).

1. Generation:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                   CalibrationPurpose,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber,
   workshopCardExpiryDate               TimeReal,
   vehicleIdentificationNumber          VehicleIdentificationNumber,
   vehicleRegistrationIdentification    VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant       W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment        K-ConstantOfRecordingEquipment,
   lTyreCircumference                   L-TyreCircumference,
   tyreSize                             TyreSize,
   authorisedSpeed                      SpeedAuthorised,
   oldOdometerValue                     OdometerShort,
   newOdometerValue                     OdometerShort,
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   nextCalibrationDate                  TimeReal
}
```

calibrationPurpose — Zweck der Kalibrierung.

workshopName, workshopAddress — Name und Anschrift der Werkstatt.

workshopCardNumber dient der Identifizierung der zur Kalibrierung verwendeten Werkstattkarte.

workshopCardExpiryDate — Ablaufdatum der Karte.

vehicleIdentificationNumber — Fahrzeugidentifizierungsnummer (VIN).

vehicleRegistrationIdentification — enthält das amtliche Kennzeichen und den zulassenden Mitgliedstaat.

wVehicleCharacteristicConstant Wegdrehzahl des Fahrzeugs.

kConstantOfRecordingEquipment — Kontrollgerätkonstante.

lTyreCircumference — tatsächlicher Reifenumfang.

tyreSize — Bezeichnung der Größe der am Fahrzeug montierten Reifen.

authorisedSpeed — zulässige Geschwindigkeit des Fahrzeugs.

oldOdometerValue, newOdometerValue — alter und neuer Kilometerstand.

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

nextCalibrationDate — Datum der nächsten von der zugelassenen Prüfstelle durchzuführenden Kalibrierung der in CalibrationPurpose angegebenen Art.

2. Generation:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Zusätzlich zur 1. Generation wird folgendes Datenelementverwendet:

sealDataVu — Informationen zu den an den verschiedenen Fahrzeugkomponenten angebrachten Plomben.

2.175. **VuCalibrationRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu den Kalibrierungen des Kontrollgeräts (Anhang 1C Randnummern 119 und 120).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType — Art des Datensatzes (VuCalibrationRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuCalibrationRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –Menge der Kalibrierungsdatensätze.

2.176. **VuCardIWData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Einsteck- und Entnahmevorgängen von Fahrerkarten oder Werkstattkarten in der Fahrzeugeinheit (Anhang 1B Randnummer 081 und Anhang 1C Randnummer 103).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords — Anzahl der Datensätze in der Menge vuCardIWRecords.

vuCardIWRecords — Datensätze zu Einsteck- und Entnahmevorgängen von Karten.

2.177. **VuCardIWRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einem Einsteck- und Entnahmevorgang einer Fahrerkarte oder Werkstattkarte in der Fahrzeugeinheit (Anhang 1B Randnummer 081 und Anhang 1C Randnummer 102).

1. Generation:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName — Name und Vorname(n) des Inhabers der Fahrer- oder Werkstattkarte in der auf der Karte gespeicherten Form.

fullCardNumber — Art der Karte, ausstellender Mitgliedstaat und Kartennummer in der auf der Karte gespeicherten Form.

cardExpiryDate — Ablaufdatum der Karte in der auf der Karte gespeicherten Form.

cardInsertionTime — Datum und Uhrzeit des Einsteckens.

vehicleOdometerValueAtInsertion — Kilometerstand des Fahrzeugs beim Einstecken der Karte.

cardSlotNumber — Steckplatz, in dem die Karte eingesteckt ist.

cardWithdrawalTime — Datum und Uhrzeit der Entnahme der Karte.

vehicleOdometerValueAtWithdrawal — Kilometerstand des Fahrzeugs bei Kartenentnahme.

previousVehicleInfo enthält Informationen zum zuvor vom Fahrer gefahrenen Fahrzeug in der auf der Karte gespeicherten Form.

manualInputFlag — Merker, der angibt, ob der Karteninhaber beim Einstecken der Karte Fahrertätigkeiten manuell eingegeben hat.

2. Generation:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Anstelle von fullCardNumber wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

fullCardNumberAndGeneration — Art der Karte, ausstellender Mitgliedstaat, Kartennummer und Generation in der auf der Karte gespeicherten Form.

2.178. **VuCardIWRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Einsteck- und Entnahmevorgängen von Fahrerkarten oder Werkstattkarten in der Fahrzeugeinheit (Anhang 1C Randnummer 103).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType — Art des Datensatzes (VuCardIWRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuCardIWRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Datensätze zu Einsteck- und Entnahmevorgängen von Karten.

2.179. **VuCardRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu einer verwendeten Fahrtenschreiberkarte (Anhang 1C Randnummer 132).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber — ausgelesen aus der Datei EF_ICC unter MF der Karte.

cardPersonaliserID — ausgelesen aus der Datei EF_ICC unter MF der Karte.

typeOfTachographCardId — ausgelesen aus der Datei EF_Application_Identification unter DF_Tachograph_G2

cardStructureVersion — ausgelesen aus der Datei EF_Application_Identification unter DF_Tachograph_G2.

cardNumber — ausgelesen aus der Datei EF_Identification unter DF_Tachograph_G2.

2.180. **VuCardRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu den in dieser VU verwendeten Fahrtenschreiberkarten. Diese Information dient der Analyse von Problemen zwischen VU und Karte (Anhang 1C Randnummer 132).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType — Art des Datensatzes (VuCardRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuCardRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Datensätze zu mit der VU verwendeten Fahrtenschreiberkarten.

2.181. **VuCertificate**

Zertifikat des öffentlichen Schlüssels einer Fahrzeugeinheit.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

2. Generation:

VU-Zertifikat plus im Download-Protokoll verwendete Metadaten.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType — Art des Datensatzes (VuCertificate). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuCertificate in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze. Der Wert muss auf 1 gesetzt werden, da die Zertifikate verschieden lang sein können.

records — Satz von VU-Zertifikaten.

2.183. **VuCompanyLocksData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Unternehmenssperren (Anhang 1B Randnummer 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks — Anzahl der in vuCompanyLocksRecords aufgeführten Sperren.

vuCompanyLocksRecords — Datensätze mit Informationen zur Unternehmenssperre.

2.184. **VuCompanyLocksRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einer Unternehmenssperre (Anhang 1B Randnummer 104 und Anhang 1C Randnummer 128).

1. Generation:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime — Datum und Uhrzeit der Sperrung und Entsperrung.

companyName, companyAddress — Name und Anschrift des Unternehmens, auf das sich die Sperrung bezieht.

companyCardNumber — Identifizierung der bei der Sperrung verwendeten Karte.

2. Generation:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Anstelle von companyCardNumber wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

companyCardNumberAndGeneration — Identifizierung der bei der Sperrung verwendeten Karte und ihrer Generation.

2.185. **VuCompanyLocksRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Unternehmenssperren (Anhang 1C Randnummer 128).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType — Art des Datensatzes (VuCompanyLocksRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuCompanyLocksRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze. Wert 0 … 255.

records — Datensätze mit Informationen zur Unternehmenssperre.

2.186. **VuControlActivityData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu unter Verwendung dieser VU ausgeführten Kontrollen (Anhang 1B Randnummer 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls — Anzahl der in vuControlActivityRecords aufgeführten Kontrollen.

vuControlActivityRecords — Kontrollaktivitätsdatensätze.

2.187. **VuControlActivityRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einer unter Verwendung dieser VU ausgeführten Kontrolle (Anhang 1B Randnummer 102 und Anhang 1C Randnummer 126).

1. Generation:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType — Art der Kontrolle.

controlTime — Datum und Uhrzeit der Kontrolle.

controlCardNumber — Identifizierung der für die Kontrolle verwendeten Kontrollkarte.

downloadPeriodBeginTime — Anfangszeit des heruntergeladenen Zeitraums beim Herunterladen.

downloadPeriodEndTime — Endzeit des heruntergeladenen Zeitraums beim Herunterladen.

2. Generation:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Anstelle von controlCardNumber wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

controlCardNumberAndGeneration — Identifizierung der für die Kontrolle verwendeten Kontrollkarte und ihrer Generation.

2.188. **VuControlActivityRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu unter Verwendung dieser VU ausgeführten Kontrollen (Anhang 1C Randnummer 126).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType — Art des Datensatzes (VuControlActivityRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuControlActivityRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –die Menge an VU-Kontrolltätigkeitsdatensätzen.

2.189. **VuDataBlockCounter**

Auf einer Karte gespeicherter Zähler, der sequenziell die Einsteck- und Entnahmevorgänge der Karte in Fahrzeugeinheiten angibt.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Wertzuweisung: Laufende Nummer mit Höchstwert 9999, danach wieder Beginn bei 0.

2.190. **VuDetailedSpeedBlock**

In einer Fahrzeugeinheit gespeicherte Information zur genauen Geschwindigkeit des Fahrzeugs während einer Minute, in der sich das Fahrzeug bewegt hat (Anhang 1B Randnummer 093 und Anhang 1C Randnummer 116).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate — Datum und Uhrzeit des ersten Geschwindigkeitswertes innerhalb des Blocks.

speedsPerSecond — chronologische Reihenfolge der gemessenen Geschwindigkeiten zu jeder Sekunde der Minute, beginnend mit speedBlockBeginDate.

2.191. **VuDetailedSpeedBlockRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zur genauen Geschwindigkeit des Fahrzeugs.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType — Art des Datensatzes (VuDetailedSpeedBlock). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuDetailedSpeedBlock in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der genauen Geschwindigkeitsblöcke.

2.192. **VuDetailedSpeedData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zur genauen Geschwindigkeit des Fahrzeugs.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks — Anzahl der Geschwindigkeitsblöcke in der Menge vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks — Menge der genauen Geschwindigkeitsblöcke.

2.193. **VuDownloadablePeriod**

Ältestes und jüngstes Datum, für das eine Fahrzeugeinheit Daten zu Fahrertätigkeiten enthält (Anhang 1B Randnummern 081, 084 oder 087 und Anhang 1C Randnummern 102, 105, 108).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime — ältestes in der VU gespeichertes Datum des Einsteckens der Karte, einer Tätigkeitsänderung oder einer Ortseingabe und Angabe der entsprechenden Uhrzeit.

maxDownloadableTime — jüngstes in der VU gespeichertes Datum des Einsteckens der Karte, einer Tätigkeitsänderung oder einer Ortseingabe und Angabe der entsprechenden Uhrzeit.

2.194. **VuDownloadablePeriodRecordArray**

2. Generation:

VUDownloadablePeriod und im Download-Protokoll verwendete Metadaten.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType — Art des Datensatzes (VuDownloadablePeriod). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuDownloadablePeriod in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –Menge der VuDownloadablePeriod-Datensätze.

2.195. **VuDownloadActivityData**

In einer Fahrzeugeinheit gespeicherte Information zu ihrem letzten Herunterladen (Anhang 1B Randnummer 105 und Anhang 1C Randnummer 129).

1. Generation:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime — Datum und Uhrzeit des Herunterladens.

fullCardNumber — identifiziert die zur Genehmigung des Herunterladens verwendete Karte.

companyOrWorkshopName — Name des Unternehmens oder der Werkstatt.

2. Generation:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Anstelle von fullCardNumber wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

fullCardNumberAndGeneration — identifiziert die zur Genehmigung des Herunterladens verwendete Karte und ihre Generation.

2.196. **VuDownloadActivityDataRecordArray**

2. Generation:

Information zum letzten VU-Download (Anhang 1C Randnummer 129).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType — Art des Datensatzes (VuDownloadActivityData). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuDownloadActivityData in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — die Menge an Datensätzen zum Herunterladen.

2.197. **VuEventData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Ereignissen (Anhang 1B Randnummer 094, mit Ausnahme Ereignis Geschwindigkeitsüberschreitung).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents — Anzahl der in den vuEventRecords aufgeführten Ereignisse.

vuEventRecords — Ereignisdatensätze.

2.198. **VuEventRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einem Ereignis (Anhang 1B Randnummer 094 und Anhang 1C Randnummer 117, mit Ausnahme Ereignis Geschwindigkeitsüberschreitung).

1. Generation:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType — Art des Ereignisses.

eventRecordPurpose — Zweck der Aufzeichnung dieses Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

cardNumberDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesteckte Karte.

cardNumberCodriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Beifahrer eingesteckte Karte.

cardNumberDriverSlotEnd identifiziert die am Ende des Ereignisses im Steckplatz Fahrer eingesteckte Karte.

cardNumberCodriverSlotEnd identifiziert die am Ende des Ereignisses im SteckplatzBeifahrer eingesteckte Karte.

similarEventsNumber — Anzahl ähnlicher Ereignisse an diesem Tag.

Diese Folge kann für alle Ereignisse mit Ausnahme von Geschwindigkeitsüberschreitungen verwendet werden.

2. Generation:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Zusätzlich zur 1. Generation werden folgende Datenelemente verwendet:

manufacturerSpecificEventFaultData — zusätzliche, herstellerspezifische Informationen zum Ereignis.

Anstelle von cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd und cardNumberCodriverSlotEnd werden in der Datenstruktur der 2. Generation folgende Datenelemente verwendet:

cardNumberAndGenDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenDriverSlotEnd identifiziert die am Ende des Ereignisses im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlotEnd identifiziert die am Ende des Ereignisses im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

Falls es sich bei dem Ereignis um einen Zeitkonflikt handelt, sind eventBeginTime und eventEndTime folgendermaßen zu interpretieren:

eventBeginTime — Datum und Uhrzeit des Kontrollgeräts.

eventEndTime — GNSS-Datum und -Uhrzeit.

2.199. **VuEventRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Ereignissen (Anhang 1C Randnummer 117, mit Ausnahme Ereignis Geschwindigkeitsüberschreitung).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType — Art des Datensatzes (VuEventRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuEventRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der Ereignisdatensätze.

2.200. **VuFaultData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Störungen (Anhang 1B Randnummer 096).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults — Anzahl der in der Menge vuFaultRecords aufgeführten Störungen.

vuFaultRecords — Störungsdatensätze.

2.201. **VuFaultRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einer Störung (Anhang 1B Randnummer 096 und Anhang 1C Randnummer 118).

1. Generation:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType — Art der Kontrollgerätstörung.

faultRecordPurpose — Zweck der Aufzeichnung dieser Störung.

faultBeginTime — Datum und Uhrzeit des Störungsbeginns.

faultEndTime — Datum und Uhrzeit des Störungsendes.

cardNumberDriverSlotBegin identifiziert die zu Beginn der Störung im Steckplatz Fahrer eingesteckte Karte.

cardNumberCodriverSlotBegin identifiziert die zu Beginn der Störung im Steckplatz Beifahrer eingesteckte Karte.

cardNumberDriverSlotEnd identifiziert die zum Zeitpunkt des Endes der Störung im Steckplatz Fahrer eingesteckte Karte.

cardNumberCodriverSlotEnd identifiziert die zum Zeitpunkt des Endes der Störung im Steckplatz Beifahrer eingesteckte Karte.

2. Generation:

```
VuFaultRecord ::= SEQUENCE {
   faultType                            EventFaultType,
   faultRecordPurpose                   EventFaultRecordPurpose,
   faultBeginTime                       TimeReal,
   faultEndTime                         TimeReal,
   cardNumberAndGenDriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd      FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Zusätzlich zur 1. Generation wird folgendes Datenelement verwendet:

manufacturerSpecificEventFaultData — zusätzliche, herstellerspezifische Informationen zur Störung.

Anstelle von cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd und cardNumberCodriverSlotEnd werden in der Datenstruktur der 2. Generation folgende Datenelemente verwendet:

cardNumberAndGenDriverSlotBegin identifiziert die zu Beginn der Störung im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlotBegin identifiziert die zu Beginn der Störung im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenDriverSlotEnd identifiziert die am Ende der Störung im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlotEnd identifiziert die am Ende der Störung im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

2.202. **VuFaultRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Störungen (Anhang 1C Randnummer 118).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType — Art des Datensatzes (VuFaultRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuFaultRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –Störungsdatensätze.

2.203. **VuGNSSCDRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Informationen zur GNSS-Position des Fahrzeugs, wenn die ununterbrochene Lenkzeit des Fahrers ein Vielfaches von drei Stunden erreicht (Anhang 1C Randnummer 108, 110).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp — Datum und Uhrzeit, wann die ununterbrochene Lenkzeit des Karteninhabers ein Vielfaches von drei Stunden erreicht.

cardNumberAndGenDriverSlot — identifiziert die im Steckplatz Fahrer eingesteckte Karte einschließlich ihrer Generation.

cardNumberAndGenCodriverSlot — identifiziert die im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

gnssPlaceRecord — Informationen zur Position des Fahrzeugs.

2.204. **VuGNSSCDRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Informationen zur GNSS-Position des Fahrzeugs, wenn die ununterbrochene Lenkzeit des Fahrers ein Vielfaches von drei Stunden erreicht (Anhang 1C Randnummern 108 und 110).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType — Art des Datensatzes (VuGNSSCDRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuGNSSCDRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –Menge der ununterbrochenen GNSS-Lenkzeitendatensätze-.

2.205. **VuIdentification**

In einer Fahrzeugeinheit gespeicherte Information zur Identifizierung der Fahrzeugeinheit (Anhang 1B Randnummer 075 und Anhang 1C Randnummern 93 und 121).

1. Generation:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName — Name des Herstellers der Fahrzeugeinheit.

vuManufacturerAddress — Anschrift des Herstellers der Fahrzeugeinheit.

vuPartNumber — Teilnummer der Fahrzeugeinheit.

vuSerialNumber — Seriennummer der Fahrzeugeinheit.

vuSoftwareIdentification identifiziert die in der Fahrzeugeinheit implementierte Software.

vuManufacturingDate — Herstellungsdatum der Fahrzeugeinheit.

vuApprovalNumber –Typgenehmigungsnummer der Fahrzeugeinheit.

2. Generation:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

Zusätzlich zur 1. Generation werden folgende Datenelemente verwendet:

vuGeneration –identifiziert die Generation der Fahrzeugeinheit.

vuAbility — enthält Informationen darüber, ob die VU Fahrtenschreiberkarten der 1. Generation unterstützt.

2.206. **VuIdentificationRecordArray**

2. Generation:

VuIdentification und im Download-Protokoll verwendete Metadaten.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType — Art des Datensatzes (VuIdentification). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuIdentification in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der VuIdentification-Datensätze.

2.207. **VuITSConsentRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Informationen zur Zustimmung eines Fahrers, intelligente Verkehrssysteme zu nutzen.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen — identifiziert die Karte und ihre Generation. Bei dieser muss es sich um eine Fahrer- oder Werkstattkarte handeln.

consent — Merker, der angibt, ob der Fahrer der Verwendung intelligenter Verkehrssysteme mit diesem Fahrzeug/dieser Fahrzeugeinheit zugestimmt hat.

Wertzuweisung:

TRUE zeigt die Zustimmung des Fahrers zur Verwendung intelligenter Verkehrssysteme an

FALSE zeigt die Ablehnung des Fahrers betreffend die Verwendung intelligenter Verkehrssysteme an

2.208. **VuITSConsentRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information bezüglich der Zustimmung des Fahrers zur Verwendung intelligenter Verkehrssysteme (Anhang 1C Randnummer 200).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType — Art des Datensatzes (VuITSConsentRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuITSConsentRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Datensätze mit Informationen zur ITS-Zustimmung.

2.209. **VuManufacturerAddress**

Anschrift des Herstellers der Fahrzeugeinheit.

```
VuManufacturerAddress ::= Address
```

Wertzuweisung: nicht spezifiziert.

2.210. **VuManufacturerName**

Name des Herstellers der Fahrzeugeinheit.

```
VuManufacturerName ::= Name
```

Wertzuweisung: nicht spezifiziert.

2.211. **VuManufacturingDate**

Herstellungsdatum der Fahrzeugeinheit.

```
VuManufacturingDate ::= TimeReal
```

Wertzuweisung: nicht spezifiziert.

2.212. **VuOverSpeedingControlData**

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Geschwindigkeitsüberschreitung seit der letzten Kontrolle Geschwindigkeitsüberschreitung (Anhang 1B Randnummer 095 und Anhang 1C Randnummer 117).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime — Datum und Uhrzeit der letzten Kontrolle Geschwindigkeitsüberschreitung.

firstOverspeedSince — Datum und Uhrzeit der ersten Geschwindigkeitsüberschreitung nach dieser Kontrolle Geschwindigkeitsüberschreitung.

numberOfOverspeedSince –Anzahl der Ereignisse Geschwindigkeitsüberschreitung seit der letzten Kontrolle Geschwindigkeitsüberschreitung.

2.213. **VuOverSpeedingControlDataRecordArray**

2. Generation:

VuOverSpeedingControlData und im Download-Protokoll verwendete Metadaten.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType — Art des Datensatzes (VuOverSpeedingControlData). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuOverSpeedingControlData in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Kontrolldatensätze Geschwindigkeitsüberschreitung.

2.214. **VuOverSpeedingEventData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Geschwindigkeitsüberschreitung (Anhang 1B Randnummer 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents — Anzahl der in der Menge vuOverSpeedingEventRecords aufgeführten Ereignisse.

vuOverSpeedingEventRecords — Ereignisdatensätze Geschwindigkeitsüberschreitung.

2.215. **VuOverSpeedingEventRecord**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Ereignissen Geschwindigkeitsüberschreitung (Anhang 1B Randnummer 094 und Anhang 1C Randnummer 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType — Art des Ereignisses.

eventRecordPurpose — Zweck der Aufzeichnung dieses Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

maxSpeedValue — die während des Ereignisses gemessene Höchstgeschwindigkeit.

averageSpeedValue — die während des Ereignisses gemessene arithmetische Durchschnittsgeschwindigkeit.

cardNumberDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesteckte Karte.

similarEventsNumber — Anzahl ähnlicher Ereignisse an diesem Tag.

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Ereignissen Geschwindigkeitsüberschreitung (Anhang 1B Randnummer 094 und Anhang 1C Randnummer 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

Anstelle von cardNumberDriverSlotBegin wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

cardNumberAndGenDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

2.216. **VuOverSpeedingEventRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Geschwindigkeitsüberschreitung (Anhang 1C Randnummer 117).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType — Art des Datensatzes (VuOverSpeedingEventRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuOverSpeedingEventRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Ereignisdatensätze Geschwindigkeitsüberschreitung.

2.217. **VuPartNumber**

Teilnummer der Fahrzeugeinheit.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Wertzuweisung: VU-Herstellerspezifisch

2.218. **VuPlaceDailyWorkPeriodData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zum Ort des Beginns und/oder Endes des Arbeitstages (Anhang 1B Randnummer 087 und Anhang 1C Randnummern 108 und 110).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords — Anzahl der in der Menge vuPlaceDailyWorkPeriodRecords aufgeführten Datensätze.

vuPlaceDailyWorkPeriodRecords — ortsbezogene Datensätze.

2.219. **VuPlaceDailyWorkPeriodRecord**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu einem Ort des Beginns oder Endes des Arbeitstages eines Fahrers (Anhang 1B Randnummer 087 und Anhang 1C Randnummern 108 und 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber — Art der Karte des Fahrers, ausstellender Mitgliedstaat und Kartennummer.

placeRecord enthält die Informationen zum eingegebenen Ort.

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu einem Ort des Beginns oder Endes des Arbeitstages eines Fahrers (Anhang 1B Randnummer 087 und Anhang 1C Randnummern 108 und 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Anstelle von fullCardNumber wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

fullCardNumberAndGeneration — Art der Karte, ausstellender Mitgliedstaat, Kartennummer und Generation in der auf der Karte gespeicherten Form.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zum Ort des Beginns und/oder Endes des Arbeitstages (Anhang 1C Randnummern 108 und 110).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType — Art des Datensatzes (VuPlaceDailyWorkPeriodRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuPlaceDailyWorkPeriodRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — ortsbezogene Datensätze.

2.221. **VuPrivateKey**

1. Generation:

Der private Schlüssel einer Fahrzeugeinheit.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

1. Generation:

Der öffentliche Schlüssel einer Fahrzeugeinheit.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Seriennummer der Fahrzeugeinheit (Anhang 1B Randnummer 075 sowie Anhang 1C Randnummer 93).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Installationsdatum der VU-Softwareversion.

```
VuSoftInstallationDate ::= TimeReal
```

Wertzuweisung: nicht spezifiziert.

2.225. **VuSoftwareIdentification**

In einer Fahrzeugeinheit gespeicherte Information zur installierten Software.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion — Softwareversionsnummer der Fahrzeugeinheit.

vuSoftInstallationDate — Installationsdatum der Softwareversion.

2.226. **VuSoftwareVersion**

Softwareversionsnummer der Fahrzeugeinheit.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Wertzuweisung: nicht spezifiziert.

2.227. **VuSpecificConditionData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu spezifischen Bedingungen.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords — Anzahl der in der Menge specificConditionRecords aufgeführten Datensätze.

specificConditionRecords — Datensätze mit Bezug auf spezifische Bedingungen.

2.228. **VuSpecificConditionRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu spezifischen Bedingungen (Anhang 1C Randnummer 130).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType — Art des Datensatzes (SpecificConditionRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von SpecificConditionRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Datensätze mit Bezug auf spezifische Bedingungen.

2.229. **VuTimeAdjustmentData**

1. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Zeiteinstellungen außerhalb einer normalen Kalibrierung (Anhang 1B Randnummer 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords — Anzahl der in der Menge vuTimeAdjustmentRecords aufgeführten Datensätze.

vuTimeAdjustmentRecords — Zeiteinstellungsdatensätze.

2.230. **VuTimeAdjustmentGNSSRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu einer Zeiteinstellung auf Grundlage der GNSS-Zeitdaten (Anhang 1C Randnummer 124 und 125).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

2.231. **VuTimeAdjustmentGNSSRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu einer Zeiteinstellung auf Grundlage der GNSS-Zeitdaten (Anhang 1C Randnummer 124 und 125).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType — Art des Datensatzes (VuTimeAdjustmentGNSSRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuTimeAdjustmentGNSSRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — GNSS-Zeiteinstellungsdatensätze.

2.232. **VuTimeAdjustmentRecord**

In einer Fahrzeugeinheit gespeicherte Information zu einer Zeiteinstellung außerhalb einer normalen Kalibrierung (Anhang 1B Randnummer 101 und Anhang 1C Randnummern 124 und 125).

1. Generation:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

workshopName, workshopAddress — Name und Anschrift der Werkstatt.

workshopCardNumber — identifiziert die für die Durchführung der Zeiteinstellung verwendete Werkstattkarte.

2. Generation:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Anstelle von workshopCardNumber wird in der Datenstruktur der 2. Generation folgendes Datenelement verwendet:

workshopCardNumberAndGeneration identifiziert die für die Durchführung der Zeiteinstellung verwendete Werkstattkarte und ihre Generation.

2.233. **VuTimeAdjustmentRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu Zeiteinstellungen außerhalb einer normalen Kalibrierung (Anhang 1C Randnummern 124 und 125).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType — Art des Datensatzes (VuTimeAdjustmentRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuTimeAdjustmentRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Zeiteinstellungsdatensätze.

2.234. **WorkshopCardApplicationIdentification**

Auf einer Werkstattkarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Anhang 1C Randnummern 307 und 330).

1. Generation:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion gibt die Version der auf der Karte implementierten Struktur an.

noOfEventsPerType — Anzahl der Ereignisse je Ereignisart, die die Karte speichern kann.

noOfFaultsPerType — Anzahl der Störungen je Störungsart, die die Karte speichern kann.

activityStructureLength — gibt die Zahl der Bytes an, die für die Speicherung von Tätigkeitsdatensätzen zur Verfügung stehen.

noOfCardVehicleRecords — Anzahl der Fahrzeugdatensätze, die die Karte enthalten kann.

noOfCardPlaceRecords — Anzahl der Orte, die die Karte aufzeichnen kann.

noOfCalibrationRecords — Anzahl der Kalibrierungsdatensätze, die die Karte speichern kann.

2. Generation:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Zusätzlich zur 1. Generation werden folgende Datenelemente verwendet:

noOfGNSSCDRecords — Anzahl der ununterbrochenen GNSS-Lenkzeitendatensätze, die die Karte speichern kann.

noOfSpecificConditionRecords — Anzahl der Datensätze mit Bezug auf spezifische Bedingungen, die die Karte speichern kann.

2.235. **WorkshopCardCalibrationData**

Auf einer Werkstattkarte gespeicherte Information zur mit der Karte durchgeführten Werkstatttätigkeit (Anhang 1C Randnummern 314, 316, 337 und 339).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber — Gesamtzahl der mit der Karte durchgeführten Kalibrierungen.

calibrationPointerNewestRecord — Index des zuletzt aktualisierten Kalibrierungsdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Kalibrierungsdatensatzes entspricht, beginnend mit '0' für das erste Auftreten der Kalibrierungsdatensätze in der Struktur.

calibrationRecords — Datensätze mit Informationen zu Kalibrierung und/oder Zeiteinstellung.

2.236. **WorkshopCardCalibrationRecord**

Auf einer Werkstattkarte gespeicherte Information zu einer mit der Karte durchgeführten Kalibrierung (Anhang 1C Randnummern 314 und 337).

1. Generation:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose — Zweck der Kalibrierung.

vehicleIdentificationNumber — Fahrzeugidentifizierungsnummer (VIN).

vehicleRegistration enthält das amtliche Kennzeichen und den zulassenden Mitgliedstaat.

wVehicleCharacteristicConstant — Wegdrehzahl des Fahrzeugs.

kConstantOfRecordingEquipment — Kontrollgerätkonstante.

lTyreCircumference — tatsächlicher Reifenumfang.

tyreSize — Bezeichnung der Größe der am Fahrzeug montierten Reifen.

authorisedSpeed — zulässige Höchstgeschwindigkeit des Fahrzeugs.

oldOdometerValue, newOdometerValue — alter und neuer Kilometerstand.

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

nextCalibrationDate — Datum der nächsten von der zugelassenen Prüfstelle durchzuführenden Kalibrierung der in CalibrationPurpose angegebenen Art.

vuPartNumber, **vuSerialNumber** und **sensorSerialNumber** — Datenelemente zur Identifizierung des Kontrollgeräts.

2. Generation:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Zusätzlich zur 1. Generation werden folgende Datenelementeverwendet:

sensorGNSSSerialNumber — identifiziert eine externe GNSS-Ausrüstung.

rcmSerialNumber — identifiziert das Fernkommunikationsmodul.

sealDataCard — Informationen zu den an den verschiedenen Fahrzeugkomponenten angebrachten Plomben.

2.237. **WorkshopCardHolderIdentification**

Auf einer Werkstattkarte gespeicherte Information zur Identifizierung des Karteninhabers (Anhang 1C Randnummern 311 und 334).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName — Name der Werkstatt des Karteninhabers.

workshopAddress — Anschrift der Werkstatt des Karteninhabers.

cardHolderName — Name und Vorname(n) des Inhabers (z. B. Name des Mechanikers).

cardHolderPreferredLanguage — bevorzugte Sprache des Karteninhabers.

2.238. **WorkshopCardPIN**

PIN-Code (Personal Identification Number) der Werkstattkarte (Anhang 1C Randnummern 309 und 332).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Wertzuweisung: Der dem Karteninhaber bekannte PIN-Code, nach rechts mit 'FF'-Bytes bis zu 8 Bytes aufgefüllt.

2.239. **W-VehicleCharacteristicConstant**

Wegdrehzahl des Fahrzeugs (Begriffsbestimmung k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Wertzuweisung: Impulse je Kilometer im Betriebsbereich 0 bis 64 255 Imp/km.

2.240. **VuPowerSupplyInterruptionRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Unterbrechung der Stromversorgung (Anhang 1C Randnummer 117).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType — Art des Ereignisses.

eventRecordPurpose — Zweck der Aufzeichnung dieses Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

cardNumberAndGenDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenDriverSlotEnd identifiziert die am Ende des Ereignisses im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlotBegin identifiziert die am Ende des Ereignisses im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

similarEventsNumber — Anzahl ähnlicher Ereignisse an diesem Tag.

2.241. **VuPowerSupplyInterruptionRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Unterbrechung der Stromversorgung (Anhang 1C Randnummer 117).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType — Art des Datensatzes (VuPowerSupplyInterruptionRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von VuPowerSupplyInterruptionRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –Ereignisdatensätze Unterbrechung der Stromversorgung.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

2. Generation:

Satz von SensorExternalGNSSCoupledRecord plus im Download-Protokoll verwendete Metadaten.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType — Art des Datensatzes (SensorExternalGNSSCoupledRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von SensorExternalGNSSCoupledRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records –Datensätze Kopplung des -externen GNSS mit dem Sensor.

2.243. **VuSensorPairedRecordArray**

2. Generation:

Satz von SensorPairedRecord plus im Download-Protokoll verwendete Metadaten.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType — Art des Datensatzes (SensorPairedRecord). **Wertzuweisung**: siehe RecordType

recordSize — die Größe von SensorPairedRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Sensorkoppelungsdatensätze.

3. DEFINITIONEN FÜR WERT- UND GRÖSSENBEREICHE

Definition variabler Werte, die für die Definitionen in Abschnitt 2 verwendet werden.

```
TimeRealRange ::= 2^32-1
```

4. ZEICHENSÄTZE

In den IA5Strings werden die ASCII-Zeichen laut Definition in ISO/IEC 8824-1 verwendet. Aus Gründen der Lesbarkeit und zur Bezugnahme ist die Wertzuweisung nachfolgend angegeben. Bei Diskrepanzen mit dieser zu Informationszwecken aufgeführten Angabe gilt stets die Norm ISO/IEC 8824-1.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Andere Zeichenfolgen (Anschrift, Name, VehicleRegistrationNumber) verwenden darüber hinaus die Zeichen der Dezimalzeichencodes 161 bis 255 der folgenden 8-Bit-Standardzeichensätze, spezifiziert durch die Codeseiten-Nummern: Standardzeichensatz	Codeseite (Dezimal)
ISO/IEC 8859-1 Latin-1 Westeuropäisch	1
ISO/IEC 8859-2 Latin-2 Mitteleuropäisch	2
ISO/IEC 8859-3 Latin-3 Südeuropäisch	3
ISO/IEC 8859-5 Latin/Kyrillisch	5
ISO/IEC 8859-7 Latin/Griechisch	7
ISO/IEC 8859-9 Latin-5 Türkisch	9
ISO/IEC 8859-13 Latin-7 Baltisch	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 Südosteuropäisch	16
KOI8-R Latin/Kyrillisch	80
KOI8-U Latin/Kyrillisch	85

5. KODIERUNG

Bei Kodierung anhand der ASN.1-Kodierungsregeln werden alle Datentypen gemäß ISO/IEC 8825-2 (ausgerichtet) kodiert.

6. OBJEKTKENNUNGEN UND ANWENDUNGSBEZEICHNER

6.1. **Objektkennungen**

Die in diesem Kapitel aufgeführten Objektkennungen (OID) sind nur für die 2. Generation von Bedeutung. Diese OID werden in TR-03110-3 definiert und hier der Vollständigkeit halber wiederholt. Die betreffenden OID sind im bsi-de-Teilbaum enthalten:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Protokollkennungen für die VU-Authentisierung

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Beispiel: Wenn die VU-Authentisierung mit SHA-384 erfolgen muss, lautet die zu verwendende Objektkennung (in ASN.1-Notation) `bsi-de protocols(2) smartcard(2) 2 2 4`. Der Wert dieser Objektkennung in Punktnotation lautet `0.4.0.127.0.7.2.2.2.2.4`.

	Do tnotation	Byte notation
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	„04 00 7F 00 07 02 02 02 02 03“
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	„04 00 7F 00 07 02 02 02 02 04“
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	„04 00 7F 00 07 02 02 02 02 05“

Protokollkennungen für die Chip-Authentisierung

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Beispiel: Es wird davon ausgegangen, dass die Chip-Authentisierung per ECDH-Algorithmus erfolgen soll, was zu einer Länge des AES-Sitzungsschlüssels von 128 Bits führt. Dieser Sitzungsschlüssel wird anschließend im CBC-Betriebsmodus verwendet, um den Datenschutz zu gewährleisten, sowie mit dem CMAC-Algorithmus zur Gewährleistung der Datenauthentizität. Somit lautet die zu verwendende Objektkennung (in ASN.1-Notation) `bsi-de protocols(2) smartcard(2) 3 2 2`. Der Wert dieser Objektkennung in Punktnotation lautet `0.4.0.127.0.7.2.2.3.2.2`.

	Punktnotation	Byte-Notation
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. Anwendungskennungen

2. Generation:

Die Anwendungskennung (AID) für die externe GNSS-Ausrüstung (2. Generation) ist durch ‘FF 44 54 45 47 4D’ gegeben. Dies ist eine proprietäre AID gemäß ISO/IEC 7816-4.

Hinweis: Die letzten 5 Bytes kodieren DTEGM für die externe GNSS-Ausrüstung des intelligenten Fahrtenschreibers.

Die Anwendungskennung für die Fahrtenschreiberanwendung der 2. Generation ist durch 'FF 53 4D 52 44 54' gegeben. Dies ist eine proprietäre AID gemäß ISO/IEC 7816-4.

Anlage 2

SPEZIFIKATION DER FAHRTENSCHREIBERKARTEN

INHALTSVERZEICHNIS

1. EINLEITUNG ... 175
1.1. Abkürzungen ... 175
1.2. Referenzdokumente ... 176
2. ELEKTRISCHE UND PHYSIKALISCHE EIGENSCHAFTEN ... 176
2.1. Versorgungsspannung und Stromverbrauch ... 177
2.2. Programmierspannung V_{PP} ... 177
2.3. Taktversorgung und -frequenz ... 177
2.4. E/A-Kontakt ... 177
2.5. Kartenzustände ... 177
3. HARDWARE UND DATENAUSTAUSCH ... 177
3.1. Einleitung ... 177
3.2. Übertragungsprotokoll ... 178
3.2.1 Protokolle ... 178
3.2.2 ATR ... 179
3.2.3 PTS ... 179
3.3. Zugriffsregeln ... 180
3.4. Befehle und Fehlercodes — Übersicht ... 183
3.5. Beschreibung der Befehle ... 185
3.5.1 SELECT ... 186
3.5.2 READ BINARY ... 187
3.5.3 UPDATE BINARY ... 194
3.5.4 GET CHALLENGE ... 200
3.5.5 VERIFY ... 200
3.5.6 GET RESPONSE ... 202
3.5.7 PSO: VERIFY CERTIFICATE ... 202
3.5.8 INTERNAL AUTHENTICATE ... 204
3.5.9 EXTERNAL AUTHENTICATE ... 205
3.5.10 GENERAL AUTHENTICATE ... 206
3.5.11 MANAGE SECURITY ENVIRONMENT ... 207
3.5.12 PSO: HASH ... 210
3.5.13 PERFORM HASH of FILE ... 211
3.5.14 PSO: COMPUTE DIGITAL SIGNATURE ... 212
3.5.15 PSO: VERIFY DIGITAL SIGNATURE ... 213
3.5.16 PROCESS DSRC MESSAGE ... 214
4. STRUKTUR DER FAHRTENSCHREIBERKARTEN ... 216
4.1. Wurzelverzeichnis (MF) ... 216

4.2. Fahrerkartenanwendungen 217
4.2.1 Fahrerkartenanwendung der 1. Generation 217
4.2.2 Fahrerkartenanwendung der 2. Generation 221
4.3. Werkstattkartenanwendungen 224
4.3.1 Werkstattkartenanwendung der 1. Generation 224
4.3.2 Werkstattkartenanwendung der 2. Generation 228
4.4. Kontrollkartenanwendungen 233
4.4.1 Kontrollkartenanwendung der 1. Generation 233
4.4.2 Kontrollkartenanwendung der 2. Generation 235
4.5. Unternehmenskartenanwendungen 237
4.5.1 Unternehmenskartenanwendung der 1. Generation 237
4.5.2 Unternehmenskartenanwendung der 2. Generation 238

1. EINLEITUNG

1.1. **Abkürzungen**

Im Sinne dieser Anlage gelten folgende Abkürzungen.

AC	Access conditions (Zugriffsbedingungen)
AES	Advanced Encryption Standard
AID	Application Identifier (Anwendungskennung)
ALW	Always (immer)
APDU	Application Protocol Data Unit (Befehlsstruktur)
ATR	Aswer To Reset (Antwort auf Zurücksetzen)
AUT	Authenticated (authentisiert)
C6, C7	Kontakte Nr. 6 und 7 der Karte laut Beschreibung in ISO/IEC 7816-2
cc	Taktgeberzyklen
CHV	Card holder Verification Information (Information zur Überprüfung des Karteninhabers)
CLA	Klassenbyte eines APDU-Befehls
DSRC	Dedicated Short Range Communication (Dedizierte Nahbereichskommunikation)
DF	Dedicated File (Verzeichnis). Ein DF kann andere Dateien enthalten (EF oder DF)
ECC	Elliptic Curve Cryptography (Elliptische-Kurven-Kryptografie)
EF	Elementary File (Elementardatei)
etu	elementary time unit (Elementarzeiteinheit)
G1	1. Generation
G2	2. Generation
IC	Integrated Circuit (Integrierter Schaltkreis)
ICC	Integrated Circuit Card (Chipkarte)
ID	Identifier (Bezeichner, Kennung)
IFD	Interface Device (Schnittstellengerät, Kartenterminal)
IFS	Information Field Size (Informationsfeldgröße)
IFSC	Informationsfeldgröße der Karte

IFSD	Informationsfeldgröße des Schnittstellengeräts, Terminals
INS	Befehlsbyte eines APDU-Befehls
Lc	Länge der Eingabedaten für einen APDU-Befehl
Le	Länge der erwarteten Daten (Ausgabedaten für einen Befehl)
MF	Master File (Wurzel-DF)
NAD	Knotenadresse, verwendet im Protokoll T=1
NEV	Never (nie)
P1-P2	Parameterbytes
PIN	Persönliche Geheimzahl (Personal Identification Number)
PRO SM	Mit Secure Messaging geschützt
PTS	Protocol Transmission Selection (Auswahl der Protokollübertragung)
RFU	Reserved for Future Use (für künftige Anwendungen reserviert)
RST	Zurücksetzen (der Karte)
SFID	Kurz-Elementardateikennung
SM	Secure Messaging
SW1-SW2	Statusbytes
TS	ATR-Anfangszeichen
VPP	Programmierspannung
VU	Fahrzeugeinheit
XXh	Wert XX in Hexadezimalnotation
'XXh'	Wert XX in Hexadezimalnotation
||	Verkettungssymbol 03||04=0304

1.2. **Referenzdokumente**

In dieser Anlage werden folgende Referenzdokumente herangezogen:

ISO/IEC 7816-2 Identification cards — Integrated circuit cards — Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards — Integrated circuit cards — Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Berichtigung 1: 2014.

ISO/IEC 7816-6 Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards — Integrated circuit cards — Part 8: Commands for security operations. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011

2. ELEKTRISCHE UND PHYSIKALISCHE EIGENSCHAFTEN

TCS_01 Sofern nicht anderweitig spezifiziert, erfüllen alle elektronischen Signale die Norm ISO/IEC 7816-3.

TCS_02 Maße und Anordnung der Kartenkontakte erfüllen die Norm ISO/IEC 7816-2.

2.1. **Versorgungsspannung und Stromverbrauch**

TCS_03 Die Karte arbeitet gemäß Spezifikation innerhalb der Grenzen für die Leistungsaufnahme nach ISO/IEC 7816-3.

TCS_04 Die Karte arbeitet mit Vcc = 3 V (± 0,3 V) oder mit Vcc = 5 V (± 0,5 V).

Die Spannungswahl erfolgt gemäß ISO/IEC 7816-3.

2.2. **Programmierspannung V_{pp}**

TCS_05 Die Karte benötigt am Kontakt C6 keine Programmierspannung. Es wird davon ausgegangen, dass Kontakt C6 in einem Schnittstellengerät nicht angeschlossen ist. Der Kontakt C6 kann an V_{cc} auf der Karte angeschlossen sein, aber nicht an Masse. Auf jeden Fall ist diese Spannung nicht zu interpretieren.

2.3. **Taktversorgung und -frequenz**

TCS_06 Die Karte arbeitet im Frequenzbereich von 1 bis 5 MHz und kann unter Umständen höhere Frequenzen unterstützen. Innerhalb eines Kartenvorgangs darf die Taktfrequenz um ± 2 % schwanken. Die Taktfrequenz wird von der Fahrzeugeinheit und nicht von der Karte selbst erzeugt. Für den Arbeitszyklus ist eine Schwankung zwischen 40 und 60 % zulässig.

TCS_07 Unter den in der Kartendatei EF ICC enthaltenen Bedingungen kann der externe Taktgeber angehalten werden. Das erste Byte des Hauptteils der EF ICC-Datei kodiert die Bedingungen für den Clockstop-Modus:

L-Pegel	H-Pegel		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop zulässig, kein Vorzugspegel
0	1	1	Clockstop zulässig, Vorzugspegel: H
1	0	1	Clockstop zulässig, Vorzugspegel: L
0	0	0	Clockstop nicht zulässig
0	1	0	Clockstop nur bei H-Pegel zulässig
1	0	0	Clockstop nur bei L-Pegel zulässig

Bits 4 bis 8 werden nicht genutzt.

2.4. **E/A-Kontakt**

TCS_08 Der E/A-Kontakt C7 wird für den Empfang von Daten vom Schnittstellengerät und das Senden von Daten zum Schnittstellengerät verwendet. Während des Betriebs befindet sich entweder die Karte oder das Schnittstellengerät im Sendemodus. Sollten sich beide Einheiten im Sendemodus befinden, darf die Karte dadurch nicht beschädigt werden. Sofern die Karte nicht sendet, tritt sie in den Empfangsmodus.

2.5. **Kartenzustände**

TCS_09 Bei angelegter Versorgungsspannung arbeitet die Karte in zwei Zuständen:

im Betriebszustand während der Ausführung von Befehlen oder während der Verbindung zur Digitaleinheit,

im Ruhezustand zu allen anderen Zeiten; in diesem Zustand bleiben alle Daten auf der Karte erhalten.

3. HARDWARE UND DATENAUSTAUSCH

3.1. **Einleitung**

Dieser Abschnitt beschreibt die für die Fahrtenschreiberkarten und Fahrzeugeinheit (VU) erforderliche Mindestfunktionalität, mit der ein korrekter Betrieb und Interoperabilität gewährleistet werden.

Fahrtenschreiberkarten erfüllen so weit wie möglich die geltenden ISO/IEC-Normen (insbesondere ISO/IEC 7816). Befehle und Protokolle werden jedoch vollständig beschrieben, um gegebenenfalls bestimmte eingeschränkte Verwendungen oder Unterschiede herauszustellen. Die spezifizierten Befehle entsprechen, sofern nicht anders angegeben, in vollem Umfang den angeführten Normen.

3.2. **Übertragungsprotokoll**

TCS_10 Das Übertragungsprotokoll entspricht den Festlegungen von ISO/IEC 7816-3 für T = 0 und T = 1. Insbesondere erkennt die VU von der Karte gesendete Wartezeitverlängerungen.

3.2.1 *Protokolle*

TCS_11 Die Karte unterstützt sowohl Protokoll **T=0** als auch Protokoll **T=1**. Darüber hinaus kann die Karte weitere kontaktorientierte Protokolle unterstützen.

TCS_12 **T=0** ist das Standardprotokoll; zum Wechsel auf das Protokoll **T=1** ist daher ein **PTS**-Befehl erforderlich.

TCS_13 Die Geräte unterstützen in beiden Protokollen die „**direct convention**“, die somit für die Karte obligatorisch ist.

TCS_14 Das Byte für die **Informationsfeldgröße der Karte** wird im ATR im Zeichen TA3 dargestellt. Dieser Wert beträgt mindestens ‘F0h’ (= 240 Bytes).

Für die Protokolle gelten die folgenden Einschränkungen:

TCS_15 **T=0**

— Das Schnittstellengerät unterstützt eine Antwort bei E/A nach der ansteigenden Flanke des Signals bei RST von 400 cc.

— Das Schnittstellengerät muss Zeichen im Abstand von 12 etu lesen können.

— Das Schnittstellengerät liest ein fehlerhaftes Zeichen und dessen Wiederholung, wenn der Abstand 13 etu beträgt. Wird ein fehlerhaftes Zeichen festgestellt, kann das Fehlersignal bei E/A zwischen 1 etu und 2 etu auftreten. Das Gerät unterstützt eine Verzögerung von 1 etu.

— Das Schnittstellengerät akzeptiert ein ATR von 33 Bytes (TS+32).

— Befindet sich TC1 im ATR, ist für vom Schnittstellengerät gesendete Zeichen die Extra Guard Time vorhanden, obwohl von der Karte gesendete Zeichen weiterhin mit 12 etu getrennt werden können. Dies gilt auch für das von der Karte gesendete ACK-Zeichen nach Aussendung eines P3-Zeichens vom Schnittstellengerät.

— Das Schnittstellengerät berücksichtigt ein von der Karte ausgesendetes NUL-Zeichen.

— Das Schnittstellengerät akzeptiert den Ergänzungsmodus für ACK.

— Der Befehl GET RESPONSE kann im Verkettungsmodus nicht zum Einholen von Daten verwendet werden, deren Länge 255 Bytes übersteigen könnte.

TCS_16 **T=1**

— NAD-Byte: nicht verwendet (NAD ist auf ‘00’ gesetzt).

— S-Block ABORT: nicht verwendet.

— S-Block VPP-Zustandsfehler: nicht verwendet.

— Die Gesamtverkettungslänge für ein Datenfeld darf 255 Bytes (vom Schnittstellengerät abzusichern) nicht übersteigen.

— Die Information Field Size Device (IFSD) wird vom Schnittstellengerät unmittelbar nach dem ATR angezeigt: Das Schnittstellengerät überträgt die S-Block IFS-Anforderung nach dem ATR, und die Karte sendet S-Block IFS zurück. Der empfohlene Wert für IFSD ist 254 Bytes.

— Die Karte fordert keine IFS-Nachkorrektur an.

3.2.2 *ATR*

TCS_17 Das Gerät überprüft ATR-Bytes gemäß ISO/IEC 7816-3. Es erfolgt keine Überprüfung von historischen ATR-Zeichen.

Beispiel für ein Zweiprotokoll-Basis-ATR gemäß ISO/IEC 7816-3

Zeichen	Wert	Bemerkungen
TS	'3Bh'	Anzeiger für „direct convention".
T0	'85h'	TD1 vorhanden; 5 historische Bytes vorhanden
TD1	'80h'	TD2 vorhanden; T=0 verwenden
TD2	'11h'	TA3 vorhanden; T=1 verwenden
TA3	'XXh' (mind. 'F0h')	Informationsfeldgröße der Karte (IFSC)
TH1 bis TH5	'XXh'	Historische Zeichen
TCK	'XXh'	Prüfzeichen (ohne OR)

TCS_18 Nach der Antwort auf das Zurücksetzen (ATR) wird das Wurzelverzeichnis (MF) implizit ausgewählt und zum aktuellen Verzeichnis.

3.2.3 *PTS*

TCS_19 Das Standardprotokoll ist T=0. Zur Einstellung des Protokolls T=1 muss ein PTS (auch PPS genannt) vom Gerät gesendet werden.

TCS_20 Da für die Karte beide Protokolle, T=0 und T=1, obligatorisch sind, ist das Basis-PTS für die Protokollumschaltung ebenfalls obligatorisch.

Wie in ISO/IEC 7816-3 angegeben, kann das PTS zur Umschaltung auf höhere Übertragungsraten als die von der Karte im ATR vorgeschlagene Geschwindigkeit verwendet werden (TA(1) Byte).

Höhere Übertragungsraten sind für die Karte fakultativ.

TCS_21 Wird keine andere Übertragungsrate als die Standardgeschwindigkeit unterstützt (oder wird die ausgewählte Übertragungsrate nicht unterstützt), antwortet die Karte auf das PTS korrekt gemäß ISO/IEC 7816-3 durch Weglassen des PPS1-Byte.

Beispiele für ein Basis-PTS zur Protokollwahl:

Zeichen	Wert	Bemerkungen
PPSS	'FFh'	Startzeichen
PPS0	'00h' oder '01h'	PPS1 bis PPS3 nicht vorhanden; '00h' zur Auswahl von T0, '01h' zur Auswahl von T1.
PK	'XXh'	Prüfzeichen: 'XXh' = 'FFh' wenn PPS0 = '00h', 'XXh' = 'FEh' wenn PPS0 = '01h',

3.3. **Zugriffsregeln**

TCS_22 Eine Zugriffsregel legt für einen Zugriffsmodus, d. h. Befehl, die zugehörigen Sicherheitsbedingungen fest. Sind diese Sicherheitsbedingungen erfüllt, wird der entsprechende Befehl verarbeitet.

TCS_23 Für die Fahrtenschreiberkarte werden folgende Sicherheitsbedingungen genutzt:

Abkürzung	Bedeutung
ALW	Die Aktion ist immer möglich und kann ohne Einschränkung ausgeführt werden. Befehls- und Antwort-APDU werden als Klartext übermittelt, d. h. ohne Secure Messaging.
NEV	Die Aktion ist nie möglich.
PLAIN-C	Die Befehls-APDU werden als Klartext übermittelt, d. h. ohne Secure Messaging.
PWD	Die Aktion wird nur ausgeführt, wenn die PIN der Werkstattkarte erfolgreich verifiziert wurde, d. h. der interne Sicherheitsstatus der Karte auf „PIN_Verified“ gesetzt ist. Der Befehl muss ohne Secure Messaging übertragen werden.
EXT-AUT-G1	Die Aktion kann nur ausgeführt werden, wenn der Befehl External Authenticate für die Authentisierung der 1. Generation (siehe auch Anlage 11 Teil A) erfolgreich ausgeführt wurde.
SM-MAC-G1	Die (Befehls- und Antwort-) APDU muss mit Secure Messaging der 1. Generation im reinen Authentisierungsmodus angewandt werden (siehe Anlage 11 Teil A).
SM-C-MAC-G1	Die (Befehls-)APDU muss mit Secure Messaging der 1. Generation im reinen Authentisierungsmodus angewandt werden (siehe Anlage 11 Teil A).
SM-R-ENC-G1	Die Antwort-APDU muss mit Secure Messaging der 1. Generation im Verschlüsselungsmodus angewandt werden (siehe Anlage 11 Teil A), d. h. so, dass kein Code für die Nachrichtenauthentisierung zurückgesendet wird.
SM-R-ENC-MAC-G1	Die (Antwort-) APDU muss mit Secure Messaging der 1. Generation im Verschlüsselungs-dann-Authentisierungsmodus angewandt werden (siehe Anlage 11 Teil A).
SM-MAC-G2	Die (Befehls- und Antwort-) APDU muss mit Secure Messaging der 2. Generation im reinen Authentisierungsmodus angewandt werden (siehe Anlage 11 Teil B).
SM-C-MAC-G2	Die (Befehls-) APDU muss mit Secure Messaging der 2. Generation im reinen Authentisierungsmodus angewandt werden (siehe Anlage 11 Teil B).
SM-R-ENC-MAC-G2	Die (Antwort-) APDU muss mit Secure Messaging der 2. Generation im Verschlüsselungs-dann-Authentisierungsmodus angewandt werden (siehe Anlage 11 Teil B).

TCS_24 Diese Sicherheitsbedingungen können folgendermaßen verknüpft werden:

AND: Alle Sicherheitsbedingungen müssen erfüllt sein.

OR: Mindestens eine Sicherheitsbedingung muss erfüllt sein.

Die Zugriffsregeln für das Dateisystem, d. h. die Befehle SELECT, READ BINARY und UPDATE BINARY sind in Kapitel 4 spezifiziert. Die Zugriffsregeln für die verbleibenden Befehle sind in den folgenden Tabellen beschrieben.

TCS_25 In der Anwendung DF Tachograph der 1. Generation kommen folgende Zugriffsregeln zum Einsatz:

Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmens-karte
External Authenticate				
— Zur Authentisierung für die 1. Generation	ALW	ALW	ALW	ALW
— Zur Authentisierung für die 2 Generation	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nicht zutreffend	Nicht zutreffend
PSO: Hash	Nicht zutreffend	Nicht zutreffend	ALW	Nicht zutreffend
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nicht zutreffend	Nicht zutreffend
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nicht zutreffend	Nicht zutreffend	ALW	Nicht zutreffend
Verify	Nicht zutreffend	ALW	Nicht zutreffend	Nicht zutreffend

TCS_26 In der Anwendung DF Tachograph der 2. Generation kommen folgende Zugriffsregeln zum Einsatz:

Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmens-karte
External Authenticate				
— Zur Authentisierung für die 1. Generation	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
— Zur Authentisierung für die 2 Generation	ALW	PWD	ALW	ALW
Internal Authenticate	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmens-karte
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Mes-sage	Nicht zutreffend	ALW	ALW	Nicht zutreffend
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nicht zutreffend	Nicht zutreffend
PSO: Hash	Nicht zutreffend	Nicht zutreffend	ALW	Nicht zutreffend
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nicht zutreffend	Nicht zutreffend
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nicht zutreffend	Nicht zutreffend	ALW	Nicht zutreffend
Verify	Nicht zutreffend	ALW	Nicht zutreffend	Nicht zutreffend

TCS_27 In MF kommen folgende Zugriffsregeln zum Einsatz:

Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmens-karte
External Authenticate				
— Zur Authentisie-rung für die 1. Ge-neration	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
— Zur Authentisie-rung für die 2 Ge-neration	ALW	PWD	ALW	ALW
Internal Authenticate	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Mes-sage	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmens-karte
PSO: Compute Digital Signature	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PSO: Hash	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PSO: Hash of File	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Nicht zutreffend	ALW	Nicht zutreffend	Nicht zutreffend

TCS_28 Eine Fahrtenschreiberkarte kann unter Umständen Befehle eines Sicherheitsniveaus akzeptieren, das über dem in den Sicherheitsbedingungen festgelegten Niveau liegt, d. h. bei den Sicherheitsbedingungen ALW (oder PLAIN-C) kann die Karte Befehle mit Secure Messaging (Verschlüsselungs- und/oder Authentisierungsmodus) akzeptieren. Falls die Sicherheitsbedingungen Secure Messaging mit Authentisierungsmodus voraussetzen, kann die Fahrtenschreiberkarte Befehle mit Secure Messaging der gleichen Generation im Authentisierungs- und Verschlüsselungsmodus akzeptieren.

Hinweis: Die Beschreibung der Befehle liefert weitere Informationen zur Unterstützung der Befehle für die verschiedenen Fahrtenschreiberkartentypen und DF.

3.4. Befehle und Fehlercodes — Übersicht

Befehle und Dateiorganisation sind von der ISO/IEC 7816-4 abgeleitet und erfüllen diese Norm.

Dieser Abschnitt beschreibt die folgenden APDU-Befehl-Antwort-Paare. Die durch die Anwendungen der 1. und 2. Generation unterstützten Befehlsvarianten sind in der zugehörigen Befehlsbeschreibung angegeben.

Befehl	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Befehl	INS
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 In jeder Antwortnachricht werden die Statusbytes SW1 SW2 zurückgesendet, die den Verarbeitungszustand des Befehls bezeichnen.

SW1	SW2	Bedeutung
90	00	Normale Verarbeitung
61	XX	Normale Verarbeitung. XX = Zahl der verfügbaren Antwortbytes
62	81	Verarbeitungswarnung. Ein Teil der zurückgesendeten Daten kann beschädigt sein
63	00	Authentisierung fehlgeschlagen (Warnung)
63	CX	Falsche CHV (PIN). Zähler für verbleibende Versuche „X“.
64	00	Ausführungsfehler — Zustand des nichtflüchtigen Speichers unverändert. Integritätsfehler.
65	00	Ausführungsfehler — Zustand des nichtflüchtigen Speichers verändert
65	81	Ausführungsfehler — Zustand des nichtflüchtigen Speichers verändert — Speicherfehler
66	88	Sicherheitsfehler: falsche kryptografische Prüfsumme (bei Secure Messaging) oder falsches Zertifikat (bei Zertifikatsverifizierung) oder falsches Kryptogramm (bei externer Authentisierung) oder falsche Signatur (bei Signaturverifizierung)
67	00	Falsche Länge (falsche Lc oder Le)
68	82	Secure Messaging nicht unterstützt
68	83	Letzter Befehl der Kette erwartet
69	00	Verbotener Befehl (keine Antwort verfügbar in T=0)
69	82	Sicherheitsstatus nicht erfüllt
69	83	Authentisierungsverfahren blockiert
69	85	Nutzungsbedingungen nicht erfüllt
69	86	Befehl nicht zulässig (keine aktuelle EF)

SW1	SW2	Bedeutung
69	87	Erwartete Secure-Messaging-Datenobjekte fehlen
69	88	Inkorrekte Secure-Messaging-Datenobjekte
6A	80	Falsche Parameter im Datenfeld
6A	82	Datei nicht gefunden
6A	86	Falsche Parameter P1-P2
6A	88	Bezugsdaten nicht gefunden
6B	00	Falsche Parameter (Offset außerhalb der EF)
6C	XX	Falsche Länge, SW2 gibt die genaue Länge an. Kein Datenfeld wird zurückgesendet.
6D	00	Befehlscode nicht unterstützt oder ungültig.
6E	00	Klasse nicht unterstützt
6F	00	Sonstige Prüffehler

TCS_30 Erfüllt ein einzelner APDU-Befehl mehr als eine Fehlerbedingung, kann die Karte beliebige der zugehörigen Statusbytes zurücksenden.

3.5. **Beschreibung der Befehle**

In diesem Kapitel werden die obligatorischen Befehle für die Fahrtenschreiberkarten beschrieben.

Weitere sachdienliche Einzelheiten zu kryptografischen Operationen sind in Anlage 11, Gemeinsame Sicherheitsmechanismen für Fahrtenschreiber der 1. und 2. Generation, aufgeführt.

Alle Befehle werden unabhängig vom verwendeten Protokoll (T=0 oder T=1) beschrieben. Die APDU-Bytes CLA, INS, P1, P2, Lc und Le werden immer angegeben. Wird Lc oder Le für den beschriebenen Befehl nicht benötigt, bleiben die entsprechende Länge, der Wert und die Beschreibung leer.

TCS_31 Werden beide Längenbytes (Lc und Le) angefordert, ist der Befehl in zwei Teile aufzuspalten, wenn das IFD das Protokoll T=0 verwendet: Das IFD sendet den Befehl wie beschrieben mit P3=Lc + Daten und sendet dann einen GET RESPONSE-Befehl (siehe Abschnitt 3.5.6) bei P3=Le.

TCS_32 Wenn beide Längenbytes angefordert werden und wenn Le=0 (Secure Messaging) gilt Folgendes:

— Bei Verwendung von Protokoll T=1 antwortet die Karte auf Le=0 mit dem Senden aller verfügbaren Ausgabedaten.

— Bei Verwendung von Protokoll T=0 sendet das IFD den ersten Befehl mit P3=Lc + Daten und die Karte antwortet auf dieses implizierte Le=0 mit den Statusbytes '**61La**', wobei La die Anzahl der verfügbaren Antwortbytes ist. Daraufhin generiert das IFD einen GET RESPONSE-Befehl mit P3=La zum Lesen der Daten.

TCS_33 Optional kann eine Fahrtenschreiberkarte erweiterte Längenfelder gemäß ISO/IEC 7816-4 unterstützen. Eine Fahrtenschreiberkarte, die erweiterte Längenfelder unterstützt,

— gibt die Unterstützung erweiterter Längenfelder in der ATR an

— gibt die unterstützten Puffergrößen durch erweiterte Längenangabe in der EF ATR/INFO an, siehe TCS_146

— gibt die Unterstützung erweiterter Längenfelder für T = 1 und/oder T = 0 in der EF Extended Length an, siehe TCS_147

— unterstützt erweiterte Längenfelder für die Fahrtenschreiberanwendung der 1. und 2. Generation.

Hinweise:

Sämtliche Befehle sind für kurze Längenfelder spezifiziert. Die Verwendung von APDU erweiterter Länge ergibt sich aus ISO/IEC 7816-4.

Generell sind die Befehle für den Klarmodus spezifiziert, d. h. ohne Secure Messaging, da die Secure-Messaging-Schicht in Anlage 11 beschrieben wird. Aus den Zugriffsregeln für einen Befehl ergibt sich, ob der Befehl Secure Messaging unterstützt und ob sich die Unterstützung auf Secure Messaging der 1. und/oder 2. Generation bezieht. Einige Befehlsvarianten werden mit Secure Messaging beschrieben, um die Verwendung dieser Funktion zu veranschaulichen.

TCS_34 Die VU führt für eine Sitzung das gesamte Protokoll zur gegenseitigen Authentisierung von VU der 2. Generation und Karte aus, einschließlich (erforderlichenfalls) der Zertifikatsverifizierung entweder im DF Tachograph, dem DF Tachograph_G2 oder in MF.

3.5.1 *SELECT*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl SELECT wird verwendet:

— zur Auswahl eines Applikations-DF (Auswahl nach Namen obligatorisch)

— zur Auswahl einer Elementardatei, die der vorgelegten Datei-ID entspricht.

3.5.1.1 Auswahl nach Namen (AID)

Dieser Befehl ermöglicht die Auswahl eines Applikations-DF auf der Karte.

TCS_35 Dieser Befehl kann von jeder beliebigen Stelle in der Dateistruktur aus ausgeführt werden (nach dem ATR oder jederzeit).

TCS_36 Bei Auswahl einer Anwendung wird die derzeitige Sicherheitsumgebung zurückgesetzt. Nach Auswahl der Anwendung wird kein aktueller öffentlicher Schlüssel mehr ausgewählt. Die Zugriffsbedingung EXT-AUT-G1 geht ebenfalls verloren. Wurde der Befehl ohne Secure Messaging ausgeführt, stehen die früheren Sitzungsschlüssel nicht mehr für das Secure Messaging zur Verfügung.

TCS_37 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Auswahl nach Namen (AID)
P2	1	'0Ch'	Keine Antwort erwartet
Lc	1	'NNh'	Anzahl der an die Karte gesendeten Bytes (Länge der AID): '06h' für die Fahrtenschreiberanwendung
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' für die Fahrtenschreiberanwendung der 1. Generation AID: 'FF 53 4D 52 44 54' für die Fahrtenschreiberanwendung der 2. Generation

Es wird keine Antwort auf den Befehl SELECT benötigt (Le fehlt in T=1 oder keine Antwort angefordert in T=0).

TCS_38 **Antwortnachricht (keine Antwort angefordert)**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Wird die der AID entsprechende Anwendung nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus '**6A82**'.

— Bei Vorhandensein des Byte Le lautet in T=1 der zurückgesendete Status '**6700**'.

— Wenn nach dem Befehl SELECT eine Antwort angefordert wird, lautet in T=0 der zurückgesendete Status '**6900**'.

— Wird die ausgewählte Anwendung als verfälscht betrachtet (weil in den Dateiattributen ein Integritätsfehler festgestellt wurde), lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

3.5.1.2 Auswahl einer Elementardatei anhand ihrer Dateikennung

TCS_39 **Befehlsnachricht**

TCS_40 Die Fahrtenschreiberkarte muss Secure Messaging der 2. Generation gemäß Anlage 11 Teil B für diese Befehlsvarianten unterstützen.

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Auswahl einer EF unter dem aktuellen DF
P2	1	'0Ch'	Keine Antwort erwartet
Lc	1	'02h'	Anzahl der an die Karte gesendeten Bytes
#6-#7	2	'XXXXh'	Dateikennung

Es wird keine Antwort auf den Befehl SELECT benötigt (Le fehlt in T=1 oder keine Antwort angefordert in T=0).

TCS_41 **Antwortnachricht (keine Antwort angefordert)**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Wird die der Dateikennung entsprechende Datei nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus '**6A82**'.

— Bei Vorhandensein des Byte Le lautet in T=1 der zurückgesendete Status '**6700**'.

— Wenn nach dem Befehl SELECT eine Antwort angefordert wird, lautet in T=0 der zurückgesendete Status '**6900**'.

— Wird die ausgewählte Datei als verfälscht betrachtet (weil in den Dateiattributen ein Integritätsfehler festgestellt wurde), lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

3.5.2 *READ BINARY*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl READ BINARY wird zum Auslesen von Daten aus einer transparenten Datei verwendet.

Die Antwort der Karte besteht im Zurücksenden der gelesenen Daten, die optional in einer Secure-Messaging-Struktur eingekapselt werden können.

3.5.2.1 Befehl mit Offset in P1-P2

Dieser Befehl ermöglicht dem IFD das Lesen von Daten aus der zu dem entsprechenden Zeitpunkt ausgewählten EF ohne Secure Messaging.

Hinweis: Dieser Befehl ohne Secure Messaging kann nur genutzt werden, um eine Datei auszulesen, die die ALW-Sicherheitsbedingung für den Lese-Zugriffsmodus unterstützt.

TCS_42 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Offset in Bytes vom Dateianfang: höchstwertiges Byte
P2	1	'XXh'	Offset in Bytes vom Dateianfang: niedrigstwertiges Byte
Le	1	'XXh'	Erwartete Datenlänge. Anzahl der zu lesenden Bytes.

Hinweis: Bit 8 von P1 muss auf 0 gesetzt sein.

TCS_43 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#X	X	'XX..XXh'	Gelesene Daten
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist keine EF ausgewählt, lautet der zurückgesendete Verarbeitungsstatus '**6986**'.

— Sind die Sicherheitsbedingungen der ausgewählten Datei nicht erfüllt, wird der Befehl mit '**6982**' abgebrochen.

— Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6B00**'.

— Ist die Größe der auszulesenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6700**' oder '**6Cxx**', wobei 'xx' die genaue Länge angibt.

— Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wiederherstellbar und der zurückgesendete Verarbeitungsstatus lautet '**6400**' oder '**6581**'.

— Wird in den gespeicherten Daten ein Integritätsfehler festgestellt, so gibt die Karte die angeforderten Daten aus und der zurückgesendete Verarbeitungsstatus lautet '**6281**'.

3.5.2.1.1 Befehl mit Secure Messaging (Beispiele)

Dieser Befehl ermöglicht dem IFD das Lesen von Daten aus der zu dem entsprechenden Zeitpunkt ausgewählten EF mit Secure Messaging, um die Integrität der empfangenen Daten zu überprüfen und die Vertraulichkeit der Daten bei als verschlüsselt gekennzeichneter SM-R-ENC-MAC-G1 (1. Generation) oder SM-R-ENC-MAC-G2 (2. Generation) zu schützen.

TCS_44 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'0Ch'	Secure Messaging angefordert
INS	1	'B0h'	Read Binary
P1	1	'XXh'	P1 (Offset in Bytes vom Dateianfang): höchstwertiges Byte
P2	1	'XXh'	P2 (Offset in Bytes vom Dateianfang): niedrigstwertiges Byte
Lc	1	'XXh'	Länge der Eingabedaten für Secure Messaging
#6	1	'97h'	T_{LE}: Tag zur Spezifikation der erwarteten Länge
#7	1	'01h'	L_{LE}: Erwartete Länge
#8	1	'NNh'	Spezifikation der erwarteten Länge (Original Le): Anzahl der zu lesenden Bytes
#9	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#10	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '04h' für Secure Messaging der 1. Generation (siehe Anlage 11 Teil A) '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#11-#(10+L)	L	'XX..XXh'	Kryptografische Prüfsumme
Le	1	'00h'	Gemäß ISO/IEC 7816-4

TCS_45 **Antwortnachricht, wenn SM-R-ENC-MAC-G1 (1. Generation)/SM-R-ENC-MAC-G2 (2. Generation) nicht erforderlich und Secure-Messaging-Eingabeformat korrekt:**

Byte	Länge	Wert	Beschreibung
#1	1	'99h'	Tag für Verarbeitungsstatus (SW1-SW2) — optional für Secure Messaging der 1. Generation
#2	1	'02h'	Länge des Verarbeitungsstatus
#3 — #4	2	'XX XXh'	Verarbeitungsstatus der ungeschützten APDU-Antwort
#5	1	'81h'	T_{PV}: Tag für Klarwertdaten
#6	L	'NNh' oder '81 NNh'	L_{PV}: Länge der zurückgesendeten Daten (= Original Le). L gleich 2 Bytes, wenn L_{PV} > 127 Bytes

Byte	Länge	Wert	Beschreibung
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Klardatenwert
#(6+L+NN)	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#(7+L+NN)	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '04h' für Secure Messaging der 1. Generation (siehe Anlage 11 Teil A) '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografische Prüfsumme
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

TCS_46 **Antwortnachricht, wenn SM-R-ENC-MAC-G1 (1. Generation)/SM-R-ENC-MAC-G2 (2. Generation) erforderlich und Secure-Messaging-Eingabeformat korrekt:**

Byte	Länge	Wert	Beschreibung
#1	1	'87h'	$T_{PI\ CG}$: Tag für verschlüsselte Daten (Kryptogramm)
#2	L	'MMh' oder '81 MMh'	$L_{PI\ CG}$: Länge der zurückgesendeten verschlüsselten Daten (wegen Auffüllung anders als Original-Le des Befehls). L gleich 2 Bytes, wenn $L_{PI\ CG}$ > 127 Bytes.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Verschlüsselte Daten: Auffüllindikator und Kryptogramm
#(2+L+MM)	1	'99h'	Tag für Verarbeitungsstatus (SW1-SW2) — optional für Secure Messaging der 1. Generation
#(3+L+MM)	1	'02h'	Länge des Verarbeitungsstatus
#(4+L+MM) — #(5+L+MM)	2	'XX XXh'	Verarbeitungsstatus der ungeschützten APDU-Antwort
#(6+L+MM)	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#(7+L+MM)	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '04h' für Secure Messaging der 1. Generation (siehe Anlage 11 Teil A) '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Kryptografische Prüfsumme
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

Der Befehl READ BINARY kann die regulären Verarbeitungszustände, die in TCS_43 unter Tag '99h' aufgelistet und in TCS_59 beschrieben sind, mittels Secure-Messaging-Antwortstruktur zurücksenden.

Darüber hinaus können einige Fehler speziell im Zusammenhang mit Secure Messaging auftreten. In diesem Fall wird der Verarbeitungsstatus einfach ohne Secure-Messaging-Struktur zurückgesendet:

TCS_47 **Antwortnachricht bei inkorrektem Secure-Messaging-Eingabeformat**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist kein aktueller Sitzungsschlüssel vorhanden, wird der Verarbeitungsstatus '**6A88**' zurückgesendet. Dies geschieht entweder, wenn der Sitzungsschlüssel noch nicht erzeugt wurde oder wenn seine Gültigkeit abgelaufen ist (in diesem Fall muss das IFD erneut eine gegenseitige Authentisierung durchführen, um einen neuen Sitzungsschlüssel zu setzen).

— Wenn im Secure-Messaging-Format einige erwartete Datenobjekte (siehe oben) fehlen, wird der Verarbeitungsstatus '**6987**' zurückgesendet. Dieser Fehler tritt auf, wenn ein erwartetes Tag fehlt oder wenn der Befehlskörper nicht den Anforderungen entsprechend aufgebaut ist.

— Sind Datenobjekte nicht korrekt, lautet der zurückgesendete Verarbeitungsstatus '**6988**'. Dieser Fehler tritt auf, wenn zwar alle benötigten Tags vorhanden sind, einige Längen sich jedoch von den erwarteten unterscheiden.

— Schlägt die Überprüfung der kryptografischen Prüfsumme fehl, lautet der zurückgesendete Verarbeitungsstatus '**6688**'.

3.5.2.2 Befehl mit Kurz-Elementardateikennung

Mit dieser Befehlsvariante kann das IFD eine EF mithilfe einer Kurz-Elementardateikennung auswählen und Daten aus dieser EF lesen.

TCS_48 Eine Fahrtenschreiberkarte unterstützt diese Befehlsvariante für alle Elementardateien mit angegebener Kurz-Elementardateikennung. Diese Kurz-Elementardateikennungen sind in Kapitel 4 angegeben.

TCS_49 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Bit 8 auf 1 gesetzt Bit 7 und 6 auf 00 gesetzt Bit 5 — 1 kodieren die Kurz-Elementardateikennung der entsprechenden EF
P2	1	'XXh'	Kodiert ein Offset von 0 bis 255 Bytes in der durch P1 angegebenen EF
Le	1	'XXh'	Erwartete Datenlänge. Anzahl der zu lesenden Bytes.

Hinweis: Die für die Fahrtenschreiberanwendung der 2. Generation verwendeten Kurz-Elementardateikennungen sind in Kapitel 4 angegeben.

Wenn P1 eine Kurz-Elementardateikennung kodiert und der Befehl erfolgreich ist, wird die angegebene EF zur derzeit ausgewählten EF (aktuelle EF).

TCS_50 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#L	L	'XX..XXh'	Gelesene Daten
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Wird die der Kurz-Elementardateikennung entsprechende Datei nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus '**6A82**'.

— Sind die Sicherheitsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit '**6982**' abgebrochen.

— Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6B00**'.

— Ist die Größe der auszulesenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6700**' oder '**6Cxx**', wobei 'xx' die genaue Länge angibt.

— Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wiederherstellbar und der zurückgesendete Verarbeitungsstatus lautet '**6400**' oder '**6581**'.

— Wird in den gespeicherten Daten ein Integritätsfehler festgestellt, so gibt die Karte die angeforderten Daten aus und der zurückgesendete Verarbeitungsstatus lautet '**6281**'.

3.5.2.3 Befehl mit ungeradem Befehlsbyte

Mit dieser Befehlsvariante kann das IFD Daten aus einer EF mit 32 768 Bytes oder mehr lesen.

TCS_51 Eine Fahrtenschreiberkarte, die EF mit 32 768 Bytes oder mehr unterstützt, unterstützt diese Befehlsvariante für diese EF. Eine Fahrtenschreiberkarte kann diese Befehlsvariante ggf. für andere EF unterstützen, ausgenommen die EF Sensor_Installation_Data (siehe TCS_156 und TCS_160).

TCS_52 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuelle EF
P2	1	'00h'	
Lc	1	'NNh'	Lc = Länge des Datenobjekts „offset".
#6-#(5+NN)	NN	'XX..XXh'	Datenobjekt „offset": Tag '54h' Länge '01h' oder '02h' Wert offset
Le	1	'XXh'	Anzahl der zu lesenden Bytes.

Das IFD kodiert die Länge des Datenobjekts „offset" mit einer minimal möglichen Anzahl an Oktetten, d. h. bei der Verwendung des Längenbytes '01h' kodiert das IFD ein Offset zwischen 0 und 255 und bei der Verwendung des Längenbytes '02h' ein Offset zwischen 256 und 65 535 Bytes.

TCS_53 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#L	L	'XX..XXh'	Lesen von Daten, die in einem beliebigen Datenobjekt mit Tag '53h' eingekapselt sind.
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist keine EF ausgewählt, lautet der zurückgesendete Verarbeitungsstatus '**6986**'.

— Sind die Sicherheitsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit '**6982**' abgebrochen.

— Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6B00**'.

— Ist die Größe der auszulesenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6700**' oder '**6Cxx**', wobei 'xx' die genaue Länge angibt.

— Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wieder herstellbar und der zurückgesendete Verarbeitungsstatus lautet '**6400**' oder '**6581**'.

— Wird in den gespeicherten Daten ein Integritätsfehler festgestellt, so gibt die Karte die angeforderten Daten aus und der zurückgesendete Verarbeitungsstatus lautet '**6281**'.

3.5.2.3.1 Befehl mit Secure Messaging (Beispiel)

Im folgenden Beispiel wird die Verwendung von Secure Messaging dargestellt, wenn die Sicherheitsbedingung SM-MAC-G2 gilt.

TCS_54 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	'0Ch'	Secure Messaging angefordert
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuelle EF
P2	1	'00h'	
Lc	1	'XXh'	Länge des gesicherten Datenfelds
#6	1	'B3h'	Tag für in BER-TLV kodierte Klarwertdaten
#7	1	'NNh'	L_{PV}: Länge der übermittelten Daten
#(8)-#(7+NN)	NN	'XX..XXh'	In BER-TLV kodierte Klardaten, d. h. das Datenobjekt „offset" mit Tag „54"
#(8+NN)	1	'97h'	T_{LE}: Tag zur Spezifikation der erwarteten Länge
#(9+NN)	1	'01h'	L_{LE}: Erwartete Länge
#(10+NN)	1	'XXh'	Spezifikation der erwarteten Länge (Original Le): Anzahl der zu lesenden Bytes
#(11+NN)	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#(12+NN)	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Kryptografische Prüfsumme
Le	1	'00h'	Gemäß ISO/IEC 7816-4

TCS_55 Antwortnachricht bei erfolgreichem Befehl

Byte	Länge	Wert	Beschreibung
#1	1	'B3h'	In BER-TLV kodierte Klarwertdaten
#2	L	'NNh' oder '81 NNh'	L_{PV}: Länge der zurückgesendeten Daten (= Original Le). L gleich 2 Bytes, wenn L_{PV} > 127 Bytes
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	In BER-TLV kodierter Klarwertdaten, d. h. Lesen von Daten, die in einem beliebigen Datenobjekt mit Tag '53h' eingekapselt sind.
#(2+L+NN)	1	'99h'	Verarbeitungsstatus der ungeschützten APDU-Antwort
#(3+L+NN)	1	'02h'	Länge des Verarbeitungsstatus
#(4+L+NN) — #(5+L+NN)	2	'XX XXh'	Verarbeitungsstatus der ungeschützten APDU-Antwort
#(6+L+NN)	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#(7+L+NN)	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografische Prüfsumme
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

3.5.3 *UPDATE BINARY*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Die Befehlsnachricht UPDATE BINARY initiiert die Aktualisierung (erase + write) der bereits in einer EF-Binärzahl vorhandenen Bits mit den im APDU-Befehl gegebenen Bits.

3.5.3.1 Befehl mit Offset in P1-P2

Dieser Befehl ermöglicht dem IFD das Schreiben von Daten in die zu dem entsprechenden Zeitpunkt ausgewählte EF, ohne dass die Karte die Integrität der empfangenen Daten überprüft.

Hinweis: Dieser Befehl ohne Secure Messaging kann nur genutzt werden, um eine Datei zu aktualisieren, die die ALW-Sicherheitsbedingung für den Aktualisierungs-Zugriffsmodus unterstützt.

TCS_56 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'D6h'	Update Binary

Byte	Länge	Wert	Beschreibung
P1	1	'XXh'	Offset in Bytes vom Dateianfang: höchstwertiges Byte
P2	1	'XXh'	Offset in Bytes vom Dateianfang: niedrigstwertiges Byte
Lc	1	'NNh'	Lc = Länge des zu aktualisierenden Datenobjekts. Anzahl der zu schreibenden Bytes
#6-#(5+NN)	NN	'XX..XXh'	Zu schreibende Daten

Hinweis: Bit 8 von P1 muss auf 0 gesetzt sein.

TCS_57 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist keine EF ausgewählt, lautet der zurückgesendete Verarbeitungsstatus '**6986**'.

— Sind die Sicherheitsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit '**6982**' abgebrochen.

— Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6B00**'.

— Ist die Größe der zu schreibenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6700**'.

— Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wiederherstellbar und der zurückgesendete Verarbeitungsstatus lautet '**6400**' oder '**6500**'.

— Schlägt der Schreibvorgang fehl, so lautet der zurückgesendete Verarbeitungsstatus '**6581**'.

3.5.3.1.1 Befehl mit Secure Messaging (Beispiele)

Dieser Befehl ermöglicht dem IFD das Schreiben von Daten in die zu dem entsprechenden Zeitpunkt ausgewählte EF, wobei die Karte die Integrität der empfangenen Daten überprüft. Da keine Vertraulichkeit erforderlich ist, werden die Daten nicht verschlüsselt.

TCS_58 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'0Ch'	Secure Messaging angefordert
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Offset in Bytes vom Dateianfang: höchstwertiges Byte
P2	1	'XXh'	Offset in Bytes vom Dateianfang: niedrigstwertiges Byte
Lc	1	'XXh'	Länge des gesicherten Datenfelds

Byte	Länge	Wert	Beschreibung
#6	1	'81h'	T_{PV}: Tag für Klarwertdaten
#7	L	'NNh' oder '81 NNh'	L_{PV}: Länge der übermittelten Daten. L gleich 2 Bytes, wenn L_{PV} > 127 Bytes
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Klardatenwert (zu schreibende Daten)
#(7+L+NN)	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#(8+L+NN)	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '04h' für Secure Messaging der 1. Generation (siehe Anlage 11 Teil A) '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptografische Prüfsumme
Le	1	'00h'	Gemäß ISO/IEC 7816-4

TCS_59 **Antwortnachricht bei korrektem Secure-Messaging-Eingabeformat**

Byte	Länge	Wert	Beschreibung
#1	1	'99h'	T_{SW}: Tag für Statusbytes (durch CC zu schützen)
#2	1	'02h'	L_{SW}: Länge der zurückgesendeten Statusbytes
#3-#4	2	'XXXXh'	Verarbeitungsstatus der ungeschützten APDU-Antwort
#5	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#6	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '04h' für Secure Messaging der 1. Generation (siehe Anlage 11 Teil A) '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#7-#(6+L)	L	'XX..XXh'	Kryptografische Prüfsumme
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

Die für den Befehl UPDATE BINARY ohne Secure Messaging beschriebenen „regulären" Verarbeitungszustände (siehe Abschnitt 3.5.3.1) können unter Verwendung der oben aufgeführten Antwortnachrichtstrukturen zurückgesendet werden.

Darüber hinaus können einige Fehler speziell im Zusammenhang mit Secure Messaging auftreten. In diesem Fall wird der Verarbeitungsstatus einfach ohne Secure-Messaging-Struktur zurückgesendet:

TCS_60 **Antwortnachricht bei Fehler im Secure Messaging**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist kein aktueller Sitzungsschlüssel vorhanden, wird der Verarbeitungsstatus '**6A88**' zurückgesendet.

— Wenn im Secure-Messaging-Format einige erwartete Datenobjekte (siehe oben) fehlen, wird der Verarbeitungsstatus '**6987**' zurückgesendet. Dieser Fehler tritt auf, wenn ein erwartetes Tag fehlt oder wenn der Befehlskörper nicht den Anforderungen entsprechend aufgebaut ist.

— Sind Datenobjekte nicht korrekt, lautet der zurückgesendete Verarbeitungsstatus '**6988**'. Dieser Fehler tritt auf, wenn zwar alle benötigten Tags vorhanden sind, einige Längen sich jedoch von den erwarteten unterscheiden.

— Schlägt die Überprüfung der kryptografischen Prüfsumme fehl, lautet der zurückgesendete Verarbeitungsstatus '**6688**'.

3.5.3.2 Befehl mit Kurz-Elementardateikennung

Mit dieser Befehlsvariante kann das IFD eine EF mithilfe einer Kurz-Elementardateikennung auswählen und Daten aus dieser EF schreiben.

TCS_61 Eine Fahrtenschreiberkarte sollte die Befehlsvariante für alle Elementardateien mit angegebener Kurz-Elementardateikennung unterstützen. Diese Kurz-Elementardateikennungen sind in Kapitel 4 angegeben.

TCS_62 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Bit 8 auf 1 gesetzt Bit 7 und 6 auf 00 gesetzt Bit 5 — 1 kodieren die Kurz-Elementardateikennung der entsprechenden EF
P2	1	'XXh'	Kodiert ein Offset von 0 bis 255 Bytes in der durch P1 angegebenen EF
Lc	1	'NNh'	Lc = Länge der zu aktualisierenden Daten. Anzahl der zu schreibenden Bytes
#6-#(5+NN)	NN	'XX..XXh'	Zu schreibende Daten

TCS_63 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

Hinweis: Die für die Fahrtenschreiberanwendung der 2. Generation verwendeten Kurz-Elementardateikennungen sind in Kapitel 4 angegeben.

Wenn P1 eine Kurz-Elementardateikennung kodiert und der Befehl erfolgreich ist, wird die angegebene EF zur derzeit ausgewählten EF (aktuelle EF).

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Wird die der Kurz-Elementardateikennung entsprechende Datei nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus '**6A82**'.

— Sind die Sicherheitsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit '**6982**' abgebrochen.

— Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6B00**'.

— Ist die Größe der zu schreibenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6700**'.

— Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wiederherstellbar und der zurückgesendete Verarbeitungsstatus lautet '**6400**' oder '**6581**'.

— Schlägt der Schreibvorgang fehl, so lautet der zurückgesendete Verarbeitungsstatus '**6581**'.

3.5.3.3 Befehl mit ungeradem Befehlsbyte

Mit dieser Befehlsvariante kann das IFD Daten in eine EF mit 32 768 Bytes oder mehr schreiben.

TCS_64 Eine Fahrtenschreiberkarte, die EF mit 32 768 Bytes oder mehr unterstützt, unterstützt diese Befehlsvariante für diese EF. Eine Fahrtenschreiberkarte kann diese Befehlsvariante für andere EF ggf. unterstützen.

TCS_65 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuelle EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Länge der Daten im Befehlsdatenfeld
#6-#(5+NN)	NN	'XX..XXh'	Datenobjekt „offset" mit Tag '54h' || Beliebiges Datenobjekt mit Tag '53h', das die zu schreibenden Daten einkapselt

Das IFD kodiert die Länge des Datenobjekts „offset" und des beliebigen Datenobjekts mit einer minimal möglichen Anzahl an Oktetten, d. h. bei der Verwendung des Längenbytes '01h' kodiert das IFD ein Offset/eine Länge zwischen 0 und 255 und bei der Verwendung des Längenbytes '02h' ein Offset/eine Länge zwischen 256 und 65 535 Bytes.

TCS_66 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist keine EF ausgewählt, lautet der zurückgesendete Verarbeitungsstatus '**6986**'.

— Sind die Sicherheitsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit '**6982**' abgebrochen.

— Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6B00**'.

— Ist die Größe der zu schreibenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus '**6700**'.

— Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wiederherstellbar und der zurückgesendete Verarbeitungsstatus lautet '**6400**' oder '**6500**'.

— Schlägt der Schreibvorgang fehl, so lautet der zurückgesendete Verarbeitungsstatus '**6581**'.

3.5.3.3.1 Befehl mit Secure Messaging (Beispiel)

Im folgenden Beispiel wird die Verwendung von Secure Messaging dargestellt, wenn die Sicherheitsbedingung SM-MAC-G2 gilt.

TCS_67 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	'0Ch'	Secure Messaging angefordert
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuelle EF
P2	1	'00h'	
Lc	1	'XXh'	Länge des gesicherten Datenfelds
#6	1	'B3h'	Tag für in BER-TLV kodierte Klarwertdaten
#7	L	'NNh' oder '81 NNh'	L_{PV}: Länge der übermittelten Daten. L gleich 2 Bytes, wenn L_{PV} > 127 Bytes
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	In BER-TLV kodierte Klardaten, d. h. Datenobjekt „offset" mit Tag '54h' || Beliebiges Datenobjekt mit Tag '53h', das die zu schreibenden Daten einkapselt
#(7+L+NN)	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme
#(8+L+NN)	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptografische Prüfsumme
Le	1	'00h'	Gemäß ISO/IEC 7816-4

TCS_68 Antwortnachricht bei erfolgreichem Befehl

Byte	Länge	Wert	Beschreibung
#1	1	'99h'	T_{SW}: Tag für Statusbytes (durch CC zu schützen)
#2	1	'02h'	L_{SW}: Länge der zurückgesendeten Statusbytes
#3-#4	2	'XXXXh'	Verarbeitungsstatus der ungeschützten APDU-Antwort
#5	1	'8Eh'	T_{CC}: Tag für kryptografische Prüfsumme

Byte	Länge	Wert	Beschreibung
#6	1	'XXh'	L_{CC}: Länge der folgenden kryptografischen Prüfsumme '08h', '0Ch' oder '10h' in Abhängigkeit von der AES-Schlüssellänge für Secure Messaging der 2. Generation (siehe Anlage 11 Teil B)
#7-#(6+L)	L	'XX..XXh'	Kryptografische Prüfsumme
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

3.5.4 *GET CHALLENGE*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl GET CHALLENGE fordert die Karte zur Ausgabe einer Zufallszahl aus, damit diese in einem sicherheitsbezogenen Verfahren verwendet werden kann, bei dem ein Kryptogramm oder chiffrierte Daten an die Karte gesendet werden.

TCS_69 Die von der Karte ausgegebene Zufallszahl ist nur für den nächsten Befehl gültig, der eine an die Karte gesendete Zufallszahl verwendet.

TCS_70 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Länge der erwarteten Zufallszahl).

TCS_71 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#8	8	'XX..XXh'	Zufallszahl
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Unterscheidet sich Le von '08h', ist der Verarbeitungsstatus '**6700**'.

— Sind die Parameter P1-P2 inkorrekt, ist der Verarbeitungsstatus '**6A86**'.

3.5.5 *VERIFY*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Nur die Werkstattkarte muss diesen Befehl unterstützen.

Andere Arten von Fahrtenschreiberkarten können diesen Befehl ggf. unterstützen; für diese Karten wird allerdings keine Bezugs-CHV personalisiert. Aus diesem Grund können diese Karten diesen Befehl nicht erfolgreich ausführen. Für andere Arten von Fahrtenschreiberkarten als Werkstattkarten ist dieses Verhalten, d. h. der zurückgesendete Fehlercode, beim Senden dieses Befehls nicht erforderlich.

Der Befehl Verify leitet auf der Karte den Vergleich der vom Befehl gesendeten CHV (PIN)-Daten mit der auf der Karte gespeicherten Bezugs-CHV ein.

TCS_72 Die vom Benutzer eingegebene PIN muss ASCII-kodiert und durch das IFD bis zu einer Länge von 8 Byte nach rechts mit 'FFh'-Bytes aufgefüllt sein (siehe auch Datentyp WorkshopCardPIN in Anlage 1).

TCS_73 Die Fahrtenschreiberanwendungen der 1. und 2. Generation verwenden die gleiche Bezugs-CHV.

TCS_74 Die Fahrtenschreiberkarte überprüft, ob der Befehl richtig kodiert ist. Wenn der Befehl nicht richtig kodiert ist, darf die Karte die CHV-Werte nicht vergleichen, den Zähler für die verbleibenden CHV-Versuche nicht herabsetzen und den Sicherheitsstatus „PIN_Verified" nicht zurücksetzen, sondern muss den Befehl abbrechen. Ein Befehl ist richtig kodiert, wenn die Bytes CLA, INS, P1, P2, Lc die angegebenen Werte aufweisen, Le nicht vorhanden ist und das Befehlsdatenfeld die richtige Länge aufweist.

TCS_75 Ist der Befehl erfolgreich, wird der Zähler für die verbleibenden CHV-Versuche reinitialisiert. Der Anfangswert des Zählers für die verbleibenden CHV-Versuche ist 5. Ist der Befehl erfolgreich, setzt die Karte den internen Sicherheitsstatus auf „PIN_Verified". Die Karte diesen Sicherheitsstatus zurücksetzen, wenn die Karte zurückgesetzt ist oder der im Befehl übertragene CHV-Code nicht mit dem gespeicherten Bezugs-CHV übereinstimmt.

Hinweis: Durch die Verwendung des gleichen Bezugs-CHV und eines globalen Sicherheitsstatus wird verhindert, dass ein Mitarbeiter der Werkstatt nach Auswahl eines anderen Fahrtenschreibe-ranwendung-DF die PIN neu eingeben muss.

TCS_76 Ein fehlgeschlagener Vergleich wird auf der Karte gespeichert, d. h., dass der Zähler für die verbleibenden CHV-Versuche um eins herabgesetzt wird, um die Anzahl weiterer Versuche, die Bezugs-CHV zu verwenden, zu begrenzen.

TCS_77 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (die verifizierte CHV ist implizit bekannt)
Lc	1	'08h'	Länge des übermittelten CHV-Codes
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Wird die Bezugs-CHV nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Ist die CHV blockiert (der Zähler für verbleibende Versuche steht auf null), lautet der zurückgesendete Verarbeitungsstatus '**6983**'. Wenn dieser Zustand erreicht ist, kann die CHV nie wieder erfolgreich präsentiert werden.

— Ist der Vergleich erfolglos, wird der Zähler für die verbleibenden Versuche herabgesetzt und der Status '**63CX**' zurückgesendet (X > 0, und X ist gleich dem Zähler für verbleibende CHV-Versuche.

— Wird die Bezugs-CHV als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

— Unterscheidet sich Lc von '08h', ist der Verarbeitungsstatus '**6700**'.

3.5.6 *GET RESPONSE*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4.

Dieser (nur für das Protokoll T=0 notwendige und verfügbare) Befehl wird zur Übertragung vorbereiteter Daten von der Karte zum Schnittstellengerät verwendet (wenn ein Befehl sowohl Lc als auch Le enthalten hat).

Der Befehl GET RESPONSE muss sofort nach dem Befehl zur Vorbereitung der Daten ausgegeben werden, sonst gehen die Daten verloren. Nach der Ausführung des Befehls GET RESPONSE (außer bei Auftreten der Fehler '**61xx**' oder '**6Cxx**', siehe unten) stehen die zuvor vorbereiteten Daten nicht mehr zur Verfügung.

TCS_79 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Anzahl der erwarteten Bytes

TCS_80 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#X	X	'XX..XXh'	Daten
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Wurden von der Karte keine Daten vorbereitet, lautet der zurückgesendete Verarbeitungsstatus '**6900**' oder '**6F00**'.

— Übersteigt Le die Anzahl der verfügbaren Bytes oder ist Le gleich null, lautet der zurückgesendete Verarbeitungsstatus '**6Cxx**', wobei 'xx' die genaue Anzahl der verfügbaren Bytes bezeichnet. In diesem Fall stehen die vorbereiteten Daten für einen weiteren Befehl GET RESPONSE zur Verfügung.

— Ist Le nicht null und kleiner als die Anzahl der verfügbaren Bytes, werden die angeforderten Daten normal von der Karte gesendet. Der zurückgesendete Verarbeitungsstatus lautet '**61xx**', wobei 'xx' die Anzahl der zusätzlichen Bytes angibt, die noch für einen nachfolgenden Befehl GET RESPONSE zur Verfügung stehen.

— Wird der Befehl nicht unterstützt (Protokoll T=1), sendet die Karte '**6D00**' zurück.

3.5.7 *PSO: VERIFY CERTIFICATE*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-8, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl VERIFY CERTIFICATE wird von der Karte zur Einholung eines öffentlichen Schlüssels von außen und zur Prüfung seiner Gültigkeit verwendet.

3.5.7.1 Befehl-Antwort-Paar der 1. Generation

TCS_81 Diese Befehlsvariante wird lediglich durch eine Fahrtenschreiberanwendung der 1. Generation unterstützt.

TCS_82 Ist der Befehl VERIFY CERTIFICATE erfolgreich, wird der öffentliche Schlüssel zur künftigen Verwendung in der Sicherheitsumgebung gespeichert. Dieser Schlüssel wird explizit zur Verwendung in sicherheitsbezogenen Befehlen (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE oder VERIFY CERTIFICATE) durch den Befehl MSE (siehe Abschnitt 3.5.11) unter Verwendung seines Schlüsselbezeichners gesetzt.

TCS_83 Auf jeden Fall verwendet der Befehl VERIFY CERTIFICATE den zuvor vom Befehl MSE zur Eröffnung des Zertifikats ausgewählten öffentlichen Schlüssel. Dabei muss es sich um den öffentlichen Schlüssel eines Mitgliedstaates oder Europas handeln.

TCS_84 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	P1
P2	1	'AEh'	P2: nicht BER-TLV kodierte Daten (Verkettung von Datenelementen)
Lc	1	'C2h'	Lc: Länge des Zertifikats, 194 Bytes
#6-#199	194	'XX..XXh'	Zertifikat: Verkettung von Datenelementen (gemäß Beschreibung in Anlage 11)

TCS_85 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Schlägt die Zertifikatsverifizierung fehl, lautet der zurückgesendete Verarbeitungsstatus '**6688**'. Das Prüfungs- und Entpackungsverfahren für das Zertifikat wird für G1 und G2 in Anlage 11 beschrieben.

— Ist kein öffentlicher Schlüssel in der Sicherheitsumgebung vorhanden, wird '**6A88**' zurückgesendet.

— Wird der (zum Entpacken des Zertifikats verwendete) ausgewählte öffentliche Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

— Nur 1. Generation: Weist der (zum Entpacken des Zertifikats verwendete) öffentliche Schlüssel ein CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) mit einem anderen Wert als '00' auf (d. h., es ist der Schlüssel eines Mitgliedstaates oder Europas), so lautet der zurückgesendete Verarbeitungsstatus '**6985**'.

3.5.7.2 Befehl-Antwort-Paar der 2. Generation

Je nach Kurvengröße können ECC-Zertifikate so lang sein, dass sie sich nicht in einem einzigen APDU übermitteln lassen. In einem solchen Fall muss eine Befehlsverkettung gemäß ISO/IEC 7816-4 erfolgen und das Zertifikat in zwei aufeinander folgenden PSO: Verify Certificate APDU-Befehlen übermittelt werden.

Zertifikatstruktur und Domänenparameter werden in Anlage 11 definiert.

TCS_86 Der Befehl kann in MF, DF Tachograph und DF Tachograph_G2 ausgeführt werden, siehe auch TCS_33.

TCS_87 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'X0h'	CLA-Byte zur Angabe einer Befehlsverkettung: '00h' als einziger oder letzter Befehl der Kette '10h' nicht als letzter Befehl einer Kette
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'BEh'	Selbstbeschreibendes Zertifikat verifizieren
Lc	1	'XXh'	Länge des Befehlsdatenfelds, siehe TCS_88 und TCS_89.
#6-#5+L	L	'XX..XXh'	DER-TLV-kodierte Daten: Datenobjekt „ECC Certificate Body" als erstes Datenobjekt, verkettet mit dem Datenobjekt „ECC Certificate Signature" als zweites Datenobjekt oder als Teil dieser Verkettung. Der Tag '7F21' und die damit einhergehende Länge sind nicht zu übermitteln. Die Reihenfolge dieser Datenobjekte ist fest.

TCS_88 Für APDU mit kurzen Längenfeldern gilt Folgendes: Das IFD verwendet die Mindestanzahl an APDU, die erforderlich sind, um die Befehlsdaten zu übermitteln und die Höchstzahl an Bytes im APDU des ersten Befehls gemäß dem Wert des Byte für die Informationsfeldgröße der Karte zu übermitteln (siehe TCS_14). Wenn das IFD ein anderes Verhalten zeigt, liegt das Verhalten der Karte außerhalb des Gültigkeitsbereichs.

TCS_89 Für APDU mit erweiterten Längenfeldern gilt Folgendes: Passt das Zertifikat nicht in eine einzige APDU, so unterstützt die Karte die Befehlsverkettung. Das IFD verwendet die Mindestanzahl an APDU, die erforderlich sind, um die Befehlsdaten zu übermitteln und die Höchstzahl an Bytes im ersten APDU-Befehl zu übermitteln. Wenn das IFD ein anderes Verhalten zeigt, liegt das Verhalten der Karte außerhalb des Gültigkeitsbereichs.

Hinweis: Gemäß Anlage 11 speichert die Karte das Zertifikat oder die relevanten Inhalte des Zertifikats und aktualisiert ihren Wert currentAuthenticatedTime.

Struktur und Statusbytes der Antwortnachricht entsprechen der Definition in TCS_85.

TCS_90 Zusätzlich zu den in TCS_85 aufgeführten Fehlercodes kann die Karte die folgenden Fehlercodes zurücksenden:

— Weist der (zum Entpacken des Zertifikats verwendete) ausgewählte öffentliche Schlüssel einen CHA.LSB (CertificateHolderAuthorisation.equipmentType) auf, der nicht für die Verifizierung des Zertifikats gemäß Anlage 11 geeignet ist, lautet der zurückgesendete Verarbeitungsstatus '**6985**'.

— Weist der Wert currentAuthenticatedTime der Karte einen späteren Zeitpunkt als das Ablaufdatum des Zertifikats auf, lautet der zurückgesendete Verarbeitungsstatus '**6985**'.

— Wird der letzte Befehl der Kette erwartet, sendet die Karte '**6883**' zurück.

— Werden im Befehlsdatenfeld falsche Parameter gesendet, sendet die Karte '**6A80**' zurück (wird auch verwendet, wenn die Datenobjekte nicht in der festgelegten Reihenfolge gesendet werden).

3.5.8 *INTERNAL AUTHENTICATE*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4.

TCS_91 Alle Fahrtenschreiberkarten müssen diesen Befehl in DF Tachograph der 1. Generation verwenden. Der Befehl kann in MF und/oder DF Tachograph_G2 gegebenenfalls zur Verfügung stehen. In einem solchen Fall muss der Befehl mit einem geeigneten Fehlercode enden, da der private Schlüssel der Karte (Card.SK) für das Authentisierungsprotokoll der 1. Generation nur in DF_Tachograph der 1. Generation zugreifbar ist.

Mit Hilfe des Befehls INTERNAL AUTHENTICATE kann das IFD die Karte authentisieren. Der Authentisierungsvorgang wird in Anlage 11 beschrieben. Er beinhaltet folgende Aussagen:

TCS_92 Der Befehl INTERNAL AUTHENTICATE verwendet den (implizit ausgewählten) privaten Kartenschlüssel zum Signieren von Authentisierungsdaten einschließlich K1 (erstes Element für die Sitzungsschlüsselvereinbarung) und RND1 und verwendet den aktuell (durch den letzten MSE-Befehl) ausgewählten öffentlichen Schlüssel zur Verschlüsselung der Signatur und zur Bildung des Authentisierungstokens (nähere Angaben in Anlage 11).

TCS_93 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Länge der an die Karte gesendeten Daten
#6 — #13	8	'XX..XXh'	Zur Authentisierung der Karte verwendete Zufallszahl
#14 -#21	8	'XX..XXh'	VU.CHR (siehe Anlage 11)
Le	1	'80h'	Länge der von der Karte erwarteten Daten

TCS_94 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#128	128	'XX..XXh'	Token zur Authentisierung der Karte (siehe Anlage 11)
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist in der Sicherheitsumgebung kein öffentlicher Schlüssel vorhanden, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Ist in der Sicherheitsumgebung kein privater Schlüssel vorhanden, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Stimmt VU.CHR nicht mit dem aktuellen Bezeichner des öffentlichen Schlüssels überein, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Wird der ausgewählte private Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

TCS_95 Ist der Befehl INTERNAL AUTHENTICATE erfolgreich, wird der aktuelle Sitzungsschlüssel, sofern vorhanden, gelöscht und ist nicht mehr verfügbar. Um einen neuen Sitzungsschlüssel zur Verfügung zu haben, muss der Befehl EXTERNAL AUTHENTICATE für den Authentisierungsmechanismus der 1. Generation erfolgreich ausgeführt werden.

3.5.9 *EXTERNAL AUTHENTICATE*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4.

Mit Hilfe des Befehls EXTERNAL AUTHENTICATE kann die Karte das IFD authentisieren. Das Authentisierungsverfahren wird in Anlage 11 für die Fahrtenschreiber der 1. und 2. Generation beschrieben (VU-Authentisierung).

TCS_96 Die Befehlsvariante für den Mechanismus zur gegenseitigen Authentisierung der 1. Generation wird nur von einer Fahrtenschreiberanwendung der 1. Generation unterstützt.

TCS_97 Die Befehlsvariante für die gegenseitige VU-Karten-Authentisierung der 2. Generation kann in MF, DF Tachograph und DF Tachograph_G2 erfolgen (siehe auch TCS_34).

TCS_98 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Schlüssel und Algorithmen implizit bekannt
P2	1	'00h'	
Lc	1	'XXh'	Lc (Länge der an die Karte gesendeten Daten)
#6-#(5+L)	L	'XX..XXh'	Authentisierung der 1. Generation: Kryptogramm (siehe Anlage 11 Teil A) Authentisierung der 2 Generation: Vom IFD erstellte Signatur (siehe Anlage 11 Teil B)

TCS_99 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist die CHA des derzeit gesetzten Schlüssels nicht die Verkettung der AID der Fahrtenschreiberanwendung und eines VU-Gerätetyps, lautet der zurückgesendete Verarbeitungsstatus '**6F00**'.

— Geht dem Befehl nicht unmittelbar ein GET CHALLENGE-Befehl voraus, lautet der zurückgesendete Verarbeitungsstatus '**6985**'.

Die Fahrtenschreiberanwendung der 1. Generation kann gegebenenfalls die folgenden Fehlercodes zurücksenden:

— Ist kein öffentlicher Schlüssel in der Sicherheitsumgebung vorhanden, wird '**6A88**' zurückgesendet.

— Ist in der Sicherheitsumgebung kein privater Schlüssel vorhanden, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Schlägt die Prüfung des Kryptogramms fehl, lautet der zurückgesendete Verarbeitungsstatus '**6688**'.

— Wird der ausgewählte private Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

Die Befehlsvariante für die Authentisierung der 2. Generation kann gegebenenfalls die folgenden Fehlercodes zurücksenden:

— Schlägt die Verifizierung der Signatur fehl, sendet die Karte '**6300**' zurück.

3.5.10 *GENERAL AUTHENTICATE*

Dieser Befehl wird für das Chip-Authentisierungsprotokoll der 2. Generation gemäß Anlage 11 Teil B verwendet und entspricht den Festlegungen von ISO/IEC 7816-4.

TCS_100 Der Befehl kann in MF, DF Tachograph und DF Tachograph_G2 ausgeführt werden, siehe auch TCS_34.

TCS_101 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Schlüssel und Protokoll implizit bekannt
P2	1	'00h'	
Lc	1	'NNh'	Lc: Länge des folgenden Datenfelds
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	DER-TLV-kodierter Wert des flüchtigen öffentlichen Schlüssels (siehe Anlage 11) Die VU sendet die Datenobjekte in dieser Reihenfolge.

TCS_102 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	DER-TLV-kodierte Dynamic Authentication Data: Nonce und Authentisierungstoken (siehe Anlage 11)
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Bei falschen Parametern im Datenfeld sendet die Karte '**6A80**' zurück.

— Wurde der Befehl External Authenticate nicht erfolgreich ausgeführt, sendet die Karte '**6982**' zurück.

Das Datenobjekt Dynamic Authentication — 7Chv

— muss bei erfolgreicher Ausführung vorhanden sein, d. h. die Statusbytes lauten '**9000**',

— muss bei einem Ausführungs- oder Prüffehler fehlen, d. h. wenn die Statusbytes im Bereich '**6400**' — '**6FFF**' liegen, und

— muss bei einer Warnung fehlen, d. h. wenn die Statusbytes im Bereich '**6200**' — '**63FF**' liegen.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Dieser Befehl wird zum Setzen eines öffentlichen Schlüssels zu Authentisierungszwecken verwendet.

3.5.11.1 Befehl-Antwort-Paar der 1. Generation

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4. Die Verwendung des Befehls ist jedoch im Vergleich zur entsprechenden Norm eingeschränkt.

TCS_103 Dieser Befehl wird lediglich durch eine Fahrtenschreiberanwendung der 1. Generation unterstützt.

TCS_104 Der Schlüssel, auf den im MSE-Datenfeld verwiesen wird, bleibt der aktuelle öffentliche Schlüssel, bis der nächste korrekte MSE-Befehl eingeht, ein DF ausgewählt wird oder die Karte zurückgesetzt wird.

TCS_105 Ist der Schlüssel, auf den verwiesen wird, (noch) nicht in der Karte vorhanden, bleibt die Sicherheitsumgebung unverändert.

TCS_106 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: Schlüssel, auf den verwiesen wird, gültig für alle kryptografischen Operationen
P2	1	'B6h'	P2 (mit Verweis versehene Daten zur digitalen Signatur)
Lc	1	'0Ah'	Lc: Länge des folgenden Datenfelds
#6	1	'83h'	Tag zum Verweis auf einen öffentlichen Schlüssel in asymmetrischen Fällen
#7	1	'08h'	Länge des Schlüsselverweises (Schlüsselbezeichner)
#8-#15	8	'XX..XXh'	Schlüsselbezeichner laut Anlage 11

TCS_107 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Ist der Schlüssel, auf den verwiesen wird, auf der Karte nicht vorhanden, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Fehlen einige erwartete Datenobjekte im Secure-Messaging-Format, wird '**6987**' zurückgesendet. Dies kann der Fall sein, wenn der Tag '83h' fehlt.

— Sind einige Datenobjekte inkorrekt, lautet der zurückgesendete Verarbeitungsstatus '**6988**'. Dies kann der Fall sein, wenn der Schlüsselbezeichner nicht '08h' ist.

— Wird der ausgewählte Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

3.5.11.2 Befehl-Antwort-Paare der 2. Generation

Für die Authentisierung der 2. Generation unterstützt die Fahrtenschreiberkarte folgenden MSE: Befehlsvarianten zum Setzen, die den Festlegungen von ISO/IEC 7816-4 entsprechen. Diese Befehlsvarianten werden bei der Authentisierung der 1. Generation nicht unterstützt.

3.5.11.2.1 MSE:SET AT für die Chip-Authentisierung

Mit Hilfe des folgenden Befehls MSE:SET AT werden die Parameter für die Chip-Authentisierung ausgewählt, die durch einen nachfolgenden Befehl General Authenticate durchgeführt wird.

TCS_108 Der Befehl kann in MF, DF Tachograph und DF Tachograph_G2 ausgeführt werden, siehe auch TCS_34.

TCS_109 **MSE:SET AT Befehlsnachricht für die Chip-Authentisierung**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'22h'	

Byte	Länge	Wert	Beschreibung
P1	1	'41h'	Zur internen Authentisierung gesetzt
P2	1	'A4h'	Authentisierung
Lc	1	'NNh'	Lc: Länge des folgenden Datenfelds
#6-#(5+L)	L	'80h' + 0Ah + 'XX..XXh'	DER-TLV-kodierter Verweis zu kryptografischen Mechanismen: Objektkennung der Chip-Authentisierung (nur Wert, Tag '06h' wird weggelassen). Für die Werte der Objektkennungen siehe Anlage 1; es wird die Byte-Notation verwendet. Anleitungen zur Auswahl einer dieser Objektkennungen befinden sich in Anlage 11.

3.5.11.2.2 MSE:SET AT für die VU-Authentisierung

Mit Hilfe des folgenden Befehls MSE:SET AT werden die Parameter und Schlüssel für die VU-Authentisierung ausgewählt, die durch einen nachfolgenden Befehl External Authenticate durchgeführt wird.

TCS_110 Der Befehl kann in MF, DF Tachograph und DF Tachograph_G2 ausgeführt werden, siehe auch TCS_34.

TCS_111 **MSE:SET AT Befehlsnachricht für die VU-Authentisierung**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Zur externen Authentisierung gesetzt
P2	1	'A4h'	Authentisierung
Lc	1	'NNh'	Lc: Länge des folgenden Datenfelds
#6-#(5+L)	L	'80h' + 0Ah + 'XX..XXh'	DER-TLV-kodierter Verweis zu kryptografischen Mechanismen: Objektkennung der VU-Authentisierung (nur Wert, Tag '06h' wird weggelassen). Für die Werte der Objektkennungen siehe Anlage 1; es wird die Byte-Notation verwendet. Anleitungen zur Auswahl einer dieser Objektkennungen befinden sich in Anlage 11.
		'83h' + 08h + 'XX..XXh'	DER-TLV-kodierter Verweis auf den öffentlichen Schlüssel der FE durch die im Zertifikat erwähnte Referenz des Zertifikatinhabers.
		'91h' + L_{91} + 'XX..XXh'	DER-TLV-kodierte komprimierte Darstellung des flüchtigen öffentlichen Schlüssels der VU, die während der Chip-Authentisierung verwendet wird (siehe Anlage 11)

3.5.11.2.3 MSE:SET DST

Der folgende Befehls MSE:SET AT wird verwendet, um einen öffentlichen Schlüssel entweder

— zur Verifizierung einer Signatur, die in einem nachfolgenden Befehl PSO: Verify Digital Signature bereitgestellt wird, oder

— zur Verifizierung der Signatur eines Zertifikats, das in einem nachfolgenden Befehl PSO: Verify Certificate bereitgestellt wird, zu setzen.

TCS_112 Der Befehl kann in MF, DF Tachograph und DF Tachograph_G2 ausgeführt werden, siehe auch TCS_33.

TCS_113 **MSE:SET DST Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Zur Verifizierung gesetzt
P2	1	'B6h'	Digitale Signatur
Lc	1	'NNh'	Lc: Länge des folgenden Datenfelds
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	DER-TLV-kodierter Verweis auf einen öffentlichen Schlüssel, d. h. die Referenz des Zertifikatinhabers im Zertifikat eines öffentlichen Schlüssels (siehe Anlage 11)

Für sämtliche Befehlsversionen werden Struktur und Statusbytes der Antwortnachricht bereitgestellt durch:

TCS_114 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück. Das Protokoll wurde ausgewählt und initialisiert.

— '**6A80**' kennzeichnet fehlerhafte Parameter im Befehlsdatenfeld.

— '**6A88**' gibt an, dass Daten, auf die verwiesen wird (d. h. ein Schlüssel, auf den verwiesen wird), nicht verfügbar sind.

3.5.12 *PSO: HASH*

Dieser Befehl dient dazu, Ergebnisse der Hashwertberechnung für bestimmte Daten an die Karte zu übertragen. Dieser Befehl wird zur Verifizierung digitaler Signaturen verwendet. Der Hashwert wird temporär gespeichert für den folgenden Befehl PSO: Verify Digital Signature

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-8. Die Verwendung des Befehls ist jedoch im Vergleich zur entsprechenden Norm eingeschränkt.

Nur die Kontrollkarte wird benötigt, um diesen Befehl in DF Tachograph und DF Tachograph_G2 zu unterstützen.

Andere Arten von Fahrtenschreiberkarten können diesen Befehl gegebenenfalls implementieren. Der Befehl kann in MF gegebenenfalls zur Verfügung stehen.

Die Kontrollkartenanwendung der 1. Generation unterstützt nur SHA-1.

TCS_115 Der vorübergehend gespeicherte Hashwert ist zu löschen, wenn mithilfe des Befehls PSO: HASH ein neuer Hashwert berechnet wird, wenn ein DF ausgewählt wird und wenn die Fahrtenschreiberkarte zurückgesetzt wird.

TCS_116 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Hashcode zurücksenden
P2	1	'A0h'	Tag: Datenfeld enthält für Hashing relevante DO
Lc	1	'XXh'	Länge Lc des nachfolgenden Datenfelds
#6	1	'90h'	Tag für den Hashcode
#7	1	'XXh'	Länge L des Hashcodes: '14h' in Anwendung der 1. Generation (siehe Anlage 11 Teil A) '20h', '30h' oder '40h' in Anwendung der 2. Generation (siehe Anlage 11 Teil B)
#8-#(7+L)	L	'XX..XXh'	Hashcode

TCS_117 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Fehlen einige der erwarteten Datenobjekte (siehe oben), wird der Verarbeitungsstatus '**6987**' zurückgesendet. Dies kann der Fall sein, wenn der Tag '90h' fehlt.

— Sind einige Datenobjekte inkorrekt, lautet der zurückgesendete Verarbeitungsstatus '**6988**'. Dieser Fehler tritt auf, wenn der erforderliche Tag zwar vorhanden ist, aber eine andere Länge als '14h' für SHA-1, '20h' für SHA-256, '30h' für SHA-384, '40h' für SHA-512 (Anwendung der 2. Generation) aufweist.

3.5.13 *PERFORM HASH of FILE*

Dieser Befehl entspricht nicht den Festlegungen von ISO/IEC 7816-8. Das CLA-Byte dieses Befehls gibt daher an, dass eine proprietäre Verwendung von PERFORM SECURITY OPERATION/HASH erfolgt.

Nur die Fahrer- und die Werkstattkarte müssen diesen Befehl in DF Tachograph und DF Tachograph_G2 unterstützen.

Andere Arten von Fahrtenschreiberkarten können diesen Befehl gegebenenfalls implementieren. Wenn eine Unternehmens- oder Kontrollkarte diesen Befehl implementiert, muss dies gemäß den Angaben dieses Kapitels erfolgen.

Der Befehl kann in der MF gegebenenfalls zur Verfügung stehen. Wenn ja, muss er gemäß den Angaben dieses Kapitels implementiert werden, d. h. der Befehl darf nicht die Berechnung eines Hashwerts zulassen, sondern muss mit einem geeigneten Fehlercode abschließen.

TCS_118 Der Befehl PERFORM HASH of FILE wird zur Hashwertberechnung des Datenbereichs der zu dem entsprechenden Zeitpunkt ausgewählten transparenten EF verwendet.

TCS_119 Eine Fahrtenschreiberkarte darf diesen Befehl nur für die im Kapitel 4 aufgeführten EF im Rahmen von DF_Tachograph und DF_Tachograph_G2 unterstützen, mit folgender Ausnahme. Eine Fahrtenschreiberkarte darf den Befehl nicht für den EF Sensor_Installation_Data von DF Tachograph_G2 unterstützen.

TCS_120 Das Ergebnis der Hash-Operation wird auf der Karte temporär gespeichert. Es kann dann zur Einholung einer digitalen Signatur der Datei mit Hilfe des Befehls PSO: COMPUTE DIGITAL SIGNATURE verwendet werden.

TCS_121 Der temporär gespeicherte „hash of file"-Wert ist zu löschen, wenn mithilfe des Befehls PSO: Hash of File ein neuer Hashwert berechnet wird, wenn ein DF ausgewählt wird und wenn die Fahrtenschreiberkarte zurückgesetzt wird.

TCS_122 Die Fahrtenschreiberanwendung der 1. Generation muss SHA-1 unterstützen.

TCS_123 Die Fahrtenschreiberanwendung der 2. Generation muss SHA-1 und SHA-2 (256, 384 und 512 Bits) unterstützen.

TCS_124 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Tag: Hash
P2	1	'XXh'	P2: Gibt den Algorithmus an, der zum Hashing der Daten der derzeit ausgewählten transparenten Datei verwendet wird: '00h' für SHA-1 '01h' für SHA-256 '02h' für SHA-384 '03h' für SHA-512

TCS_125 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Lässt die aktuelle EF diesen Befehl (EF Sensor_Installation_Data in DF Tachograph_G2) nicht zu, wird der Verarbeitungsstatus '**6985**' zurückgesendet.

— Wird die ausgewählte EF als verfälscht betrachtet (wegen Integritätsfehlern in den Dateiattributen oder den gespeicherten Daten), lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

— Ist die ausgewählte Datei keine transparente Datei oder gibt es keine aktuelle EF, wird der Verarbeitungsstatus '**6986**' zurückgesendet.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Dieser Befehl wird zur Berechnung der digitalen Signatur des zuvor berechneten Hashcodes (siehe PERFORM HASH of FILE, Abschnitt 3.5.13) verwendet.

Nur die Fahrer- und die Werkstattkarte müssen diesen Befehl in DF Tachograph und DF Tachograph_G2 unterstützen.

Andere Arten von Fahrtenschreiberkarten können diesen Befehl gegebenenfalls implementieren, dürfen aber nicht über einen Signaturschlüssel verfügen. Aus diesem Grund können diese Karten den Befehl nicht erfolgreich ausführen, sondern schließen mit einem geeigneten Fehlercode ab.

Der Befehl kann in MF gegebenenfalls zur Verfügung stehen. Wenn ja, muss der Befehl mit einem geeigneten Fehlercode abschließen.

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-8. Die Verwendung des Befehls ist jedoch im Vergleich zur entsprechenden Norm eingeschränkt.

TCS_126 Dieser Befehl darf keine digitale Signatur eines zuvor mit dem Befehl PSO: HASH berechneten Hashcodes verarbeiten.

TCS_127 Zur Berechnung der digitalen Signatur wird der private Schlüssel der Karte, der der Karte implizit bekannt ist, herangezogen.

TCS_128 Die Fahrtenschreiberanwendung der 1. Generation führt eine digitale Signatur mit Hilfe einer Auffüllmethode gemäß PKCS1 aus (Einzelheiten siehe Anlage 11).

TCS_129 Die Fahrtenschreiberanwendung der 2. Generation berechnet eine auf elliptischen Kurven basierende digitale Signatur (Einzelheiten siehe Anlage 11).

TCS_130 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	„00h“	CLA
INS	1	„2Ah“	Perform Security Operation
P1	1	„9Eh“	Zurückzusendende digitale Signatur
P2	1	„9Ah“	Tag: Datenfeld enthält zu signierende Daten. Da kein Datenfeld vorhanden ist, wird davon ausgegangen, dass die Daten bereits in der Karte vorhanden sind (Hash of File).
Le	1	„NNh“	Länge der erwarteten Signatur

TCS_131 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#L	L	‘XX..XXh’	Signatur des zuvor berechneten Hash
SW	2	‘XXXXh’	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte ‘**9000**’ zurück.

— Wird der implizit ausgewählte private Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ‘**6400**’ oder ‘**6581**’.

— Ist der in einem vorherigen „Perform Hash of File“-Befehl berechnete Hash nicht verfügbar, wird der Verarbeitungsstatus **‘6985’** zurückgesendet.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Dieser Befehl wird zur Verifizierung der als Eingabe bereitgestellten digitalen Signatur verwendet, deren Hash der Karte bekannt ist. Der Signaturalgorithmus ist der Karte implizit bekannt.

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-8. Die Verwendung des Befehls ist jedoch im Vergleich zur entsprechenden Norm eingeschränkt.

Nur die Kontrollkarte wird benötigt, um diesen Befehl in DF Tachograph und DF Tachograph_G2 zu unterstützen.

Andere Arten von Fahrtenschreiberkarten können diesen Befehl gegebenenfalls implementieren. Der Befehl kann in MF gegebenenfalls zur Verfügung stehen.

TCS_132 Der Befehl VERIFY DIGITAL SIGNATURE verwendet stets den vom vorhergehenden Befehl Manage Security Environment MSE: Set DST ausgewählten öffentlichen Schlüssel sowie den von einem PSO: HASH- Befehl eingegebenen Hashcode.

TCS_133 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'A8h'	Tag: Datenfeld enthält zur Verifizierung relevante DO
Lc	1	'83h'	Länge Lc des nachfolgenden Datenfelds
6	1	'9Eh'	Tag für digitale Signatur
#7-#8	2	'81 XXh'	Länge der digitalen Signatur: 128 Bytes kodiert gemäß Anlage 11 Teil A für Fahrtenschreiberanwendung der 1. Generation. Je nach der für die Fahrtenschreiberanwendung der 2. Generation ausgewählten Kurve (siehe Anlage 11 Teil B)
#9-#(8+L)	L	'XX..XXh'	Inhalt der digitalen Signatur

TCS_134 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— Schlägt die Verifizierung der Signatur fehl, lautet der zurückgesendete Verarbeitungsstatus '**6688**'. Der Verifizierungsvorgang wird in Anlage 11 beschrieben.

— Ist kein öffentlicher Schlüssel ausgewählt, lautet der zurückgesendete Verarbeitungsstatus '**6A88**'.

— Fehlen einige der erwarteten Datenobjekte (siehe oben), wird der Verarbeitungsstatus '**6987**' zurückgesendet. Das kann der Fall sein, wenn der erforderliche Tag fehlt.

— Ist kein Hash-Code zur Verarbeitung des Befehls verfügbar (im Ergebnis eines PSO: Hash-Befehls), lautet der zurückgesendete Verarbeitungsstatus '**6985**'.

— Sind einige Datenobjekte inkorrekt, lautet der zurückgesendete Verarbeitungsstatus '**6988**'. Dies kann der Fall sein, wenn eine Länge der erforderlichen Datenobjekte inkorrekt ist.

— Wird der ausgewählte öffentliche Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus '**6400**' oder '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Dieser Befehl wird verwendet, um die Integrität und Authentizität der DSRC-Nachricht zu verifizieren und um die von einer VU per DSRC-Link an eine Kontrollbehörde oder eine Werkstatt gesendeten Daten zu entschlüsseln. Die Karte leitet den zur Sicherung der DSRC-Nachricht gemäß Anlage 11 Teil B Kapitel 13 verwendeten Kodierungsschlüssel samt MAC-Schlüssel ab.

Nur die Kontroll- und die Werkstattkarte müssen diesen Befehl in DF Tachograph_G2 unterstützen.

Andere Arten von Fahrtenschreiberkarten können diesen Befehl gegebenenfalls implementieren, dürfen aber nicht über einen DSRC-Hauptschlüssel verfügen. Aus diesem Grund können diese Karten den Befehl nicht erfolgreich ausführen, sondern schließen mit einem geeigneten Fehlercode ab.

Der Befehl kann in MF und/oder DF Tachograph gegebenenfalls zur Verfügung stehen. Wenn ja, muss der Befehl mit einem geeigneten Fehlercode abschließen.

TCS_135 Der DSRC-Hauptschlüssel ist nur in DF Tachograph_G2 zugreifbar, d. h. Kontroll- und Werkstattkarte unterstützen die erfolgreiche Ausführung des Befehls lediglich in DF Tachograph_G2.

TCS_136 Der Befehl darf lediglich die DSRC-Daten entschlüsseln und die kryptografische Prüfsumme verifizieren, nicht aber die Eingabedaten interpretieren.

TCS_137 Die Reihenfolge der Datenobjekte im Befehlsdatenfeld ist durch diese Spezifikation festgelegt.

TCS_138 **Befehlsnachricht**

Byte	Länge	Wert	Beschreibung
CLA	1	'80h'	Proprietäres CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'80h'	Antwortdaten: Klarwert
P2	1	'B0h'	Befehlsdaten: in BER-TLV kodierter Klarwert mit SM DO
Lc	1	'NNh'	Länge Lc des nachfolgenden Datenfelds
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	DER-TLV-kodiertes Padding-Content Indicator-Byte, gefolgt von den verschlüsselten Fahrtenschreiberdaten. Für das Padding-Content Indicator-Byte ist der Wert '00h' („keine weitere Angabe" gemäß ISO/IEC 7816-4:2013 Tabelle 52) zu verwenden. Zur Verschlüsselung siehe Anlage 11 Teil B Kapitel 13. Zulässige Werte für die Länge L_{87} sind Vielfache der AES-Blocklänge zuzüglich 1 für das Padding-Content Indicator-Byte, d. h. von 17 Bytes bis einschließlich 193 Bytes. *Hinweis:* Siehe ISO/IEC 7816-4:2013 Tabelle 49 für das SM-Datenobjekt mit Tag '87h'.
		'81h' + '10h'	DER-TLV-kodiertes Control Reference Template for Confidentiality, das die Verkettung der folgenden Datenelemente gewährleistet (siehe Anlage 1 DSRCSecurityData und Anlage 11 Teil B Kapitel 13): — 4-Byte-Zeitstempel — 3-Byte-Zähler — 8-Byte-VU-Seriennummer — 1-Byte-DSRC-Hauptschlüsselversion *Hinweis:* Siehe ISO/IEC 7816-4:2013 Tabelle 49 für das SM-Datenobjekt mit Tag '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	DER-TLV-kodiertes MAC über der DSRC-Nachricht. Zu MAC-Algorithmus und Berechnung siehe Anlage 11 Teil B Kapitel 13. *Hinweis:* Siehe ISO/IEC 7816-4:2013 Tabelle 49 für das SM-Datenobjekt mit Tag '8Eh'.

TCS_139 **Antwortnachricht**

Byte	Länge	Wert	Beschreibung
#1-#L	L	'XX..XXh'	Fehlende (im Falle eines Fehlers) oder entschlüsselte Daten (Auffüllung entfernt)
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet die Karte '**9000**' zurück.

— '**6A80**' gibt fehlerhafte Parameter im Befehlsdatenfeld an (auch verwendet, wenn die Datenobjekte nicht in der angegebenen Reihenfolge gesendet werden).

— '**6A88**' gibt an, dass Daten, auf die verwiesen wird, nicht verfügbar sind (d. h. der DSRC-Hauptschlüssel, auf den verwiesen wird, ist nicht verfügbar).

— '**6900**' gibt an, dass die Verifizierung der kryptografischen Prüfsumme oder die Entschlüsselung der Daten fehlgeschlagen ist.

4. STRUKTUR DER FAHRTENSCHREIBERKARTEN

In diesem Abschnitt werden die Dateistrukturen, die auf den Fahrtenschreiberkarten der Speicherung zugänglicher Daten dienen, spezifiziert.

Nicht spezifiziert werden vom Kartenhersteller abhängige interne Strukturen, wie z. B. Dateianfangskennsätze oder die Speicherung und Verarbeitung von Datenelementen, die nur für den internen Gebrauch benötigt werden, z. B. `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` oder `WorkshopCardPin`.

TCS_140 Eine Fahrtenschreiberkarte der 2. Generation muss das Wurzelverzeichnis (MF) und eine Fahrtenschreiberanwendung gleichen Typs der 1. und 2. Generation aufnehmen (z. B. Fahrerkartenanwendungen).

TCS_141 Eine Fahrtenschreiberkarte muss zumindest die Mindestzahl der für die entsprechenden Anwendungen angegebenen Datensätze unterstützen und darf nicht mehr als die Höchstzahl der für die entsprechenden Anwendungen angegebenen Datensätze unterstützen.

Die Höchst- und die Mindestzahl an Datensätzen sind in diesem Kapitel für die unterschiedlichen Anwendungen angegeben.

Zu den Sicherheitsbedingungen, die in den in diesem Kapitel verwendeten Zugriffsregeln verwendet werden, siehe Kapitel 3.3. Generell bezeichnet der Zugriffsmodus „Lesen" den Befehl READ BINARY mit geradem und bei entsprechender Unterstützung mit ungeradem INS-Byte, ausgenommen die EF Sensor_Installation_Data auf der Werkstattkarte, siehe TCS_156 und TCS_160. Der Zugriffsmodus „Aktualisieren" bezeichnet den Befehl Update Binary mit geraden und bei entsprechender Unterstützung mit ungeradem INS-Byte und der Zugriffsmodus „Auswählen" den Befehl SELECT.

4.1. Wurzelverzeichnis (MF)

TCS_142 Nach der Personalisierung weist das Wurzelverzeichnis (MF) folgende permanente Dateistruktur und Dateizugriffsregeln auf:

Hinweis: Die Kurz-Elementardateikennung SFID wird als Dezimalzahl ausgedrückt; beispielsweise entspricht der Wert 30 dem Binärwert 11110.

			Zugriffsregeln	
Datei	**Dateikennung**	**SFID**	**Lesen/Auswählen**	**Aktualisieren**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

In dieser Tabelle wird die folgende Abkürzung für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

TCS_143 Die Strukturen aller EF sind transparent.

TCS_144 Das Wurzelverzeichnis (MF) hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
MF		*63*	*184*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	{00..00}
│ └─icManufacturingReferences		4	4	{00..00}
├─EF DIR		*20*	*20*	
│ └─See TCS_145		*20*	*20*	{00..00}
├─EF ATR/INFO		*7*	*128*	
│ └─See TCS_146		*7*	*128*	{00..00}
├─EF EXTENDED_LENGTH		*3*	*3*	
│ └─See TCS_147		*3*	*3*	{00..00}
├─DF Tachograph				
└─DF Tachograph_G2				

TCS_145 Die Elementardatei EF DIR muss die folgenden anwendungsbezogenen Datenobjekte enthalten: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Die Elementardatei EF ATR/INFO muss vorhanden sein, wenn die Fahrtenschreiberkarte in ihrer ATR angibt, dass sie erweiterte Längenfelder unterstützt. In diesem Fall muss EF ATR/INFO das Datenobjekt mit der erweiterten Längenangabe (DO'7F66') gemäß ISO/IEC 7816-4:2013 Punkt 12.7.1 enthalten.

TCS_147 Die Elementardatei EF Extended_Length muss vorhanden sein, wenn die Fahrtenschreiberkarte in ihrer ATR angibt, dass sie erweiterte Längenfelder unterstützt. In diesem Fall muss die Elementardatei das folgende Datenobjekt enthalten: '02 01 xx', wobei der Wert 'xx' angibt, ob erweiterte Längenfelder für das Protokoll T = 1 und/oder T = 0 unterstützt werden.

Der Wert '01' zeigt die Unterstützung erweiterter Längenfelder für das Protokoll T = 1 an.

Der Wert '10' zeigt die Unterstützung erweiterter Längenfelder für das Protokoll T = 0 an.

Der Wert '11' zeigt die Unterstützung erweiterter Längenfelder für das Protokoll T = 1 und T = 0 an.

4.2. **Fahrerkartenanwendungen**

4.2.1 *Fahrerkartenanwendung der 1. Generation*

TCS_148 Nach der Personalisierung weist die Fahrerkartenanwendung der 1. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

		Zugriffsregeln		
Datei	**Dateikennung**	**Lesen**	**Auswählen**	**Aktualisieren**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

In dieser Tabelle werden die folgenden Abkürzungen für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

SC2 ALW ODER SM-MAC-G1 ODER SM-MAC-G2

SC3 SM-MAC-G1 ODER SM-MAC-G2

TCS_149 Die Strukturen aller EF sind transparent.

TCS_150 Die Fahrerkartenanwendung der 1. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Fahrerkarte für eine Anwendung der 1. Generation verwenden muss:

		Min.	**Max.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 Bytes (28 Tage * 93 Tätigkeitsveränderungen)	13 776 Bytes (28 Tage * 240 Tätigkeitsveränderungen)

4.2.2 *Fahrerkartenanwendung der 2. Generation*

TCS_152 Nach der Personalisierung weist die Fahrerkartenanwendung der 2. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

Hinweis: Die Kurz-Elementardateikennung SFID wird als Dezimalzahl ausgedrückt; beispielsweise entspricht der Wert 30 dem Binärwert 11110.

			Zugriffsregeln	
Datei	**Dateikennung**	**SFID**	**Lesen/Auswählen**	**Aktualisieren**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
├─EF Card_Download	'050Eh'	7	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

In dieser Tabelle wird die folgende Abkürzung für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

TCS_153 Die Strukturen aller EF sind transparent.

TCS_154 Die Fahrerkartenanwendung der 2. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Fahrerkarte für eine Anwendung der 2. Generation verwenden muss:

		Min.	**Max.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 Bytes (28 Tage * 93 Tätigkeitsveränderungen)	13 776 Bytes (28 Tage * 240 Tätigkeitsveränderungen)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Werkstattkartenanwendungen**

4.3.1 *Werkstattkartenanwendung der 1. Generation*

TCS_156 Nach der Personalisierung weist die Werkstattkartenanwendung der 1. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

		Zugriffsregeln		
Datei	**Dateikennung**	**Lesen**	**Auswählen**	**Aktualisieren**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	SC2	SC1	NEV
├EF Card_Download	'0509h'	SC2	SC1	**SC1**
├EF Calibration	'050Ah'	SC2	SC1	SC3
├EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├EF Events_Data	'0502h'	SC2	SC1	SC3
├EF Faults_Data	'0503h'	SC2	SC1	SC3
├EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├EF Places	'0506h'	SC2	SC1	SC3
├EF Current_Usage	'0507h'	SC2	SC1	SC3
├EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└EF Specific_Conditions	'0522h'	SC2	SC1	SC3

In dieser Tabelle werden die folgenden Abkürzungen für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

SC2 ALW ODER SM-MAC-G1 ODER SM-MAC-G2

SC3 SM-MAC-G1 ODER SM-MAC-G2

SC4 Für den Befehl READ BINARY mit geradem INS-Byte:

(PLAIN-C UND SM-R-ENC-G1) ODER (SM-C-MAC-G1 UND SM-R-ENC-MAC-G1) ODER (SM-C-MAC-G2 UND SM-R-ENC-MAC-G2)

Für den Befehl READ BINARY mit ungeradem INS-Byte (falls unterstützt): NEV

TCS_157 Die Strukturen aller EF sind transparent.

TCS_158 Die Werkstattkartenanwendung der 1. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Werkstattkarte für eine Anwendung der 1. Generation verwenden muss:

		Min.	**Max.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 Bytes (1 Tag * 93 Tätigkeitsveränderungen)	492 Bytes (1 Tag * 240 Tätigkeitsveränderungen)

4.3.2 *Werkstattkartenanwendung der 2. Generation*

TCS_160 Nach der Personalisierung weist die Werkstattkartenanwendung der 2. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

Hinweis: Die Kurz-Elementardateikennung SFID wird als Dezimalzahl ausgedrückt; beispielsweise entspricht der Wert 30 dem Binärwert 11110.

			Zugriffsregeln		
Datei	**Dateikennung**	**SFID**	**Lesen**	**Auswählen**	**Aktualisieren**
└─DF Tachograph_G2			SC1	SC1	
├─EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├─EF Identification	'0520h'	6	SC1	SC1	NEV
├─EF Card_Download	'0509h'	7	SC1	SC1	SC1
├─EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├─EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
├─EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

In dieser Tabelle werden die folgenden Abkürzungen für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

SC5 Für den Befehl Read Binary mit geradem INS-Byte: SM-C-MAC-G2 UND SM-R-ENC-MAC-G2

Für den Befehl Read Binary mit ungeradem INS-Byte (falls unterstützt): NEV

TCS_161 Die Strukturen aller EF sind transparent.

TCS_162 Die Werkstattkartenanwendung der 2. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Werkstattkarte für eine Anwendung der 2. Generation verwenden muss:

		Min.	**Max.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 Bytes (1 Tag * 93 Tätigkeitsveränderungen)	492 Bytes (1 Tag * 240 Tätigkeitsveränderungen)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Kontrollkartenanwendungen

4.4.1 *Kontrollkartenanwendung der 1. Generation*

TCS_164 Nach der Personalisierung weist die Kontrollkartenanwendung der 1. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

		Zugriffsregeln		
Datei	**Dateikennung**	**Lesen**	**Auswählen**	**Aktualisieren**
└DF Tachograph	'0500h'			
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

In dieser Tabelle werden die folgenden Abkürzungen für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

SC2 ALW ODER SM-MAC-G1 ODER SM-MAC-G2

SC3 SM-MAC-G1 ODER SM-MAC-G2

SC6 EXT-AUT-G1 ODER SM-MAC-G1 ODER SM-MAC-G2

TCS_165 Die Strukturen aller EF sind transparent.

TCS_166 Die Kontrollkartenanwendung der 1. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Kontrollkarte für eine Anwendung der 1. Generation verwenden muss:

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Kontrollkartenanwendung der 2. Generation*

TCS_168 Nach der Personalisierung weist die Kontrollkartenanwendung der 2. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

Hinweis: Die Kurz-Elementardateikennung SFID wird als Dezimalzahl ausgedrückt; beispielsweise entspricht der Wert 30 dem Binärwert 11110.

			Zugriffsregeln	
Datei	**Dateikennung**	**SFID**	**Lesen/Auswählen**	**Aktualisieren**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

In dieser Tabelle wird die folgende Abkürzung für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

TCS_169 Die Strukturen aller EF sind transparent.

TCS_170 Die Kontrollkartenanwendung der 2. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Kontrollkarte für eine Anwendung der 2. Generation verwenden muss:

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.5. Unternehmenskartenanwendungen

4.5.1 *Unternehmenskartenanwendung der 1. Generation*

TCS_172 Nach der Personalisierung weist die Unternehmenskartenanwendung der 1. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

		Zugriffsregeln		
Datei	**Dateikennung**	**Lesen**	**Auswählen**	**Aktualisieren**
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	**SC6**	SC1	NEV
EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

In dieser Tabelle werden die folgenden Abkürzungen für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

SC2 ALW ODER SM-MAC-G1 ODER SM-MAC-G2

SC3 SM-MAC-G1 ODER SM-MAC-G2

SC6 EXT-AUT-G1 ODER SM-MAC-G1 ODER SM-MAC-G2

TCS_173 Die Strukturen aller EF sind transparent.

TCS_174 Die Unternehmenskartenanwendung der 1. Generation hat folgende Datenstruktur:

Datei/Datenelement	**Anzahl Datensätze**	**Größe (Bytes) Min.**	**Max.**	**Standardwerte**
DF Tachograph		*11114*	*24454*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Unternehmenskarte für eine Anwendung der 1. Generation verwenden muss:

		Min.	**Max.**
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Unternehmenskartenanwendung der 2. Generation*

TCS_176 Nach der Personalisierung weist die Unternehmenskartenanwendung der 2. Generation folgende permanente Dateistruktur und Dateizugriffsregeln auf:

Hinweis: Die Kurz-Elementardateikennung SFID wird als Dezimalzahl ausgedrückt; beispielsweise entspricht der Wert 30 dem Binärwert 11110.

			Zugriffsregeln	
Datei	**Dateikennung**	**SFID**	**Lesen/Auswählen**	**Aktualisieren**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

In dieser Tabelle wird die folgende Abkürzung für die Sicherheitsbedingung verwendet:

SC1 ALW ODER SM-MAC-G2

TCS_177 Die Strukturen aller EF sind transparent.

TCS_178 Die Unternehmenskartenanwendung der 2. Generation hat folgende Datenstruktur:

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Unternehmenskarte für eine Anwendung der 2. Generation verwenden muss:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

Anlage 3

PIKTOGRAMME

PIC_001 Vom Fahrtenschreiber können fakultativ folgende Piktogramme und Piktogrammkombinationen (oder Piktogramme und Kombinationen, die hinreichend ähnlich sind, um eindeutig als diese erkannt zu werden) verwendet werden:

1. EINZELPIKTOGRAMME

	Personen	**Maßnahmen**	**Betriebsarten**
	Unternehmen		Betriebsart Unternehmen
	Kontrolleur	Kontrolle	Betriebsart Kontrolle
	Fahrer	Lenken	Betriebsart Betrieb
	Werkstatt/Prüfstelle	Überprüfung/Kalibrierung	Betriebsart Kalibrierung
	Hersteller		

	Tätigkeiten	**Dauer**
	Bereitschaft	Laufende Bereitschaftszeit
	Lenken	Kontinuierliche Lenkzeit
	Ruhe	Laufende Ruhezeit
	Sonstige Arbeit	Laufende Arbeitszeit
	Unterbrechung	Kumulative Pausenzeit
?	Unbekannt	

	Geräte	**Funktionen**
1	Steckplatz Fahrer	
2	Steckplatz Beifahrer	
	Karte	
	Uhr	
	Anzeige	Anzeigen
	Externe Speicherung	Herunterladen
	Stromversorgung	
	Drucker/Ausdruck	Drucken
	Sensor	
	Reifengröße	
	Fahrzeug/Fahrzeugeinheit	
	GNSS-Ausrüstung	
	Ausrüstung zur Fernkommunikation	
	ITS-Schnittstelle	

	Spezifische Bedingungen
OUT	Kontrollgerät nicht erforderlich
	Fährüberfahrt/Zugfahrt

Verschiedenes

!	Ereignisse	⨯	Störungen
⏵	Beginn des Arbeitstages	⏹	Ende des Arbeitstages
●	Ort		
M	Manuelle Eingabe der Fahrertätigkeiten		
🔒	Sicherheit		
>	Geschwindigkeit		
🕒	Zeit		
Σ	Gesamt/Zusammenfassung		

Qualifikatoren

24h	täglich
|	wöchentlich
||	zwei Wochen
+	von oder bis

2. PIKTOGRAMMKOMBINATIONEN

Verschiedenes

🏛●	Kontrollort		
●⏵	Ort des Beginns des Arbeitstages	⏹●	Ort des Endes des Arbeitstages
🕒+	Anfangszeit	+🕒	Endzeit
🚌+	von Fahrzeug		
OUT+	Kontrollgerät nicht erforderlich — Beginn	+OUT	Kontrollgerät nicht erforderlich — Ende

Karten

🪪	Fahrerkarte
🏢🪪	Unternehmenskarte
🏛🪪	Kontrollkarte
🔧🪪	Werkstattkarte
🪪– – –	Keine Karte

Lenken

🪪🪪	Team
🪪 |	Lenkzeit für eine Woche
🪪 ||	Lenkzeit für zwei Wochen

Ausdrucke

24h 🪪🖨	Täglicher Ausdruck Fahrertätigkeiten von der Karte
24h 🚌🖨	Täglicher Ausdruck Fahrertätigkeiten von der VU
! ⨯🪪🖨	Ausdruck Ereignisse und Störungen von der Karte
! ⨯🚌🖨	Ausdruck Ereignisse und Störungen von der VU
🔧🕒🖨	Ausdruck Technische Daten
>>🖨	Ausdruck Geschwindigkeitsüberschreitung

Ereignisse

	Einstecken einer ungültigen Karte
	Kartenkonflikt
	Zeitüberlappung
	Lenken ohne geeignete Karte
	Einstecken der Karte während des Lenkens
	Letzter Vorgang nicht korrekt abgeschlossen
	Geschwindigkeitsüberschreitung
	Unterbrechung der Stromversorgung
	Datenfehler Weg und Geschwindigkeit
	Datenkonflikt Fahrzeugbewegung
	Sicherheitsverletzung
	Zeiteinstellung (durch Werkstatt)
	Kontrolle Geschwindigkeitsüberschreitung

Störungen

	Kartenfehlfunktion (Steckplatz Fahrer)
	Kartenfehlfunktion (Steckplatz Beifahrer)
	Anzeigestörung
	Störung beim Herunterladen
	Druckerstörung
	Sensorstörung
	Interne VU-Störung
	GNSS-Störung
	Störung der Fernabfrage

Manueller Eingabevorgang

	Weiterhin derselbe Arbeitstag?
	Ende des vorherigen Arbeitstages?
	Bestätigung oder Eingabe Ort des Arbeitstagendes
	Eingabe Anfangszeit
	Eingabe Ort des Arbeitstagbeginns.

Anmerkung: Weitere Piktogrammkombinationen als Block- oder Datensatzbezeichner auf Ausdrucken sind in Anlage 4 festgelegt.

Anlage 4

AUSDRUCKE

INHALTSVERZEICHNIS

1. ALLGEMEINES 243
2. SPEZIFIKATION DER DATENBLÖCKE 243
3. SPEZIFIKATION DER AUSDRUCKE 250
3.1. Tagesausdruck Fahrertätigkeiten von der Karte 250
3.2. Tagesausdruck Fahrertätigkeiten von der Fahrzeugeinheit (VU) 251
3.3. Ausdruck Ereignisse und Störungen von der Karte 252
3.4. Ausdruck Ereignisse und Störungen von der VU 252
3.5. Ausdruck Technische Daten 253
3.6. Ausdruck Geschwindigkeitsüberschreitung 253
3.7. Historie der eingesteckten Karten 254

1. ALLGEMEINES

Jeder Ausdruck besteht aus einer Aneinanderreihung verschiedener Datenblöcke, die durch einen Blockbezeichner ausgewiesen werden können.

Ein Datenblock enthält einen oder mehrere Datensätze, die durch einen Datensatzbezeichner ausgewiesen werden können.

PRT_001 Steht ein Blockbezeichner unmittelbar vor einem Datensatzbezeichner, wird der Datensatzbezeichner nicht gedruckt.

PRT_002 Ist eine Datenangabe unbekannt oder darf aus datenzugriffsrechtlichen Gründen nicht gedruckt werden, werden stattdessen Leerzeichen ausgedruckt.

PRT_003 Ist der Inhalt einer ganzen Zeile unbekannt oder braucht nicht gedruckt zu werden, wird die gesamte Zeile weggelassen.

PRT_004 Nummerische Datenfelder werden rechtsbündig, mit einer Leerstelle zur Abtrennung von Tausendern und Millionen und ohne Führungsnullen gedruckt.

PRT_005 Datenfelder mit Zeichenfolgen werden linksbündig gedruckt und nach Bedarf bis zur Datenelementlänge mit Leerzeichen aufgefüllt oder auf Datenelementlänge abgeschnitten (Namen und Anschriften).

PRT_006 Bei einem Zeilenumbruch aufgrund eines langen Textes muss die neue Zeile mit einem Sonderzeichen (Punkt auf Mitte der Zeilenhöhe, „•“) beginnen.

2. SPEZIFIKATION DER DATENBLÖCKE

In diesem Kapitel wurden folgende Konventionen für die Notation verwendet:

— Zeichen in **Fettdruck** stehen für zu druckenden Klartext (im Ausdruck erscheinen die Zeichen unformatiert).

— Unformatierte Zeichen stehen für Variablen (Piktogramme oder Daten), die beim Ausdrucken durch ihre Werte ersetzt werden.

— Bezeichnungen von Variablen wurden mit Unterstrichen ergänzt, um die für die Variable verfügbare Datenelementlänge sichtbar zu machen.

— Datumsangaben sind im Format „TT/MM/JJJJ“ (Tag, Monat, Jahr) spezifiziert. Verwendet werden kann auch das Format „TT.MM.JJJJ“.

— Die „Kartenkennung“ setzt sich aus folgenden Elementen zusammen: Angabe der Kartenart durch entsprechende Piktogrammkombination, Code des ausstellenden Mitgliedstaates, Schrägstrich und Kartennummer mit durch Leerstelle abgetrenntem Ersatzindex und Erneuerungsindex:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Karten-Piktogrammkombination		Code des ausstellenden Mitgliedstaates				Erste 14 Zeichen der Kartennummer (möglichst mit einem fortlaufenden Index)														Ersatzindex		Erneuerungsindex

PRT_007 Ausdrucke verwenden die folgenden Datenblöcke und/oder Datensätze in der jeweiligen Bedeutung und Form:

Block- oder Datensatznummer Bedeutung	Datenformat
1 ***Datum und Uhrzeit des Ausdrucks***	TT/MM/JJJJ hh:mm **(UTC)**
2 ***Art des Ausdrucks*** Blockbezeichner Ausdruck Piktogrammkombination (s. Anl. 3), Einstellung des Geschwindigkeitsbegrenzers (nur bei Ausdruck Geschwindigkeitsüberschreitung)	----------T---------- Pikto xxx **km/h**
3 ***Angaben zum Karteninhaber*** Blockbezeichner. P = Piktogramm Personen Name des Karteninhabers Vorname(n) des Inhabers (wenn zutreffend) Kartenkennung Kartenablaufdatum (wenn zutreffend) und Kartengenerationsnummer (GEN 1 oder GEN 2) (*)	----------P---------- P Zuname_____ Vorname_____ Kartenkennung_____ TT/MM/JJJJ - GEN 2

Handelt es sich um eine nicht personengebundene Karte ohne Namen des Karteninhabers, ist stattdessen der Name des Unternehmens, der Werkstatt oder der Kontrollstelle zu drucken.

(*) Die Kartengenerationsnummer kann nur durch intelligente Fahrtenschreiber gedruckt werden.

4 ***Fahrzeugkennung*** Blockbezeichner Fahrzeugidentifizierungsnummer (VIN) Zulassender Mitgliedstaat und amtliches Kennzeichen (VRN)	----------A---------- A VIN_____ Nat/ VRN_____
5 ***VU-Kennung (VU = Fahrzeugeinheit)*** Blockbezeichner Name des FE-Herstellers FE-Teilnummer FE-Generationsnummer (*)	----------B---------- B VU-Hersteller_____ VU-Teilnummer__ GEN 2

(*) Die Kartengenerationsnummer kann nur durch intelligente Fahrtenschreiber gedruckt werden.

6 ***Letzte Kalibrierung des Fahrtenschreibers*** Blockbezeichner Name der Werkstatt Werkstattkartenkennung Datum der Kalibrierung	----------T---------- T Name_____ Kartenkennung_____ T TT/MM/JJJJ

7 ***Letzte Kontrolle (durch einen Kontrolleur)***

Blockbezeichner	----------▯----------
Kontrollkartenkennung	Kartenkennung_____
Datum, Uhrzeit und Art der Kontrolle	▯ TT/MM/JJJJ hh:mm ppppp

Art der Kontrolle: bis zu fünf Piktogramme. Die Art der Kontrolle kann sein (auch in Kombination):

▮: Herunterladen Karte, ↧: Herunterladen VU, ▛: Drucken, ▯: Anzeige, ⍑: Kalibrierungskontrolle unterwegs:

8 ***Fahrertätigkeiten, auf einer Karte in der Reihenfolge des Auftretens gespeichert***

Blockbezeichner	----------⊙----------
Abfragedatum (Kalendertag des Ausdrucks) + Tagesanwesenheitszähler	TT/MM/JJJJ xxx

8a	*Bedingung „Kontrollgerät nicht erforderlich" zu Tagesbeginn* (freilassen, wenn diese Bedingung nicht eingeschaltet ist)	----------OUT----------
8.1	*Zeitraum, in dem die Karte nicht eingesteckt war*	
8.1a	Datensatzbezeichner (Beginn des Zeitraums)	----------
8.1b	*Unbekannter Zeitraum*. Uhrzeit Beginn, Dauer	? hh:mm hh**h**mm
8.1c	*Manuell eingegebene Tätigkeit*. Piktogramm Tätigkeit (A), Uhrzeit Beginn, Dauer.	A hh:mm hh**h**mm
8.2	*Einstecken der Karte in Steckplatz S*	
	Datensatzbezeichner; S = Piktogramm Steckplatz	---------S---------
	Zulassender Mitgliedstaat und amtliches Kennzeichen (VRN)	Nat/ VRN_____
	Kilometerstand beim Einstecken der Karte	x xxx xxx **km**
8.3	*Tätigkeit (bei eingesteckter Karte)*	
	Piktogramm Tätigkeit (A), Uhrzeit Beginn, Dauer, Status der Fahrzeugführung (Piktogramm Team bei TEAM, Leerstellen bei EINMANNBETRIEB).	A hh:mm hh**h**mm ⊙⊙
8.3a	*Spezifische Bedingung*. Eingabezeit, Piktogramm Spezifische Bedingung (oder Piktogrammkombination).	hh:mm ---pppp---
8.4	*Entnahme der Karte*	
	Kilometerstand und zurückgelegte Wegstrecke seit dem letzten Einstecken, für das der Kilometerstand bekannt ist	x xxx xxx **km**; x xxx **km**

9 ***Fahrertätigkeiten, in einer VU je Steckplatz in chronologischer Reihenfolge gespeichert***

Blockbezeichner	----------⊙----------
Abfragedatum (Kalendertag, der Gegenstand des Ausdrucks ist)	TT/MM/JJJJ
Kilometerstand um 0:00 Uhr und 24:00 Uhr	x xxx xxx - x xxx xxx **km**

10 ***Tätigkeiten in Steckplatz S***

	Blockbezeichner	----------S----------
10a	*Bedingung "Kontrollgerät nicht erforderlich" zu Tagesbeginn* (freilassen, wenn diese Bedingung nicht eingeschaltet ist)	----------OUT----------
10.1	*Zeitraum, in dem keine Karte in Steckplatz S eingesteckt ist*	
	Datensatzbezeichner.	----------
	Keine Karte eingesteckt	⊙▮---
	Kilometerstand zu Beginn des Zeitraums	x xxx xxx **km**
10.2	*Einstecken der Karte*	
	Datensatzbezeichner Einstecken der Karte	----------
	Name des Fahrers	⊙ Name_____

	Vorname(n) des Fahrers	Vorname_____
	Fahrerkartenkennung	Kartenkennung_____
	(ggf.) Kartenablaufdatum und Kartengenerationsnummer (GEN 1 oder GEN 2) (*)	TT/MM/JJJJ - GEN 2
	Zulassender Mitgliedstaat und amtliches Kennzeichen des vorherigen Fahrzeuges	+Nat/Kennzeichen_____
	Datum und Uhrzeit der Kartenentnahme aus vorherigem Fahrzeug	TT/MM/JJJJ hh:mm
	Leerzeile	
	Kilometerstand beim Einstecken der Karte, manuelle Eingabe der Fahrertätigkeits-Flags (M = ja, leer = nein)	x xxx xxx **km** M
	Falls an dem Tag, für den der Ausdruck erfolgt, keine Fahrerkarte eingesteckt wurde, wird für Block 10.2 der Kilometerzählerstand der letzten verfügbaren Karteneinführung vor diesem Tag verwendet.	
10.3	*Tätigkeit*	
	Piktogramm Tätigkeit (A), Uhrzeit Beginn, Dauer, Status der Fahrzeugführung (Piktogramm Team bei TEAM, Leerstellen bei EINMANNBETRIEB).	A hh:mm hh**h**mm ⊙⊙
10.3a	Spezifische Bedingung. Eingabezeit, Piktogramm Spezifische Bedingung (oder Piktogrammkombination).	hh:mm ---pppp---
10.4	*Kartenentnahme oder Ende des Zeitraums „keine Karte“*	
	Kilometerstand bei Kartenentnahme oder am Ende des Zeitraums „keine Karte“ und zurückgelegte Wegstrecke seit Einstecken der Karte oder seit Beginn des Zeitraums „keine Karte“	x xxx xxx **km**; x xxx **km**

(*) Die Kartengenerationsnummer kann nur durch intelligente Fahrtenschreiber gedruckt werden.

11	***Tageszusammenfassung***	
	Blockbezeichner	----------Σ----------
11.1	***VU-Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Fahrer***	
	Blockbezeichner	1⊙----
11.2	***VU-Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Beifahrer***	
	Blockbezeichner	2⊙----
11.3	***VU-Tageszusammenfassung je Fahrer***	
	Datensatzbezeichner	----------
	Name des Fahrers	⊙ Name_____
	Vorname(n) des Fahrers	Vorname_____
	Fahrerkartenkennung	Kartenkennung_____
11.4	*Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages*	
	pi = Piktogramm Ort Beginn/Ende, Uhrzeit, Land, Region	pihh:mm Lnd Reg
	Kilometerstand	x xxx xxx **km**
11.5	*Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages*	
	sowie nach 3 Stunden ununterbrochener Lenkzeit	hh:mm
	Kilometerstand	x xxx xxx **km**
11.6	*Gesamtwerte Tätigkeiten (von einer Karte)*	
	Gesamtlenkzeit, zurückgelegte Wegstrecke	⊙ hh**h**mm x xxx **km**
	Gesamte Arbeits- und Bereitschaftszeit	⚒ hh**h**mm ⧈ hh**h**mm
	Gesamtruhezeit und unbekannte Zeiten	⊢ hh**h**mm ? hh**h**mm
	Gesamtzeit Teamtätigkeiten	⊙⊙ hh**h**mm
11.7	*Gesamtwerte Tätigkeiten (Zeitabschnitte ohne Steckplatz Fahrer)*	
	Gesamtlenkzeit, zurückgelegte Wegstrecke	⊙ hh**h**mm x xxx **km**
	Gesamte Arbeits- und Bereitschaftszeit	⚒ hh**h**mm ⧈ hh**h**mm
	Gesamtruhezeit	⊢ hh**h**mm

11.8 *Gesamtwerte Tätigkeiten (Zeitabschnitte ohne Steckplatz Beifahrer)*

Gesamte Arbeits- und Bereitschaftszeit
Gesamtruhezeit

```
⚒ hhhmm  ⧈ hhhmm
⊢ hhhmm
```

11.9 *Gesamtwerte Tätigkeiten (je Fahrer, beide Steckplätze)*

Gesamtlenkzeit, zurückgelegte Wegstrecke
Gesamte Arbeits- und Bereitschaftszeit
Gesamtruhezeit
Gesamtzeit Teamtätigkeiten

```
⊙ hhhmm  x xxx km
⚒ hhhmm  ⧈ hhhmm
⊢ hhhmm
⊙⊙ hhhmm
```

Wird ein Tagesausdruck für den aktuellen Tag benötigt, erfolgt die Berechnung der Angaben für die Tageszusammenfassung anhand der zum Zeitpunkt des Ausdrucks vorhandenen Daten.

12 ***Auf einer Karte gespeicherte Ereignisse und/oder Störungen***

12.1 Blockbezeichner für die letzten 5 Ereignisse und Störungen auf der Karte

```
----------!×▬----------
```

12.2 Blockbezeichner für alle aufgezeichneten Ereignisse auf der Karte

```
----------!▬----------
```

12.3 Blockbezeichner für alle aufgezeichneten Störungen auf der Karte

```
----------×▬----------
```

12.4 *Datensatz Ereignis und/oder Störung*

Datensatzbezeichner
Piktogramm Ereignis/Störung, Datensatzzweck, Datum/Zeit Beginn
(ggf.) weiterer Ereignis-/Störungscode, Dauer
Zulassender Mitgliedstaat und amtliches Kennzeichen des Fahrzeugs, in dem Ereignis oder Störung auftrat

```
  --------------------
Pik (z) TT/MM/JJJJ hh:mm
!xx                hhhmm
♟ Nat/ VRN__________
```

13 ***In einer VU gespeicherte oder andauernde Ereignisse und Störungen***

13.1 Blockbezeichner für die letzten 5 Ereignisse und Störungen in der VU

```
----------!×♟----------
```

13.2 Blockbezeichner für alle aufgezeichneten oder andauernden Ereignisse in der VU

```
----------!♟----------
```

13.3 Blockbezeichner für alle aufgezeichneten oder andauernden Störungen in der VU

```
----------×♟----------
```

13.4 *Datensatz Ereignis und/oder Störung*

Datensatzbezeichner
Piktogramm Ereignis/Störung, Datensatzzweck, Datum/Zeit Beginn
weiterer Ereignis-/Störungscode (wenn zutreffend), Anzahl ähnlicher Ereignisse an diesem Tag, Dauer
Kennung der zu Beginn oder am Ende des Ereignisses oder der Störung eingesteckten Karten (bis zu 4 Zeilen ohne Wiederholung derselben Kartennummern)

Falls keine Karte eingesteckt
Herstellerspezifische Daten

```
  --------------------
Pik (z) TT/MM/JJJJ hh:mm
!xx     (xxx)      hhhmm

Kartenkennung_____
Kartenkennung_____
Kartenkennung_____
Kartenkennung_____
 ▬---
< Literal><Fehlercode>
```

Der Datensatzzweck (z) ist ein numerischer Code zur Erläuterung, warum das Ereignis oder die Störung aufgezeichnet wurde; die Codierung erfolgt entsprechend dem Datenelement `EventFaultRecordPurpose`.
`Literal` ist ein für die Fahrtenschreiberhersteller spezifisches Literal mit maximal 12 Zeichen.
`Fehlercode` ist ein für die Fahrtenschreiberhersteller spezifischer Fehlercode mit maximal 12 Zeichen.

14	***VU-Kennung***	
	Blockbezeichner	----------🖯----------
	Name des VU-Herstellers	🖯 Name_____
	Anschrift des VU-Herstellers	Anschrift_____
	VU-Teilnummer	Teilnummer_____
	VU-Typgenehmigungsnummer	Genehmigungsnr._____
	VU-Seriennummer	Seriennr._____
	VU-Baujahr	JJJJ
	Version und Installationsdatum der VU-Software	V xxxx TT/MM/JJJJ
15	***Sensorkennung***	
	Blockbezeichner	----------🖪----------
15.1	*Datensatz Kopplung*	
	Seriennummer des Sensors	🖪 Seriennr._____
	Typgenehmigungsnummer des Sensors	Genehmigungsnr._____
	Datum der Sensorkopplung	TT/MM/JJJJ hh:mm
16	***GNSS-Kennnummer***	
	Blockbezeichner	----------▚----------
16.1	*Datensatz Kopplung*	
	Seriennummer der externen GNSS-Ausrüstung	▚ Seriennr._____
	Genehmigungsnummer der externen GNSS-Ausrüstung	Genehmigungsnr._____
	Kopplungsdatum der externen GNSS-Ausrüstung	TT/MM/JJJJ hh:mm
17	***Kalibrierungsdaten***	
	Blockbezeichner	----------🖬----------
17.1	*Datensatz Kalibrierung*	
	Datensatzbezeichner	---
	Werkstatt, die die Kalibrierung ausgeführt hat	🖬 Name_Werkstatt_____
	Anschrift der Werkstatt	Anschrift_Werkstatt___
	Werkstattkartenkennung	Kartenkennung_____
	Werkstattkarte gültig bis	TT/MM/JJJJ
	Leerzeile	
	Kalibrierungsdatum + Zweck der Kalibrierung	🖬 TT/MM/JJJJ (z)
	Fahrzeugidentifizierungsnummer (VIN)	🚙 VIN_____
	Zulassender Mitgliedstaat und amtliches Kennzeichen (VRN)	Nat/VRN_____
	Wegdrehzahl des Fahrzeugs	w xx xxx Imp/km
	Konstante des Kontrollgeräts	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Reifengröße	● Reifengröße_____
	Einstellung des Geschwindigkeitsbegrenzers	› xxx km/h
	Alter und neuer Kilometerstand	x xxx xxx – x xxx xxx km

Der Kalibrierungszweck (z) ist ein numerischer Code zur Erläuterung, warum diese Kalibrierungsparameter aufgezeichnet wurden; die Codierung erfolgt entsprechend dem Datenelement `CalibrationPurpose`.

18	***Zeiteinstellung***	
	Blockbezeichner	`----------◷----------`
18.1	*Datensatz Zeiteinstellung*	
	Datensatzbezeichner	`--------------------`
	Datum und Uhrzeit (alt)	`!◷ TT/MM/JJJJ hh:mm`
	Datum und Uhrzeit (neu)	`◷ TT/MM/JJJJ hh:mm`
	Werkstatt, in der die Zeiteinstellung vorgenommen wurde	`⍑ Name_Werkstatt_____`
	Anschrift der Werkstatt	`Anschrift_Werkstatt___`
	Werkstattkartenkennung	`Kartenkennung_____`
	Werkstattkarte gültig bis	`TT/MM/JJJJ`

19	***Jüngste(s) in der VU aufgezeichnete(s) Ereignis und Störung***	
	Blockbezeichner	`----------!×🖷----------`
	Jüngstes Ereignis, Datum und Uhrzeit	`! TT/MM/JJJJ hh:mm`
	Jüngste Störung, Datum und Uhrzeit	`× TT/MM/JJJJ hh:mm`

20	***Angaben zur Kontrolle Geschwindigkeitsüberschreitung (GÜ)***	
	Blockbezeichner	`----------»»----------`
	Datum und Uhrzeit der letzten KONTROLLE GÜ.	`»◘TT/MM/JJJJ hh:mm`
	Datum/Uhrzeit der ersten Geschwindigkeitsüberschreitung und Anzahl der weiteren Geschwindigkeitsüberschreitungen seitdem	`»»TT/MM/JJJJ hh:mm (nnn)`

21	***Datensatz Geschwindigkeitsüberschreitung***	
21.1	Blockbezeichner „Erste Geschwindigkeitsüberschreitung seit der letzten Kalibrierung“	`--------»»⍑---------`
21.2	Blockbezeichner „5 schwerste Geschwindigkeitsüberschreitungen in den letzten 365 Tagen“	`-------»»(365)------`
21.3	Blockbezeichner „Schwerste GÜ der letzten 10 Tage mit derartigen Ereignissen“	`-------»»(10)-------`
21.4	Datensatzbezeichner	`--------------------`
	Datum, Uhrzeit und Dauer	`»»TT/MM/JJJJ hh:mm hhhmm`
	Höchst- und Durchschnittsgeschwindigkeit, Anzahl ähnlicher Ereignisse an diesem Tag	`xxx km/h xxx km/h(xxx)`
	Name des Fahrers	`◙ Name_____`
	Vorname(n) des Fahrers	`Vorname_____`
	Fahrerkartenkennung	`Kartenkennung_____`
21.5	Falls in einem Block kein Datensatz für GÜ existiert	`»»---`

22	***Handschriftliche Angaben***	
	Blockbezeichner	`------------------------`
22.1	Ort der Kontrolle	`◘• ..................`
22.2	Unterschrift des Kontrolleurs	`◘ ..................`
22.3	Anfangszeit	`◷+ ..................`
22.4	Endzeit	`+◷ ..................`
22.5	Unterschrift des Fahrers	`◙ ..................`

„Handschriftliche Angaben“: Es sind so viele Leerzeilen über einem handschriftlichen Eintrag einzufügen, dass der Platz für die erforderlichen Angaben oder eine Unterschrift ausreicht.

23 ***Zuletzt in VU eingesteckte Karten***
Blockbezeichner
23.1 Eingesteckte Karte
Datensatzbezeichner
Art der Karte, Generation, Version, Hersteller (*)
Kartenkennung
Seriennummer der Karte
Datum und Uhrzeit des letzten Einsteckens der Karten

```
-------- ⊟■⊙ --------

----
⍑ <Gen> <Version> <HC>
Kartenkennung
Seriennummer der Karte
TT/MM/JJJJ hh:mm
```

(*) (alles in einer Zeile)
wobei Folgendes gilt:
Art der Karte: Piktogramm, ein Zeichen + Leerzeichen
Gen: GEN1 oder GEN2, 4 Zeichen + Leerzeichen
Version: bis zu 10 Zeichen
HC: Herstellercode, 3 Zeichen

3. SPEZIFIKATION DER AUSDRUCKE

In diesem Kapitel werden die folgenden Konventionen für die Notation verwendet:

N	Nummer N des Druckblocks oder -datensatzes
N	Nummer N des Druckblocks oder -datensatzes, Wiederholung so oft wie nötig
X/Y	Druckblöcke oder Datensätze X und/oder Y nach Bedarf, Wiederholung so oft wie nötig

3.1. **Tagesausdruck Fahrertätigkeiten von der Karte**

PRT_008 Der Tagesausdruck der Fahrertätigkeiten von der Karte hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Kontrolleur (bei in VU eingesteckter Kontrollkarte)
3	Angaben zum Fahrer (von der Karte, auf die sich Ausdruck bezieht + GEN)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
5	VU-Kennung (VU, mit der Ausdruck erstellt wird)
6	Letzte Kalibrierung dieser VU
7	Letzte Kontrolle des hier kontrollierten Fahrers
8	Begrenzungszeichen Fahrertätigkeiten
8a	Bedingung „Kontrollgerät nicht erforderlich“ zu Tagesbeginn
8.1a/8.1b/8.1c/ 8.2/8.3/8.3a/8.4	Fahrertätigkeiten in der Reihenfolge ihres Auftretens
11	Begrenzungszeichen Tageszusammenfassung

11.4	Eingegebene Orte in chronologischer Reihenfolge
11.5	GNSS-Daten
11.6	Gesamtwerte Tätigkeiten
12.1	Begrenzungszeichen Ereignisse und Störungen von der Karte
12.4	Datensätze Ereignis/Störung (die letzten 5 auf der Karte gespeicherten Ereignisse/Störungen)
13.1	Begrenzungszeichen Ereignisse oder Störungen von der VU
13.4	Datensätze Ereignis/Störung (die letzten 5 in der VU gespeicherten oder andauernden Ereignisse/Störungen)
22.1	Ort der Kontrolle
22.2	Unterschrift des Kontrolleurs
22.5	Unterschrift des Fahrers

3.2. **Tagesausdruck Fahrertätigkeiten von der Fahrzeugeinheit (VU)**

PRT_009 Der Tagesausdruck der Fahrertätigkeiten von der VU hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die VU eingesteckten Karten + GEN)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
5	VU-Kennung (VU, mit der Ausdruck erstellt wird)
6	Letzte Kalibrierung dieser VU
7	Letzte Kontrolle auf diesem Fahrtenschreiber
9	Begrenzungszeichen Fahrertätigkeiten
10	Begrenzungszeichen Steckplatz Fahrer (Steckplatz 1)
10a	Bedingung „Kontrollgerät nicht erforderlich“ zu Tagesbeginn
10.1/10.2/10.3 /10.3a/ 10.4	Tätigkeiten in chronologischer Reihenfolge (Steckplatz Fahrer)
10	Begrenzungszeichen Steckplatz 2. Fahrer (Steckplatz 2)
10a	Bedingung „Kontrollgerät nicht erforderlich“ zu Tagesbeginn
10.1/10.2/10.3 /10.3a/ 10.4	Tätigkeiten in chronologischer Reihenfolge (Steckplatz Beifahrer)
11	Begrenzungszeichen Tageszusammenfassung
11.1	Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Fahrer
11.4	Eingegebene Orte in chronologischer Reihenfolge
11.5	GNSS-Daten
11.6	Gesamtwerte Tätigkeiten
11.2	Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Beifahrer
11.4	Eingegebene Orte in chronologischer Reihenfolge
11.5	GNSS-Daten

11.7	Gesamtwerte Tätigkeiten
11.3	Zusammenfassung der Tätigkeiten für einen Fahrer, beide Steckplätze
11.4	Von diesem Fahrer eingegebene Orte in chronologischer Reihenfolge
11.5	GNSS-Daten
11.8	Gesamtwerte Tätigkeiten für diesen Fahrer
13.1	Begrenzungszeichen Ereignisse/Störungen
12.4	Datensätze Ereignis/Störung (die letzten 5 in der VU gespeicherten oder andauernden Ereignisse/Störungen)
13.1	Ort der Kontrolle
22.2	Unterschrift des Kontrolleurs
22.3	Anfangszeit (Raum, in dem ein Fahrer ohne Karte die für ihn zutreffenden Zeitabschnitte angeben kann) (welche Zeitabschnitte für ihn relevant sind)
22.4	Endzeit
22.5	Unterschrift des Fahrers

3.3. **Ausdruck Ereignisse und Störungen von der Karte**

PRT_010 Der Ausdruck Ereignisse und Störungen von der Karte hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Kontrolleur (bei in VU eingesteckter Kontrollkarte + GEN)
3	Angaben zum Fahrer (von der Karte, auf die der Ausdruck sich bezieht)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
12.2	Begrenzungszeichen Ereignisse
12.4	Ereignisdatensätze (alle auf der Karte gespeicherten Ereignisse)
12.3	Begrenzungszeichen Störungen
12.4	Störungsdatensätze (alle auf der Karte gespeicherten Ereignisse)
22.1	Ort der Kontrolle
22.2	Unterschrift des Kontrolleurs
22.5	Unterschrift des Fahrers

3.4. **Ausdruck Ereignisse und Störungen von der VU**

PRT_011 Der Ausdruck Ereignisse und Störungen von der VU hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die VU eingesteckten Karten + GEN)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)

13.2	Begrenzungszeichen Ereignisse
13.4	Ereignisdatensätze (alle in der VU gespeicherten oder andauernden Ereignisse)
13.3	Begrenzungszeichen Störungen
13.4	Störungsdatensätze (alle in der VU gespeicherten oder andauernden Störungen)
22.1	Ort der Kontrolle
22.2	Unterschrift des Kontrolleurs
22.5	Unterschrift des Fahrers

3.5. **Ausdruck Technische Daten**

PRT_012 Der Ausdruck Technische Daten hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die VU eingesteckten Karten + GEN)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
14	VU-Kennung
15	Sensorkennung
15.1	Sensorkopplungsdaten (alle verfügbaren Daten in chronologischer Reihenfolge)
16	GNSS-Kennnummer
16.1	Kopplungsdaten der externen GNSS-Ausrüstung (alle verfügbaren Daten in chronologischer Reihenfolge)
17	Begrenzungszeichen Kalibrierungsdaten
17.1	Kalibrierungsdatensätze (alle verfügbaren Datensätze in chronologischer Reihenfolge)
18	Begrenzungszeichen Zeiteinstellung
18.1	Datensätze Zeiteinstellung (alle verfügbaren Datensätze für Zeiteinstellung und Kalibrierung)
19	Jüngste(s) in der VU aufgezeichnete(s) Ereignis und Störung

3.6. **Ausdruck Geschwindigkeitsüberschreitung**

PRT_013 Der Ausdruck Geschwindigkeitsüberschreitung hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die VU eingesteckten Karten + GEN)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
20	Angaben zur Kontrolle Geschwindigkeitsüberschreitung
21.1	Kennung Daten Geschwindigkeitsüberschreitung
21.4/21.5	Erste Geschwindigkeitsüberschreitung nach der letzten Kalibrierung

21.2	Kennung Daten Geschwindigkeitsüberschreitung
21.4/21.5	Die 5 schwersten GÜ in den letzten 365 Tagen
21.3	Kennung Daten Geschwindigkeitsüberschreitung
21.4/21.5	Die schwersten GÜ der letzten 10 Tage mit derartigen Ereignissen
22.1	Ort der Kontrolle
22.2	Unterschrift des Kontrolleurs
22.5	Unterschrift des Fahrers

3.7. **Historie der eingesteckten Karten**

PRT_014 Der Ausdruck Historie der eingesteckten Karten hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Karteninhaberkennungen (sämtlicher in die VU eingesteckten Karten)
23	Zuletzt in VU eingesteckte Karte
23.1	Eingesteckte Karten (bis zu 88 Einträge)
12.3	Begrenzungszeichen Störungen

Anlage 5

ANZEIGE

In dieser Anlage werden folgende Konventionen für die Notation verwendet:

— Zeichen in **Fettdruck** stehen für anzuzeigenden Klartext (in der Anzeige erscheinen die Zeichen unformatiert).

— Unformatierte Zeichen stehen für Variablen (Piktogramme oder Daten), die in der Anzeige durch ihre Werte ersetzt werden:

  — TT MM JJJJ: Tag, Monat, Jahr,

  — hh: Stunden,

  — mm: Minuten,

  — D: Piktogramm Dauer,

  — EF: Piktogrammkombination Ereignis oder Störung,

  — O: Piktogramm Betriebsart.

DIS_001 Die Anzeige von Daten durch den Fahrtenschreiber erfolgt in folgendem Format:

Daten	Format
Standardanzeige	
Ortszeit	hh:mm
Betriebsart	O
Informationen zum Fahrer	1 Dhh**h**mm ‖hh**h**mm
Information zum Beifahrer	2Dhh**h**mm
Betriebsart „Kontrollgerät nicht erforderlich“ eingeschaltet	OUT
Warnanzeige	
Überschreitung der ununterbrochenen Lenkzeit	1☹hh**h**mm ‖hh**h**mm
Ereignis oder Störung	EF
Sonstige Anzeigen	
UTC-Datum Uhrzeit	UTC☻dd/mm/yyyy oder UTC☻dd.mm.yyyy hh:mm
Ununterbrochene Lenkzeit und kumulative Pausenzeit des Fahrers	1☹hh**h**mm ‖hh**h**mm
Ununterbrochene Lenkzeit und kumulative Pausenzeit des Beifahrers	2☹hh**h**mm ‖hh**h**mm
Kumulierte Lenkzeit des Fahrers für die Vorwoche und die laufende Woche	1☹‖ hhh**h**mm
Kumulierte Lenkzeit des Beifahrers für die Vorwoche und die laufende Woche	2☹‖ hhh**h**mm

Anlage 6

STECKANSCHLUSS AN DER VORDERSEITE FÜR KALIBRIERUNG UND HERUNTERLADEN

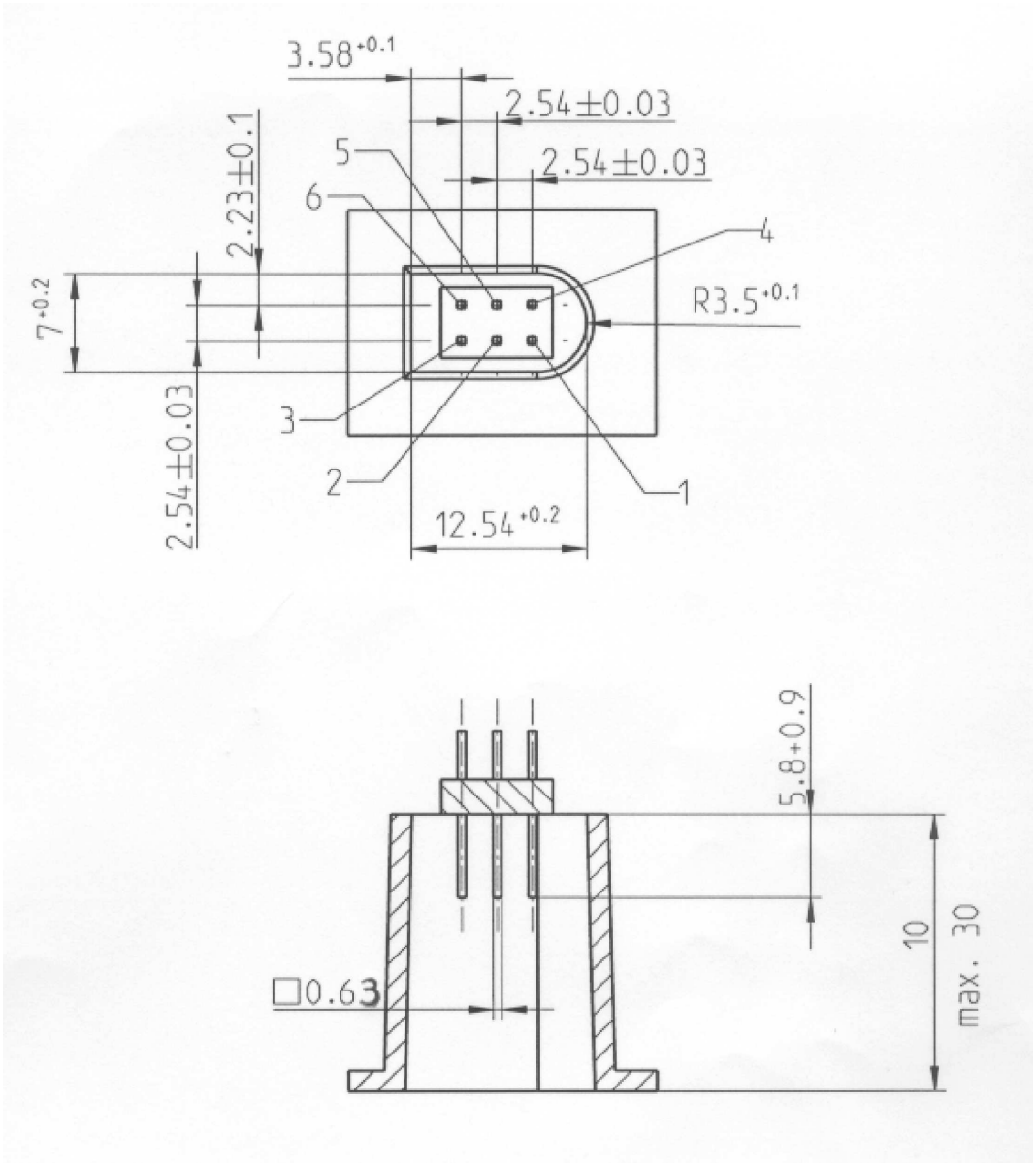
INHALTSVERZEICHNIS

1. HARDWARE 256
1.1. Steckanschluss 256
1.2. Belegung der Kontakte 257
1.3. Blockschaltbild 258
2. SCHNITTSTELLE ZUM HERUNTERLADEN 258
3. KALIBRIERUNGSSCHNITTSTELLE 259

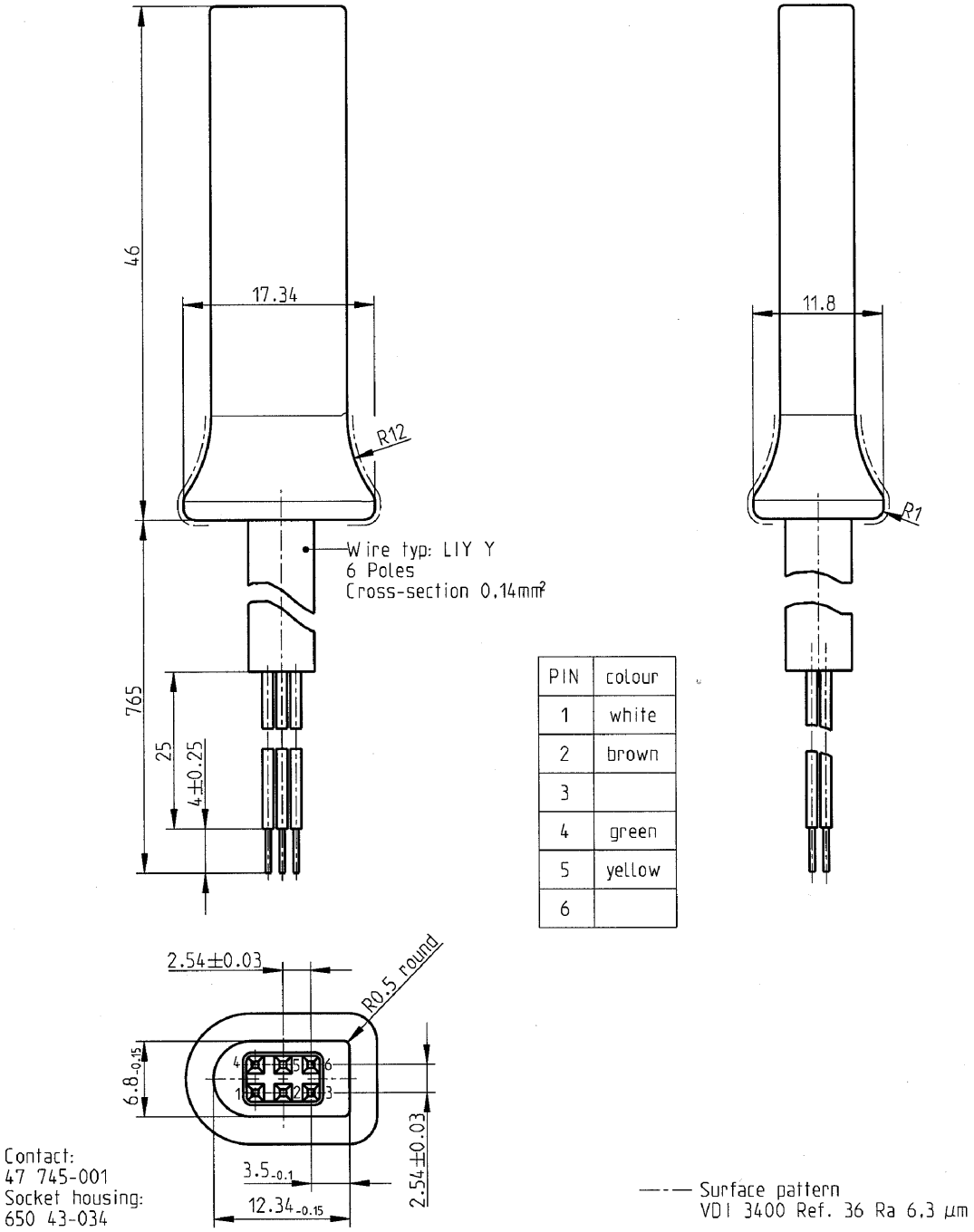
1. HARDWARE

1.1. **Steckanschluss**

INT_001 Das Herunterladen/Kalibrieren erfolgt über eine sechspolige Steckverbindung, die an der Frontplatte zugänglich ist, ohne dass ein Teil des Fahrtenschreibers abgetrennt werden muss. Sie ist entsprechend der folgenden Abbildung auszulegen (sämtliche Maßangaben in mm):



Die folgende Abbildung zeigt einen typischen sechspoligen Stecker:



1.2. **Belegung der Kontakte**

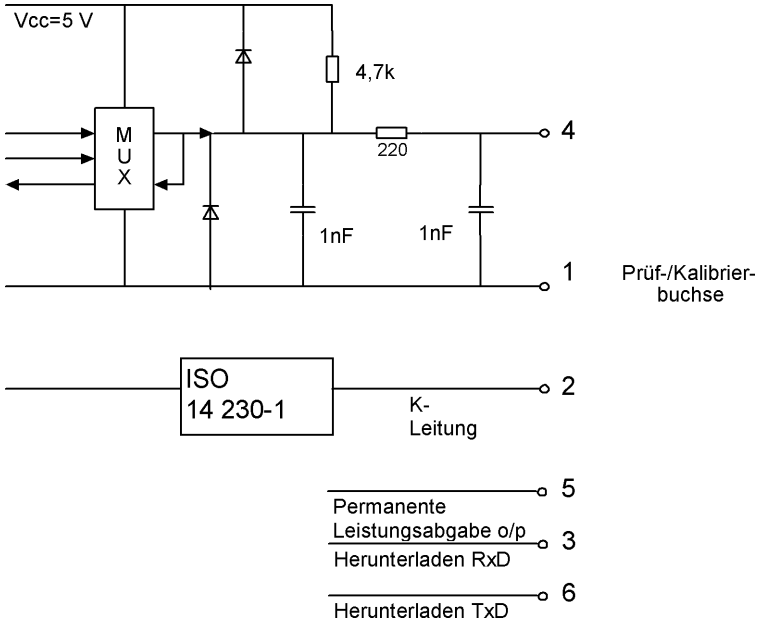
INT_002 Die Kontakte sind entsprechend der nachstehenden Tabelle zu belegen:

Stift	Beschreibung	Anmerkung
1	Batterie minus	Zum Minuspol der Fahrzeugbatterie
2	Datenkommunikation	K-Leitung (ISO 14230-1)

Stift	Beschreibung	Anmerkung
3	RxD — Herunterladen	Dateneingang Fahrtenschreiber
4	Eingabe-/Ausgabesignal	Kalibrierung
5	Dauerausgangsleistung	Zur Berücksichtigung des Spannungsabfalls am Schutzstromkreis entspricht der Spannungsbereich dem des Fahrzeugs minus 3 V Ausgangsleistung: 40 mA
6	TxD — Herunterladen	Datenausgang Fahrtenschreiber

1.3. **Blockschaltbild**

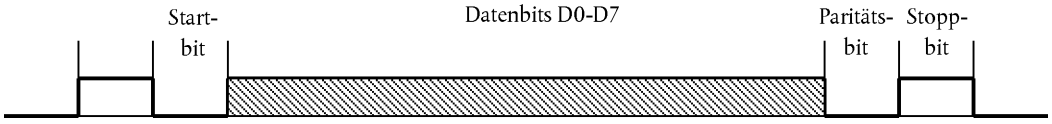
INT_003 Folgendes Blockschaltbild ist vorgegeben:



2. SCHNITTSTELLE ZUM HERUNTERLADEN

INT_004 Die Schnittstelle zum Herunterladen entspricht den RS232-Spezifikationen.

INT_005 Die Schnittstelle zum Herunterladen verwendet ein Startbit, 8 Datenbits mit dem niedrigstwertigen Bit an erster Stelle, ein Bit geradzahliger Parität und 1 Stoppbit.



Aufbau der Datenbytes

Startbit: Ein Bit mit dem Logikpegel 0

Datenbits: An erster Stelle Übertragung des niedrigstwertigen Bits

Paritätsbit: Gerade Parität

Stoppbit: Ein Bit mit dem Logikpegel 1

Bei der Übermittlung nummerischer Daten, die aus mehr als einem Byte bestehen, wird das höchstwertige Byte an erster Stelle und das niedrigstwertige Byte an letzter Stelle übertragen.

INT_006 Die Baudrate bei der Übertragung ist zwischen 9 600 und 115 200 bit/s einstellbar. Die Übertragung hat mit der höchstmöglichen Übertragungsgeschwindigkeit zu erfolgen, wobei die anfängliche Bitgeschwindigkeit nach dem Aufbau der Verbindung auf 9 600 bit/s gesetzt wird.

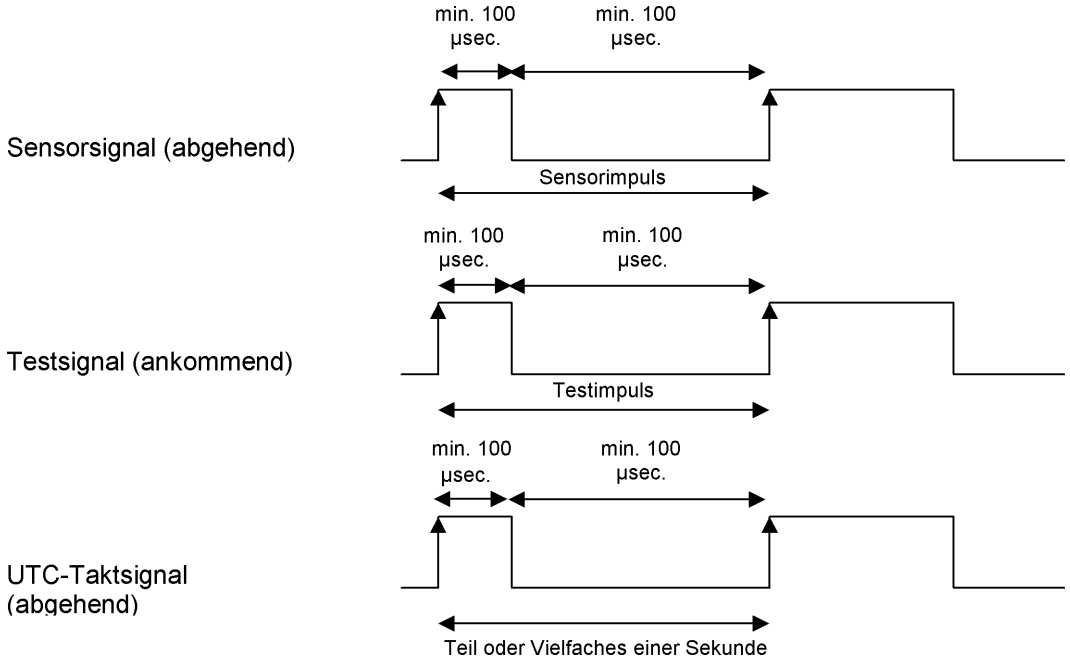
3. KALIBRIERUNGSSCHNITTSTELLE

INT_007 Die Datenkommunikation erfolgt nach ISO 14230-1 Straßenfahrzeuge — Diagnosesysteme — Schlüsselwort 2000 — Teil 1: Bitübertragungsschicht, Erste Ausgabe: 1999.

INT_008 Das Eingabe-/Ausgabesignal entspricht den folgenden elektrischen Spezifikationen:

Parameter	Minimum	Typisch	Maximum	Anmerkung
$U_{L\text{-Pegel}}$ (Eingang)			1,0 V	I = 750 µA
$U_{H\text{-Pegel}}$ (Eingang)	4 V			I = 200 µA
Frequenz			4 kHz	
$U_{L\text{-Pegel}}$ (Ausgang)			1,0 V	I = 1 mA
$U_{H\text{-Pegel}}$ (Ausgang)	4 V			I = 1 mA

INT_009 Für das Eingabe-/Ausgabesignal gelten die folgenden Zeitdiagramme:



Anlage 7

PROTOKOLLE ZUM HERUNTERLADEN DER DATEN

INHALTSVERZEICHNIS

1. EINLEITUNG 261
1.1. Geltungsbereich 261
1.2. Akronyme und Notationen 261
2. HERUNTERLADEN VON DATEN VON DER FAHRZEUGEINHEIT 262
2.1. Download-Verfahren 262
2.2. Datendownload-Protokoll 262
2.2.1 Nachrichtenstruktur 262
2.2.2 Nachrichtentypen 264
2.2.2.1 Start Communication Request (SID 81) 266
2.2.2.2 Positive Response Start Communication (SID C1) 266
2.2.2.3 Start Diagnostic Session Request (SID 10) 266
2.2.2.4 Positive Response Start Diagnostic (SID 50) 266
2.2.2.5 Link Control Service (SID 87) 266
2.2.2.6 Link Control Positive Response (SID C7) 266
2.2.2.7 Request Upload (SID 35) 266
2.2.2.8 Positive Response Request Upload (SID 75) 266
2.2.2.9 Transfer Data Request (SID 36) 266
2.2.2.10 Positive Response Transfer Data (SID 76) 267
2.2.2.11 Request Transfer Exit (SID 37) 267
2.2.2.12 Positive Response Request Transfer Exit (SID 77) 267
2.2.2.13 Stop Communication Request (SID 82) 267
2.2.2.14 Positive Response Stop Communication (SID C2) 267
2.2.2.15 Acknowledge Sub Message (SID 83) 267
2.2.2.16 Negative Response (SID 7F) 268
2.2.3 Nachrichtenfluss 268
2.2.4 Timing 269
2.2.5 Fehlerbehandlung 270
2.2.5.1 Start Communication-Phase 270
2.2.5.2 Communication-Phase 270
2.2.6 Inhalt der Antwortnachricht 272
2.2.6.1 Positive Response Transfer Data Overview 273
2.2.6.2 Positive Response Transfer Data Activities 274
2.2.6.3 Positive Response Transfer Data Events and Faults 275
2.2.6.4 Positive Response Transfer Data Detailed Speed 276
2.2.6.5 Positive Response Transfer Data Technical Data 276
2.3. ESM-Datenspeicherung 277

3. PROTOKOLL FÜR DAS HERUNTERLADEN VON DATEN VON FAHRTENSCHREIBERKARTEN 277
3.1. Geltungsbereich 277
3.2. Begriffsbestimmungen 277
3.3. Herunterladen von der Karte 277
3.3.1 Initialisierungssequenz 278
3.3.2 Sequenz für unsignierte Dateien 278
3.3.3 Sequenz für signierte Dateien 279
3.3.4 Sequenz für das Zurücksetzen des Kalibrierungszählers 279
3.4. Datenspeicherungsformat 280
3.4.1 Einleitung 280
3.4.2 Dateiformat 280
4. HERUNTERLADEN VON DER FAHRTENSCHREIBERKARTE ÜBER EINE FAHRZEUGEINHEIT 281

1. EINLEITUNG

Diese Anlage enthält die Spezifizierung der Verfahren für die verschiedenen Arten der Übertragung der Daten von der Karte auf ein externes Speichermedium (ESM) sowie die Protokolle, die zur Sicherung der korrekten Datenübertragung und der vollständigen Kompatibilität des heruntergeladenen Datenformats zu implementieren sind, damit ein Kontrolleur diese Daten inspizieren und vor ihrer Analyse ihre Echtheit und Integrität kontrollieren kann.

1.1. **Geltungsbereich**

Das Herunterladen von Daten auf ein ESM kann erfolgen:

— von einer Fahrzeugeinheit (Vehicle Unit, VU) durch ein an die VU angeschlossenes Intelligent Dedicated Equipment (IDE),

— von einer Fahrtenschreiberkarte durch ein mit einem Kartenschnittstellengerät (IFD) ausgestattetes IDE,

— von einer Fahrtenschreiberkarte über eine Fahrzeugeinheit durch ein an die VU angeschlossenes IDE.

Um eine Prüfung der Echtheit und Integrität der auf einem ESM gespeicherten heruntergeladenen Daten zu ermöglichen, werden die Daten mit einer gemäß Anlage 11 (Gemeinsame Sicherheitsmechanismen) angefügten Signatur heruntergeladen. Ebenfalls heruntergeladen werden die Kennung des Ursprungsgeräts (VU oder Karte) und dessen Sicherheitszertifikate (Mitgliedstaatszertifikat und Gerätezertifikat). Der Prüfer der Daten muss einen zuverlässigen europäischen öffentlichen Schlüssel besitzen.

DDP_001 Die während eines Download-Vorgangs heruntergeladenen Daten müssen auf dem ESM in einer einzigen Datei gespeichert werden.

1.2. **Akronyme und Notationen**

In dieser Anlage werden folgende Akronyme verwendet:

AID Application Identifier (Anwendungskennung)

ATR Answer To Reset (Antwort auf Zurücksetzen)

CS Checksum Byte (Prüfsummenbyte)

DF Dedicated File (Verzeichnis)

DS_ Diagnostic Session (Diagnosevorgang)

EF Elementary File (Elementardatei)

ESM External Storage Medium (externes Speichermedium)

FID File Identifier (File ID, Dateikennung)

FMT Formatbyte (erstes Byte eines Nachrichtenkopfes)

ICC Integrated Circuit Card (Chipkarte)

IDE Intelligent Dedicated Equipment: Gerät, das zum Herunterladen von Daten auf das ESM verwendet wird (z. B. Personalcomputer)

IFD Interface Device (Schnittstellengerät, Kartenterminal)

KWP Keyword Protocol 2000

LEN Length Byte (Längenbyte, letztes Byte eines Nachrichtenkopfes)

PPS Protocol Parameter Selection (Auswahl der Protokollparameter)

PSO Perform Security Operation (Sicherheitsoperation ausführen)

SID Service Identifier (Dienstkennung)

SRC Source Byte (Quellbyte)

TGT Target Byte (Zielbyte)

TLV Tag Length Value (Taglängenwert)

TREP Transfer Response Parameter (Antwortübertragungsparameter)

TRTP Transfer Request Parameter (Anfrageübertragungsparameter)

VU Fahrzeugeinheit (Vehicle Unit)

2. HERUNTERLADEN VON DATEN VON DER FAHRZEUGEINHEIT

2.1. **Download-Verfahren**

Zur Durchführung eines VU-Datendownloads muss der Bediener folgende Arbeitsschritte ausführen:

— Einführen seiner Kontrollgerätkarte in einen Steckplatz der VU (*);

— Anschließen des IDE an den VU-Anschluss zum Herunterladen;

— Herstellen der Verbindung zwischen IDE und VU;

— Auswählen der herunterzuladenden Daten auf dem IDE und Senden der Anforderung an die VU;

— Beenden des Download-Vorgangs.

2.2. **Datendownload-Protokoll**

Das Protokoll ist auf Master/Slave-Basis aufgebaut, wobei das IDE den Master und die VU den Slave bildet.

Nachrichtenstruktur, -typ und -fluss beruhen prinzipiell auf dem Keyword Protocol 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part2: Data link layer). (Straßenfahrzeuge — Diagnosesysteme — Schlüsselwort 2000 — Teil 2: Sicherungsschicht).

Die Anwendungsschicht beruht grundsätzlich auf dem aktuellen Normentwurf ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services (Straßenfahrzeuge — Diagnosesysteme — Teil 1: Diagnosedienste), Version 6 vom 22. Februar 2001).

2.2.1 *Nachrichtenstruktur*

DDP_002 Alle zwischen dem IDE und der VU ausgetauschten Nachrichten sind mit einer dreiteiligen Struktur formatiert, die sich zusammensetzt aus

— dem Kopf, bestehend aus einem Formatbyte (FMT), einem Zielbyte (TGT), einem Quellbyte (SRC) und möglicherweise einem Längenbyte (LEN),

— dem Datenfeld, bestehend aus einem Service-Identifier-Byte (SID) und einer variablen Anzahl von Datenbytes, z. B. ein optionales Diagnostic-Session-Byte (DS_) oder ein optionales Transfer-Parameter-Byte (TRTP oder TREP),

— der Prüfsumme, bestehend aus einem Prüfsummenbyte (CS).

Kopf				Datenfeld					Prüfsumme
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 Bytes				Max. 255 Bytes					1 Byte

(*) Die eingesetzte Karte löst die erforderlichen Zugriffsrechte für die Herunterladefunktion und die Daten aus. Das Herunterladen von Daten von einer in einen der Steckplätze der VU eingeführten Fahrerkarte ist auch möglich, wenn in den anderen Steckplatz kein anderer Kartentyp eingeführt ist.

TGT- und SRC-Byte stellen die physische Adresse des Empfängers und des Absenders der Nachricht dar. Die Werte sind F0 Hex für das IDE und EE Hex für die VU.

Das LEN-Byte ist die Länge des Datenfeldteils.

Das Prüfsummenbyte ist die 8-Bit-Summenreihe modulo 256 aller Bytes der Nachricht außer CS selbst.

Die Bytes FMT, SID, DS_, TRTP und TREP werden an anderer Stelle dieses Dokuments definiert.

DDP_003 Sind die von der Nachricht aufzunehmenden Daten länger als der im Datenfeldteil zur Verfügung stehende Platz, wird die Nachricht in mehreren Teilnachrichten gesendet. Jede Teilnachricht hat einen Kopf, die gleiche SID, TREP sowie einen 2-Byte-Teilnachrichtenzähler, der die Teilnachrichtnummer innerhalb der Gesamtnachricht angibt. Damit Fehlerprüfung und Abbruch möglich sind, bestätigt das IDE jede Teilnachricht. Das IDE kann die Teilnachricht annehmen, ihre erneute Übertragung anfordern sowie die VU zum Neubeginn oder zum Abbruch der Übertragung auffordern.

DDP_004 Enthält die letzte Teilnachricht genau 255 Bytes im Datenfeld, muss eine abschließende Teilnachricht mit leerem Datenfeld (außer SID, TREP und Teilnachrichtenzähler) angefügt werden, die das Ende der Nachricht anzeigt.

Beispiel:

Kopf	SID	TREP	Nachricht	CS
4 Bytes	Länger als 255 Bytes			

wird übertragen als:

Kopf	SID	TREP	00	01	Teilnachricht 1	CS
4 Bytes	255 Bytes					

Kopf	SID	TREP	00	02	Teilnachricht 2	CS
4 Bytes	255 Bytes					

…

Kopf	SID	TREP	xx	yy	Teilnach-richt n	CS
4 Bytes	Weniger als 255 Bytes					

oder als:

Kopf	SID	TREP	00	01	Teilnachricht 1	CS
4 Bytes	255 Bytes					

Kopf	SID	TREP	00	02	Teilnachricht 2	CS
4 Bytes	255 Bytes					

…

Kopf	SID	TREP	xx	yy	Teilnachricht n	CS
4 Bytes	255 Bytes					

Kopf	SID	TREP	xx	yy + 1	CS
4 Bytes	4 Bytes				

2.2.2 *Nachrichtentypen*

Das Kommunikationsprotokoll für das Herunterladen von Daten zwischen der VU und dem IDE verlangt den Austausch von 8 verschiedenen Nachrichtentypen.

In der folgenden Tabelle sind diese Nachrichten zusammengefasst.

Nachrichtenstruktur	Max. 4 Bytes Kopf				Max. 255 Bytes Daten			1 Byte Prüfsumme
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Baud	80	EE	F0	04	87		01,01, 01	EC
19 200 Baud	80	EE	F0	04	87		01,01, 02	ED
38 400 Baud	80	EE	F0	04	87		01,01, 03	EE
57 600 Baud	80	EE	F0	04	87		01,01, 04	EF
115 200 Baud	80	EE	F0	04	87		01,01, 05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5

Nachrichtenstruktur	Max. 4 Bytes Kopf				Max. 255 Bytes Daten			1 Byte Prüf-summe
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Daten	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Daten	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Anmerkungen:

— Sid Req = Sid der entsprechenden Anforderung.

— TREP = der TRTP der entsprechenden Anforderung.

— Geschwärzte Felder zeigen an, dass nichts übertragen wird.

— Der Ausdruck „Upload“ (vom IDE aus gesehen) wird in Anlehnung an die ISO 14229 verwendet. Er bedeutet dasselbe wie „Download“ (von der VU aus gesehen).

— Mögliche 2-Byte-Teilnachrichtenzähler sind in dieser Tabelle nicht aufgeführt.

— „Slot“ bezeichnet die Steckplatznummer, entweder „1“ (Karte im Steckplatz Fahrer) oder „2“ (Karte im Steckplatz 2. Fahrer)

— Falls der Steckplatz nicht angegeben ist, muss die VU Steckplatz 1 auswählen, wenn in diesen Steckplatz eine Karte eingesteckt wird, und Steckplatz 2 nur dann, wenn dies vom Benutzer ausdrücklich ausgewählt wird.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Diese Nachricht wird vom IDE zum Aufbau der Kommunikationsverbindung mit der VU ausgegeben. Der Verbindungsaufbau und die Kommunikation erfolgt anfangs stets mit einer Datenrate von 9 600 Baud (solange die Übertragungsgeschwindigkeit nicht durch einen Link Control Service (Verbindungssteuerungsdienst) geändert wird).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Diese Nachricht wird von der VU als positive Antwort auf einen Start Communication Request ausgegeben. Sie enthält die beiden Schlüsselbytes „EA“ „8F“ als Hinweis darauf, dass die Einheit das Protokoll mit Kopf einschließlich Ziel-, Quell- und Längeninformation unterstützt.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 Die Nachricht Start Diagnostic Session Request wird vom IDE ausgegeben, um einen neuen Diagnosevorgang mit der VU zu beginnen. Die Untervariable „default session“ (81 Hex) zeigt an, dass ein Standard-Diagnosevorgang eingeleitet werden soll.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Die Nachricht Positive Response Start Diagnostic wird von der VU als positive Antwort auf einen Diagnostic Session Request gesendet.

2.2.2.5 Link Control Service (SID 87)

DDP_052 Mit Hilfe des Link Control Service (Verbindungssteuerungsdienst) leitet die IDE einen Wechsel der Übertragungsgeschwindigkeit (Baudrate) ein. Dies erfolgt in zwei Schritten. Zunächst schlägt die IDE einen Wechsel vor und gibt dazu die neue Baudrate an. Nach einer positiven Antwort der VU sendet die IDE dann im zweiten Schritt eine Bestätigung des Geschwindigkeitswechsels an die VU und geht danach zur neuen Baudrate über. Nach Erhalt der Bestätigung geht auch die VU zur neuen Baudrate über.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Die Nachricht Link Control Positive Response wird von der VU als positive Antwort auf einen Link Control Service Request (Schritt 1) gesendet. Die Bestätigungsmeldung (Schritt 2) wird dagegen nicht beantwortet.

2.2.2.7 Request Upload (SID 35)

DDP_009 Die Nachricht Request Upload wird vom IDE als Mitteilung an die VU ausgegeben, dass eine Download-Operation angefordert wird. In Übereinstimmung mit der ISO 14229 umfasst diese Anforderung stets Angaben zu Adresse, Größe und Format der angeforderten Daten. Da diese Angaben der IDE jedoch vor dem Herunterladen nicht bekannt sind, wird die Speicheradresse auf „0“, das Format auf „verschlüsselt und unkomprimiert“ und die Speichergröße auf den Höchstwert gesetzt.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Die Nachricht Positive Response Request Upload wird von der VU gesendet, um dem IDE anzuzeigen, dass die VU zum Herunterladen der Daten bereit ist. In Übereinstimmung mit der ISO 14229 enthält diese Positive-Response-Nachricht auch Daten, mit denen der IDE mitgeteilt wird, dass spätere Nachrichten Positive Response Transfer Data höchstens 00FF Hex Bytes umfassen werden.

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 Die Nachricht Transfer Data Request wird vom IDE gesendet und spezifiziert der VU den herunterzuladenden Datentyp. Mit dem Byte Transfer Request Parameter (TRTP) wird die Übertragungsart angegeben.

Es gibt sechs Arten der Datenübertragung:

— Überblick (TRTP 01),

— Tätigkeiten eines bestimmten Tages (TRTP 02),

— Ereignisse und Störungen (TRTP 03),

— Genaue Geschwindigkeitsangaben (TRTP 04),

— Technische Daten (TRTP 05),

— Kartendownload (TRTP 06).

DDP_054 Die IDE muss beim Herunterladen eine Überblicks-Datenübertragung (TRTP 01) anfordern, da nur so die VU-Zertifikate in der heruntergeladenen Datei gespeichert werden (und die digitale Signatur geprüft werden kann).

Im zweiten Fall (TRTP 02) schließt die Nachricht Transfer Data Request die Angabe des herunterzuladenden Kalendertags (Format `TimeReal`) ein.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Die Nachricht Positive Response Transfer Data wird von der VU als Antwort auf die Transfer Data Request gesendet. Sie enthält die angeforderten Daten, wobei die Transfer Response Parameter (TREP) der TRTP der Anforderung entspricht.

DDP055 Im ersten Fall (TREP 01), sendet die VU Daten, die es dem IDE-Bediener erleichtern, die von ihm herunterzuladenden Daten auszuwählen. Diese Nachricht enthält folgende Informationen:

— Sicherheitszertifikate,

— Fahrzeugkennung,

— aktuelles Datum und Uhrzeit der VU,

— min. und max. herunterladbares Datum (VU-Daten),

— Angabe der in die VU eingesteckten Karten,

— der vorherige Download an ein Unternehmen,

— Unternehmenssperren,

— bisherige Kontrollen.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 Mit der Nachricht Request Transfer Exit teilt das IDE der VU mit, dass der Download-Vorgang beendet ist.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Die Nachricht Positive Response Request Transfer Exit wird von der VU zur Quittierung der Request Transfer Exit gesendet.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Die Nachricht Stop Communication Request wird vom IDE gesendet, um die Kommunikationsverbindung mit der VU zu trennen.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Mit der Nachricht Positive Response Stop Communication quittiert die VU die Nachricht Stop Communication Request.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Mit der Nachricht Acknowledge Sub Message bestätigt das IDE den Empfang der einzelnen Teile einer Nachricht, die in mehreren Teilnachrichten gesendet wird. Das Datenfeld enthält die von der VU empfangene SID sowie einen 2-Byte-Code wie folgt:

— MsgC + 1 quittiert den korrekten Empfang der Teilnachricht Nummer MsgC.

Anforderung vom IDE an die VU zur Sendung der nächsten Teilnachricht.

— MsgC zeigt ein Problem beim Empfang der Teilnachricht Nummer MsgC an.

Anforderung von IDE an die VU zur erneuten Sendung der Teilnachricht.

— FFFF fordert zur Beendigung der Nachricht auf.

Kann vom IDE zur Beendigung der Übertragung der VU-Nachricht aus irgendeinem Grund verwendet werden.

Die letzte Teilnachricht einer Nachricht (LEN-Byte < 255) kann unter Verwendung eines dieser Codes oder gar nicht quittiert werden.

Folgende VU-Antwort besteht aus mehreren Teilnachrichten:

— Positive Response Transfer Data (SID 76)

2.2.2.16 Negative Response (SID 7F)

DDP_018 Die Nachricht Negative Response wird von der VU als Antwort auf die oben genannten Anforderungsnachrichten gesendet, wenn sie die Anforderung nicht erfüllen kann. Die Datenfelder der Nachricht enthalten die SID der Antwort (7F), die SID der Anforderung sowie einen Code zur Angabe des Grundes der negativen Antwort. Folgende Codes stehen zur Verfügung:

— 10 general reject

Aktion kann aus einem im Folgenden nicht aufgeführten Grund nicht ausgeführt werden.

— 11 service not supported

Die SID der Anforderung wird nicht verstanden.

— 12 sub function not supported

Die DS_ oder TRTP der Anforderung wird nicht verstanden, oder es sind keine weiteren Teilnachrichten zu übertragen.

— 13 incorrect message length

Die Länge der erhaltenen Nachricht ist nicht korrekt.

— 22 conditions not correct or request sequence error

Der angeforderte Dienst ist nicht aktiv oder die Reihenfolge der Anforderungsnachrichten ist nicht korrekt.

— 31 Request out of range

Der Parameterdatensatz der Anforderung (Datenfeld) ist ungültig.

— 50 upload not accepted

Die Anforderung kann nicht ausgeführt werden (VU in einem nicht geeigneten Modus oder interne Störung der VU).

— 78 response pending

Die angeforderte Aktion kann nicht rechtzeitig abgeschlossen werden, und die VU ist nicht bereit, eine weitere Anforderung anzunehmen.

— FA data not available

Das Datenobjekt einer Datenübertragungsanforderung ist in der VU nicht verfügbar (z. B. keine Karte eingesetzt, …).

2.2.3 *Nachrichtenfluss*

Ein typischer Nachrichtenfluss während einer normalen Datendownload-Prozedur sieht folgendermaßen aus:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

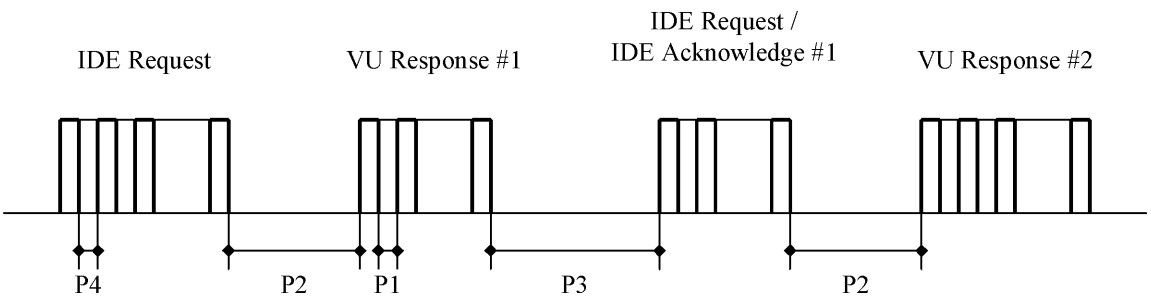
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field < 255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Timing*

DDP_019 Während des normalen Betriebs sind die in der folgenden Abbildung dargestellten Timing-Parameter relevant:

Abbildung 1

Nachrichtenfluss, Timing



Hierbei sind:

P1 = Zeit zwischen den Bytes bei VU-Antwort.

P2 = Zeit zwischen dem Ende der IDE-Anforderung und dem Beginn der VU-Antwort bzw. zwischen dem Ende der IDE-Quittung und dem Beginn der nächsten VU-Antwort.

P3 = Zeit zwischen dem Ende der VU-Antwort und dem Beginn der neuen IDE-Anforderung bzw. zwischen dem Ende der VU-Antwort und dem Beginn der IDE-Quittung bzw. zwischen dem Ende der IDE-Anforderung und dem Beginn der neuen IDE-Anforderung, wenn VU nicht antwortet.

P4 = Zeit zwischen den Bytes bei IDE-Anforderung.

P5 = Erweiterter Wert von P3 für das Herunterladen der Karte.

Die zulässigen Werte für die Timing-Parameter sind in der folgenden Tabelle aufgeführt (KWP — erweiterter Timing-Parametersatz, verwendet bei physischer Adressierung zwecks schnellerer Kommunikation).

Timing-Parameter	Unterer Grenzwert (ms)	Oberer Grenzwert (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 Minuten

(*) Wenn die VU mit einer negativen Antwort reagiert, die einen Code mit der Bedeutung „Anforderung korrekt empfangen, Antwort kommt“ enthält, wird dieser Wert auf den gleichen oberen Grenzwert erweitert wie P3.

2.2.5 *Fehlerbehandlung*

Tritt während des Nachrichtenaustauschs ein Fehler auf, erfolgt eine Modifizierung des Nachrichtenflusses in Abhängigkeit von dem Gerät, das den Fehler erkannt hat, sowie von der Nachricht, die den Fehler hervorgerufen hat.

In Abbildung 2 und 3 sind die Fehlerbehandlungsprozeduren für die VU bzw. für das IDE dargestellt.

2.2.5.1 Start Communication-Phase

DDP_020 Erkennt das IDE einen Fehler während der Start Communication-Phase entweder durch Timing oder durch den Bitstrom, wartet es P3min bis zur erneuten Ausgabe der Anforderung.

DDP_021 Erkennt die VU einen Fehler in der vom IDE eingehenden Folge, sendet sie keine Antwort und wartet innerhalb des Zeitraums P3max auf eine weitere Nachricht Start Communication Request.

2.2.5.2 Communication-Phase

Es lassen sich zwei verschiedene Fehlerbehandlungsbereiche definieren:

1. **Die VU erkennt einen IDE-Übertragungsfehler.**

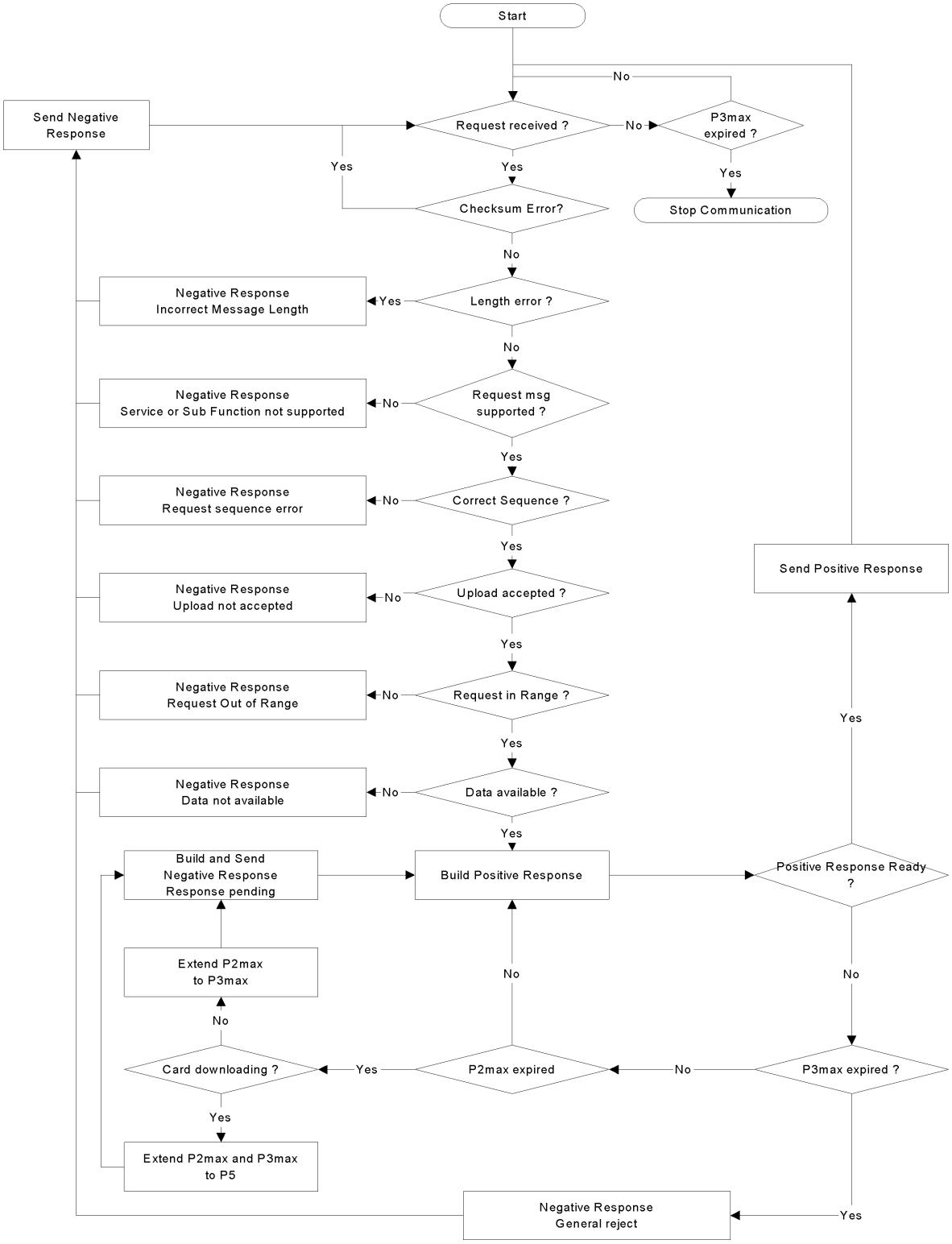
DDP_022 Die VU prüft jede empfangene Nachricht auf Timing-Fehler, Byteformatfehler (z. B. Start- und Stoppbitverletzungen) sowie Datenpaketfehler (falsche Byteanzahl empfangen, falsches Prüfsummenbyte).

DDP_023 Erkennt die VU einen der vorstehend genannten Fehler, sendet sie keine Antwort und ignoriert die empfangene Nachricht.

DDP_024 Die VU kann andere Fehler im Format oder Inhalt der empfangenen Nachricht (z. B. Nachricht nicht unterstützt) feststellen, selbst wenn die Nachricht die erforderlichen Längen und Prüfsummen einhält; in diesem Fall antwortet die VU dem IDE mit einer Negative Response-Nachricht unter Angabe der Fehlerart.

Abbildung 2

Fehlerbehandlung durch die VU



2. **Das IDE erkennt einen VU-Übertragungsfehler.**

DDP_025 Das IDE prüft jede empfangene Nachricht auf Timing-Fehler, Byteformatfehler (z. B. Start- und Stoppbitverletzungen) sowie Datenpaketfehler (falsche Byteanzahl empfangen, falsches Prüfsummenbyte).

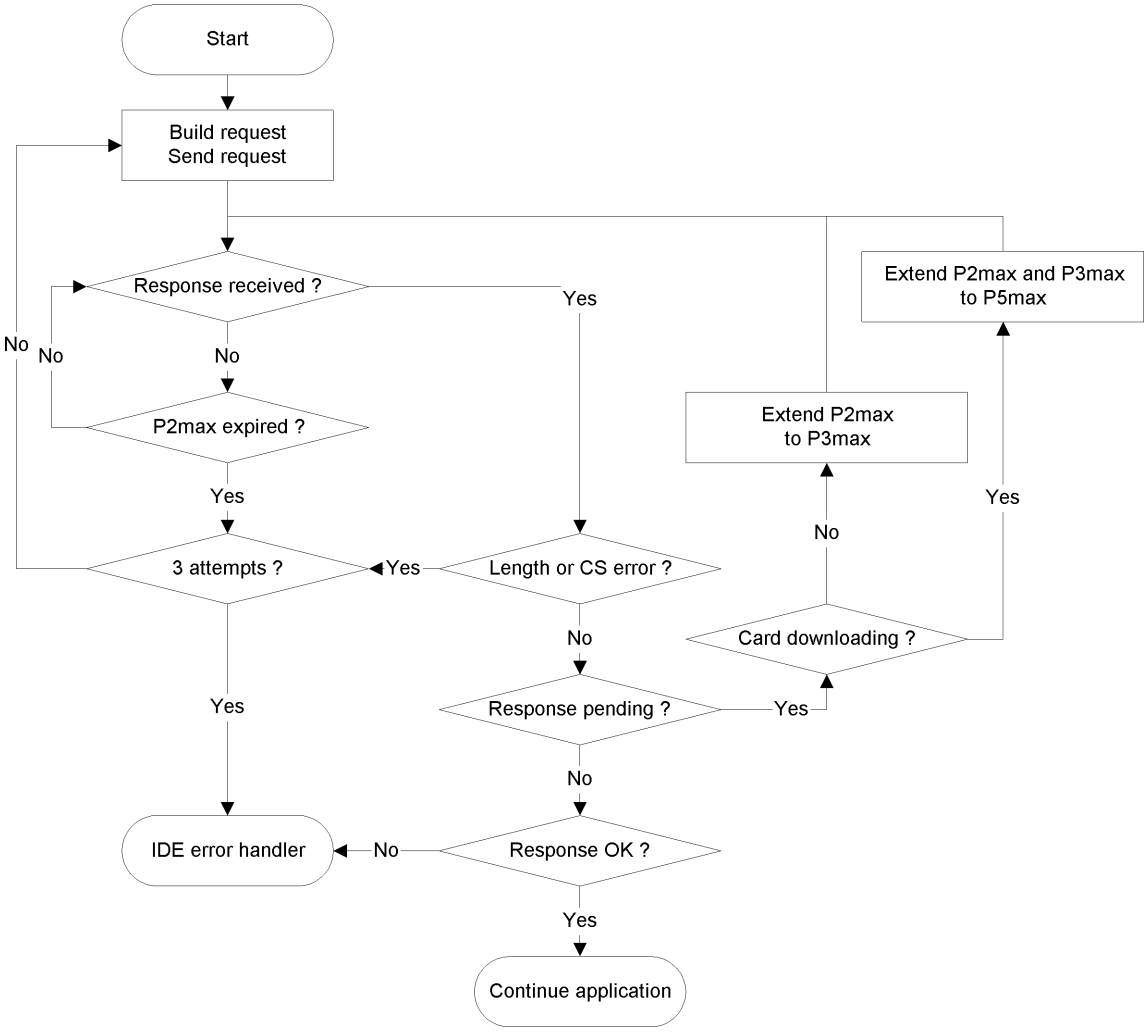
DDP_026 Das IDE erkennt Sequenzfehler, z. B. die inkorrekte Erhöhung des Teilnachrichtenzählers bei nacheinander empfangenen Nachrichten.

DDP_027 Erkennt das IDE einen Fehler oder ist innerhalb des Zeitraums P2max keine Antwort von der VU erfolgt, wird die Anforderungsnachricht für insgesamt maximal drei Übertragungen erneut gesendet. Zum Zwecke dieser Fehlererkennung wird eine Teilnachrichtquittung als Anforderung an die VU betrachtet.

DDP_028 Vor dem Beginn jeder Sendung wartet das IDE mindestens P3min; die Wartezeit wird vom letzten errechneten Auftreten eines Stoppbits nach der Fehlererkennung an gemessen.

Abbildung 3

Fehlerbehandlung durch das IDE



2.2.6 *Inhalt der Antwortnachricht*

In diesem Abschnitt wird der Inhalt der Datenfelder der verschiedenen positiven Antwortnachrichten spezifiziert.

Die Datenelemente sind in Anlage 1, Datenglossar, definiert.

Hinweis: Bei Downloads der 2. Generation wird jedes oberste Datenelement durch ein Datensatz-Array repräsentiert, auch wenn dieser lediglich einen Datensatz umfasst. Ein Datensatz-Array beginnt mit dem Kopf; dieser Kopf enthält Datensatztyp, Datensatzgröße und die Anzahl an Datensätzen. Die Datensatz-Arrays sind in den folgenden Tabellen durch „… RecordArray“ (mit Kopf) gekennzeichnet.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Das Datenfeld der Nachricht Positive Response Transfer Data Overview liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 01 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenstruktur der 1. Generation:

Datenelement	Bemerkung
MemberStateCertificate VUCertificate	VU-Sicherheitszertifikate
VehicleIdentificationNumber VehicleRegistrationIdentification	Fahrzeugkennung
CurrentDateTime	Aktuelle(s) Datum und Uhrzeit der VU
VuDownloadablePeriod	Herunterladbarer Zeitraum
CardSlotsStatus	Art der in die VU eingesteckten Karten
VuDownloadActivityData	Vorhergehender VU-Download
VuCompanyLocksData	Alle gespeicherten Unternehmenssperren. Ist der Abschnitt leer, wird lediglich noOfLocks = 0 gesendet.
VuControlActivityData	Alle in der VU gespeicherten Kontrolldatensätze. Ist der Abschnitt leer, wird lediglich noOfControls = 0 gesendet.
Signature	RSA-Signatur aller Daten (außer Zertifikate), beginnend mit VehicleIdentificationNumber bis hin zum letzten Byte des letzten VuControlActivityData.

Datenstruktur der 2. Generation:

Datenelement	Bemerkung
MemberStateCertificateRecordArray	Zertifikat des Mitgliedstaates
VUCertificateRecordArray	VU-Zertifikat
VehicleIdentificationNumberRecordArray	Fahrzeugkennung
VehicleRegistrationNumberRecordArray	Amtliches Kennzeichen des Fahrzeugs
CurrentDateTimeRecordArray	Aktuelle(s) Datum und Uhrzeit der VU
VuDownloadablePeriodRecordArray	Herunterladbarer Zeitraum
CardSlotsStatusRecordArray	Art der in die VU eingesteckten Karten
VuDownloadActivityDataRecordArray	Vorhergehender VU-Download
VuCompanyLocksRecordArray	Alle gespeicherten Unternehmenssperren. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuControlActivityRecordArray	Alle in der VU gespeicherten Kontrolldatensätze. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
SignatureRecordArray	ECC-Signatur aller vorhergehenden Daten mit Ausnahme der Zertifikate.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Das Datenfeld der Nachricht Positive Response Transfer Data Activities liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 02 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenstruktur der 1. Generation:

Datenelement	Bemerkung
TimeReal	Datum des heruntergeladenen Tages
OdometerValueMidnight	Kilometerstand am Ende des heruntergeladenen Tages
VuCardIWData	Daten zu den Einsteck-/Entnahmevorgängen dieser Karte. — Enthält dieser Abschnitt keine verfügbaren Daten, wird lediglich noOfVuCardIWRecords = 0 gesendet. — Geht ein VuCardIWRecord über 00:00 (Einstecken der Karte am Vortag) oder 24:00 (Kartenentnahme am Folgetag) hinaus, erscheint er vollständig für beide Tage.
VuActivityDailyData	Steckplatzstatus um 00:00 Uhr und aufgezeichnete Tätigkeitsänderungen für den heruntergeladenen Tag.
VuPlaceDailyWorkPeriodData	Aufgezeichnete Ortsdaten für den heruntergeladenen Tag. Ist der Abschnitt leer, wird lediglich noOfPlaceRecords = 0 gesendet.
VuSpecificConditionData	Aufgezeichnete spezifische Bedingungen für den heruntergeladenen Tag. Ist der Abschnitt leer, wird lediglich noOfSpecificConditionRecords = 0 gesendet.
Signature	RSA-Signatur aller Daten, beginnend mit TimeReal bis hin zum letzten Byte des letzten Datensatzes einer spezifischen Bedingung.

Datenstruktur der 2. Generation:

Datenelement	Bemerkung
DateOfDayDownloadedRecordArray	Datum des heruntergeladenen Tages
OdometerValueMidnightRecordArray	Kilometerstand am Ende des heruntergeladenen Tages
VuCardIWRecordArray	Daten zu den Einsteck-/Entnahmevorgängen dieser Karte. — Enthält dieser Abschnitt keine verfügbaren Daten, wird lediglich ein Array-Kopf mit noOfRecords = 0 gesendet. — Geht ein VuCardIWRecord über 00:00 (Einstecken der Karte am Vortag) oder 24:00 (Kartenentnahme am Folgetag) hinaus, erscheint er vollständig für beide Tage.
VuActivityDailyRecordArray	Steckplatzstatus um 00:00 Uhr und aufgezeichnete Tätigkeitsänderungen für den heruntergeladenen Tag.
VuPlaceDailyWorkPeriodRecordArray	Aufgezeichnete Ortsdaten für den heruntergeladenen Tag. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuGNSSCDRecordArray	GNSS-Position des Fahrzeugs, wenn die ununterbrochene Lenkzeit des Fahrers ein Vielfaches von drei Stunden erreicht. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuSpecificConditionRecordArray	Aufgezeichnete spezifische Bedingungen für den heruntergeladenen Tag. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
SignatureRecordArray	ECC-Signatur aller vorhergehenden Daten.

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Das Datenfeld der Nachricht Positive Response Transfer Data Events and Faults liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 03 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenstruktur der 1. Generation:

Datenelement	Bemerkung
VuFaultData	Alle in der VU gespeicherten oder andauernden Störungen. Ist der Abschnitt leer, wird lediglich noOfVuFaults = 0 gesendet.
VuEventData	Alle in der VU gespeicherten oder andauernden Ereignisse (außer Geschwindigkeitsüberschreitung). Ist der Abschnitt leer, wird lediglich noOfVuEvents = 0 gesendet.
VuOverSpeedingControlData	Daten zur letzten Kontrolle Geschwindigkeitsüberschreitung (Standardwert, wenn keine Daten vorhanden).
VuOverSpeedingEventData	Alle in der VU gespeicherten Ereignisse Geschwindigkeitsüberschreitung. Ist der Abschnitt leer, wird lediglich noOfVuOverSpeedingEvents = 0 gesendet.
VuTimeAdjustmentData	Alle in der VU gespeicherten Zeiteinstellungsereignisse (außerhalb des Rahmens einer vollständigen Kalibrierung). Ist der Abschnitt leer, wird lediglich noOfVuTimeAdjRecords = 0 gesendet.
Signature	RSA-Signatur aller Daten, beginnend mit noOfVuFaults bis hin zum letzten Byte des letzten Zeiteinstellungsdatensatzes.

Datenstruktur der 2. Generation:

Datenelement	Bemerkung
VuFaultRecordArray	Alle in der VU gespeicherten oder andauernden Störungen. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuEventRecordArray	Alle in der VU gespeicherten oder andauernden Ereignisse (außer Geschwindigkeitsüberschreitung). Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuOverSpeedingControlDataRecordArray	Daten zur letzten Kontrolle Geschwindigkeitsüberschreitung (Standardwert, wenn keine Daten vorhanden).
VuOverSpeedingEventRecordArray	Alle in der VU gespeicherten Ereignisse Geschwindigkeitsüberschreitung. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuTimeAdjustmentRecordArray	Alle in der VU gespeicherten Zeiteinstellungsereignisse (außerhalb des Rahmens einer vollständigen Kalibrierung). Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	ECC-Signatur aller vorhergehenden Daten.

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Das Datenfeld der Nachricht Positive Response Transfer Data Detailed Speed liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 04 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenstruktur der 1. Generation:

Datenelement	Bemerkung
VuDetailedSpeedData	Alle in der VU gespeicherten detaillierten Geschwindigkeitsdaten (ein Geschwindigkeitsblock pro Minute, in der sich das Fahrzeug bewegt hat). 60 Geschwindigkeitswerte pro Minute (ein Wert pro Sekunde).
Signature	RSA-Signatur aller Daten, beginnend mit noOfSpeedBlocks bis hin zum letzten Byte des letzten Geschwindigkeitsblocks.

Datenstruktur der 2. Generation:

Datenelement	Bemerkung
VuDetailedSpeedBlockRecordArray	Alle in der VU gespeicherten detaillierten Geschwindigkeitsdaten (ein Geschwindigkeitsblock pro Minute, in der sich das Fahrzeug bewegt hat). 60 Geschwindigkeitswerte pro Minute (ein Wert pro Sekunde).
SignatureRecordArray	ECC-Signatur aller vorhergehenden Daten.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Das Datenfeld der Nachricht Positive Response Transfer Data Technical Data liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 05 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenstruktur der 1. Generation:

Datenelement	Bemerkung
VuIdentification	
SensorPaired	
VuCalibrationData	Alle in der VU gespeicherten Kalibrierungsdatensätze.
Signature	RSA-Signatur aller Daten, beginnend mit vuManufacturerName bis hin zum letzten Byte des letzten VuCalibrationRecord.

Datenstruktur der 2. Generation:

Datenelement	Bemerkung
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Alle in der VU gespeicherten MS-Kopplungen.
VuSensorExternalGNSSCoupledRecordArray	Alle in der VU gespeicherten Kopplungen externer GNSS-Ausrüstung.
VuCalibrationRecordArray	Alle in der VU gespeicherten Kalibrierungsdatensätze.
VuCardRecordArray	Alle in der VU gespeicherten Karteneinsteckdaten.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	ECC-Signatur aller vorhergehenden Daten.

2.3. **ESM-Datenspeicherung**

DDP_034 War eine VU-Datenübertragung Bestandteil eines Download-Vorgangs, speichert das IDE in einer einzigen physischen Datei alle Daten, die während des Download-Vorgangs von der VU in Positive Response Transfer Data-Nachrichten empfangen wurden. Dabei nicht gespeichert werden Nachrichtenköpfe, Teilnachrichtenzähler, leere Teilnachrichten und Prüfsummen, gespeichert werden jedoch SID und TREP (nur der ersten Teilnachricht bei mehreren Teilnachrichten).

3. PROTOKOLL FÜR DAS HERUNTERLADEN VON DATEN VON FAHRTENSCHREIBERKARTEN

3.1. **Geltungsbereich**

Dieser Abschnitt beschreibt das direkte Herunterladen der Kartendaten einer Kontrollgerätkarte auf ein IDE. Da das IDE nicht Bestandteil der Sicherheitsumgebung ist, erfolgt keine Authentisierung zwischen der Karte und dem IDE.

3.2. **Begriffsbestimmungen**

Download-Vorgang: Die Ausführung eines Download der Chipkartendaten. Der Vorgang umfasst die gesamte Prozedur vom Zurücksetzen der Chipkarte durch ein IFD bis zur Deaktivierung der Chipkarte (Entnahme der Karte oder nächstes Zurücksetzen).

Signierte Datei: Eine Datei von der Chipkarte. Die Datei wird in Klartext zum IFD übertragen. Auf der Chipkarte erfolgt eine Hash-Code-Anwendung für die Datei, sie wird signiert, und die Signatur wird an das IFD übertragen.

3.3. **Herunterladen von der Karte**

DDP_035 Das Herunterladen einer Fahrtenschreiberkarte beinhaltet die folgenden Schritte:

— Herunterladen der gemeinsamen Informationen der Karte in den EF ICC und IC. Diese Informationen sind fakultativ und werden nicht mit einer digitalen Signatur gesichert.

— Herunterladen der EF Card_Certificate (oder CardSignCertificate) und CA_Certificate. Diese Informationen werden nicht mit einer digitalen Signatur gesichert.

Das Herunterladen dieser Dateien ist bei jedem Download-Vorgang obligatorisch.

— Herunterladen der anderen Anwendungsdaten-EF (innerhalb der DF Tachograph DF bzw. Tachograph_G2 DF) außer EF Card_Download. Diese Informationen werden mit einer digitalen Signatur gesichert.

— Bei jedem Download-Vorgang ist zumindest das Herunterladen der EF Application_Identification und ID obligatorisch.

— Beim Herunterladen einer Fahrerkarte ist zudem der Download folgender EF obligatorisch:

- `Events_Data`,
- `Faults_Data`,
- `Driver_Activity_Data`,
- `Vehicles_Used`,
- `Places`,
- `GNSS_Places (falls relevant)`,
- `Control_Activity_Data`,
- `Specific_Conditions`.

— Beim Herunterladen einer Fahrerkarte wird das Datum `LastCardDownload` in EF `Card_Download` aktualisiert.

— Beim Herunterladen einer Werkstattkarte ist der Kalibrierungszähler in der EF `Card_Download` zurückzusetzen.

— Beim Herunterladen einer Werkstattkarte ist `EF Sensor_Installation_Data` nicht herunterzuladen.

3.3.1 *Initialisierungssequenz*

DDP_036 Das IDE leitet die folgende Sequenz ein:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇦	Hardware zurücksetzen	
ATR	⇨		

Mit PPS kann auf eine höhere Baudrate gewechselt werden, sofern die Chipkarte diese Baudrate unterstützt.

3.3.2 *Sequenz für unsignierte Dateien*

DDP_037 Die Sequenz für das Herunterladen der EF ICC, IC, Card_Certificate (oder CardSignCertificate) und CA_Certificate lautet folgendermaßen:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇦	**Select File**	Auswahl nach Dateikennung
OK	⇨		
	⇦	**Read Binary**	Enthält die Datei mehr Daten, als der Puffer des Lesers oder der Karte fassen kann, ist der Befehl so lange zu wiederholen, bis die gesamte Datei ausgelesen ist.
File Data **OK**	⇨	Daten auf ESM speichern	gemäß **3.4** Data storage format

Hinweis 1: Vor Auswahl der EF Card_Certificate (CardSignCertificate) muss die Fahrtenschreiberanwendung ausgewählt werden (Auswahl durch AID).

Hinweis 2: Das Auswählen und Auslesen einer Datei kann mithilfe des Befehls Read Binary mit Kurz-Elementardateikennung in einem Schritt erfolgen.

3.3.3 *Sequenz für signierte Dateien*

DDP_038 Die folgende Sequenz wird für die folgenden Dateien verwendet, die jeweils mit ihrer Signatur herunterzuladen sind:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Berechnet den Hashwert über dem Dateninhalt der ausgewählten Datei mithilfe des vorgeschriebenen Hash-Algorithmus gemäß Anlage 11. Dieser Befehl ist kein ISO-Befehl.
Hash of File berechnen und Hashwert temporär speichern			
OK	⇨		
	⇦	**Read Binary**	Enthält die Datei mehr Daten, als der Puffer des Lesers oder der Karte fassen kann, ist der Befehl so lange zu wiederholen, bis die gesamte Datei ausgelesen ist.
File Data **OK**	⇨	Empfangene Daten auf ESM speichern	gemäß **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature**	
Perform Security Operation „Compute Digital Signature“ mithilfe des temporär gespeicherten Hashwerts			
Signature **OK**	⇨	Daten an die zuvor auf dem ESM gespeicherten Daten anfügen	gemäß **3.4** Data storage format

Hinweis: Das Auswählen und Auslesen einer Datei kann mithilfe des Befehls Read Binary mit Kurz-Elementardateikennung in einem Schritt erfolgen. In diesem Fall kann die EF ausgewählt und ausgelesen werden, bevor der Befehl Perform Hash of File angewendet wird.

3.3.4 *Sequenz für das Zurücksetzen des Kalibrierungszählers*

DDP_039 Die Sequenz für das Zurücksetzen des Zählers `NoOfCalibrationsSinceDownload` in der EF `Card_Download` auf einer Werkstattkarte lautet folgendermaßen:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇦	**Select File** EF Card_Download	Auswahl nach Dateikennung
OK	⇨		

Karte	Rich-tung	IDE/IFD	Bedeutung/Bemerkungen
	⇦	**Update Binary** NoOfCalibrationsSince-Download = „00 00“	
setzt Kartendownload zurück			
OK	⇨		

Hinweis: Das Auswählen und Aktualisieren einer Datei kann mithilfe des Befehls Update Binary mit Kurz-Elementardateikennung in einem Schritt erfolgen.

3.4. **Datenspeicherungsformat**

3.4.1 *Einleitung*

DDP_040 Die heruntergeladenen Daten sind nach folgenden Bedingungen zu speichern:

— Die Daten sind transparent zu speichern, d. h. die Reihenfolge der von der Karte übertragenen Bytes sowie die Reihenfolge der in ihnen enthaltenen Bits müssen während der Speicherung erhalten bleiben.

— Alle im Rahmen eines Download-Vorgangs heruntergeladenen Dateien der Karte werden in einer einzigen Datei auf dem ESM gespeichert

3.4.2 *Dateiformat*

DDP_041 Das Dateiformat ist eine Verkettung mehrerer TLV-Objekte.

DDP_042 Der Tag für eine EF ist die FID sowie der Zusatz „00“.

DDP_043 Der Tag der Signatur einer EF ist die FID der Datei sowie der Zusatz „01“.

DDP_044 Die Länge ist ein 2-Byte-Wert. Der Wert legt die Anzahl der Bytes im Wertfeld fest. Der Wert „FF FF“ im Längenfeld ist für eine künftige Verwendung reserviert.

DDP_045 Wird eine Datei nicht heruntergeladen, ist auch nichts zu speichern, was mit der Datei im Zusammenhang steht (also kein Tag und keine Nulllänge).

DDP_046 Eine Signatur wird als nächstes TLV-Objekt unmittelbar nach dem Objekt, das die Daten der Datei enthält, gespeichert.

Definition	Bedeutung	Länge
FID (2 Bytes) || „00“	Tag für EF (FID)	3 Bytes
FID (2 Bytes) || „01“	Tag für Signatur der EF (FID)	3 Bytes
xx xx	Länge des Wertfelds	2 Bytes

Beispiel für Daten in einer Download-Datei auf einem ESM:

Tag	Länge	Wert
00 02 00	00 11	Daten von EF ICC
C1 00 00	00 C2	Daten von EF Card_Certificate
		…
05 05 00	0A 2E	Daten von EF Vehicles_Used
05 05 01	00 80	Signatur von EF Vehicles_Used

4. HERUNTERLADEN VON DER FAHRTENSCHREIBERKARTE ÜBER EINE FAHRZEUGEINHEIT

DDP_047 Die VU muss das Herunterladen des Inhalts einer eingesteckten und an ein IDE angeschlossenen Fahrerkarte zulassen.

DDP_048 Zum Starten dieses Modus sendet das IDE die Nachricht Transfer Data Request Card Download an die VU (siehe 2.2.2.9).

DDP_049 Daraufhin lädt die VU die gesamte Karte dateiweise in Übereinstimmung mit dem in Abschnitt 3 definierten Download-Protokoll herunter und leitet alle von der Karte empfangenen Daten im entsprechenden TLV-Dateiformat (siehe 3.4.2) sowie eingekapselt in eine Positive Response Transfer Data-Nachricht an das IDE weiter.

DDP_050 Das IDE ruft die Kartendaten aus der Nachricht Positive Response Transfer Data ab (unter Fortlassung aller Köpfe, SID, TREP, Teilnachrichtenzähler und Prüfsummen) und speichert sie innerhalb einer in Abschnitt 2.3 beschriebenen physischen Datei.

DDP_051 Danach aktualisiert die VU gegebenenfalls die Dateien `Control_Activity_Data` oder `Card_Download` der Fahrerkarte.

Anlage 8

KALIBRIERUNGSPROTOKOLL

INHALTSVERZEICHNIS

1. EINLEITUNG 283

2. BEGRIFFE, BEGRIFFSBESTIMMUNGEN UND REFERENZDOKUMENTE 283

3. DIENSTEÜBERSICHT 284

3.1. Verfügbare Dienste 284

3.2. Antwortcodes 285

4. KOMMUNIKATIONSDIENSTE 285

4.1. Der Dienst StartCommunication 285

4.2. Der Dienst StopCommunication 287

4.2.1 Beschreibung der Nachricht 287

4.2.2 Nachrichtenformat 288

4.2.3 Parameterdefinition 289

4.3. Der Dienst TesterPresent 289

4.3.1 Beschreibung der Nachricht 289

4.3.2 Nachrichtenformat 289

5. VERWALTUNGSDIENSTE 291

5.1. Der Dienst StartDiagnosticSession 291

5.1.1 Beschreibung der Nachricht 291

5.1.2 Nachrichtenformat 292

5.1.3 Parameterdefinition 293

5.2. Der Dienst SecurityAccess 294

5.2.1 Beschreibung der Nachricht 294

5.2.2 Nachrichtenformat — SecurityAccess — requestSeed 295

5.2.3 Nachrichtenformat — SecurityAccess — sendKey 296

6. DATENÜBERTRAGUNGSDIENSTE 297

6.1. Dienst ReadDataByIdentifier 298

6.1.1 Beschreibung der Nachricht 298

6.1.2 Nachrichtenformat 298

6.1.3 Parameterdefinition 299

6.2. Der Dienst WriteDataByIdentifier 300

6.2.1 Beschreibung der Nachricht 300

6.2.2 Nachrichtenformat 300

6.2.3 Parameterdefinition 302

7. PRÜFIMPULSSTEUERUNG — FUNKTIONSEINHEIT EINGABE/AUSGABE-STEUERUNG 302

7.1. Der Dienst InputOutputControlByIdentifier 302

7.1.1 Beschreibung der Nachricht 302

7.1.2 Nachrichtenformat 303

7.1.3 Parameterdefinition 304

8. DATARECORDS-FORMATE 305

8.1. Wertebereiche der übertragenen Parameter 305

8.2. dataRecords-Formate 306

1. EINLEITUNG

In dieser Anlage wird der Datenaustausch zwischen einer Fahrzeugeinheit und einem Prüfgerät über die K-Leitung, die Teil der in Anlage 6 beschriebenen Kalibrierungsschnittstelle ist, beschrieben. Außerdem enthält sie eine Beschreibung der Steuerung der Eingangs-/Ausgangssignalleitung am Kalibrierungsanschluss.

Das Aufbauen der K-Leitungskommunikation wird im Abschnitt 4 „Kommunikationsdienste“ beschrieben.

In dieser Anlage ist vom Konzept der Diagnosevorgänge die Rede, mit dem der Umfang der K-Leitungssteuerung unter verschiedenen Bedingungen festgelegt wird. Der Standardvorgang ist dabei die „StandardDiagnosticSession“, bei der aus einer Fahrzeugeinheit alle Daten ausgelesen, jedoch keine Daten in die Fahrzeugeinheit geschrieben werden können.

Die Auswahl des Diagnosevorgangs wird im Abschnitt 5 „Verwaltungsdienste“ beschrieben.

Dieser Anhang gilt als relevant für beide Generationen von VU- und Werkstattkarten gemäß den in dieser Verordnung beschriebenen Interoperabilitätsanforderungen.

CPR_001 Im Programmiervorgang „ECUProgrammingSession“ ist es möglich, Daten in die Fahrzeugeinheit einzugeben. Bei der Eingabe von Kalibrierungsdaten muss sich die Fahrzeugeinheit außerdem in der Betriebsart KALIBRIERUNG befinden.

Die Datenübertragung über die K-Leitung wird im Abschnitt 6 „Datenübertragungsdienste“ beschrieben. Die Formate der übertragenen Daten werden in Abschnitt 8 „dataRecords-Formate“ erläutert.

CPR_002 Der Einstellvorgang „ECUAdjustmentSession“ ermöglicht die Auswahl der E/A-Betriebsart der Kalibrierungs-E/A-Signalleitung über die Schnittstelle der K-Leitung. Die Steuerung der Kalibrierungs-E/A-Signalleitung wird in Abschnitt 7 „Prüfimpulssteuerung — Funktionseinheit Eingabe/Ausgabe-Steuerung“ beschrieben.

CPR_003 Im vorliegenden Dokument wird als Adresse für das Prüfgerät durchgängig ‘tt’ verwendet. Ungeachtet dessen, dass für Prüfgeräte bevorzugte Adressen verwendet werden können, muss die VU auf jede Prüfgerätadresse richtig antworten. Die physische Adresse der VU ist 0xEE.

2. BEGRIFFE, BEGRIFFSBESTIMMUNGEN UND REFERENZDOKUMENTE

Die Protokolle, Nachrichten und Fehlercodes beruhen grundsätzlich auf einem Normentwurf von ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, Version 6 vom 22. Februar 2001).

Für die Service Identifier (SID), die Bedienanforderungen und -antworten sowie die Standardparameter werden Byte-Codierungen und hexadezimale Werte verwendet.

Der Begriff „Prüfgerät“ bezeichnet das zur Eingabe der Programmierungs-/Kalibrierungsdaten in die VU verwendete Gerät.

Die Begriffe „Client“ und „Server“ beziehen sich auf das Prüfgerät bzw. die VU.

Der Begriff „ECU“ bedeutet „elektronische Steuereinheit“ und bezieht sich auf die VU.

Referenzdokumente:

ISO 14230-2:

Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999.

Straßenfahrzeuge — Diagnose.

3. DIENSTEÜBERSICHT

3.1. **Verfügbare Dienste**

Die folgende Tabelle gibt einen Überblick über die in dieser Anlage beschriebenen Dienste, die im Fahrtenschreiber verfügbar sein werden.

CPR_004 In der Tabelle sind die Dienste aufgeführt, die bei aktiviertem Diagnosevorgang verfügbar sind.

— **Spalte 1** enthält die verfügbaren Dienste.

— **Spalte 2** nennt den Abschnitt in der vorliegenden Anlage, in der der Dienst näher beschrieben wird.

— **Spalte 3** ordnet die Service-Identifier-Werte bei Anforderungsnachrichten zu.

— **Spalte 4** gibt die Dienste des Standardvorgangs**„StandardDiagnosticSession" (SD)** an, die in jeder VU implementiert sein müssen.

— **Spalte 5** gibt die Dienste des Einstellvorgangs **„ECUAdjustmentSession" (ECUAS)** an, die implementiert sein müssen, um die Steuerung der E/A-Signalleitung der für die Kalibrierung vorgesehenen Steckverbindung an der Frontplatte der VU zu gestatten.

— **Spalte 6** gibt die Dienste des Programmiervorgangs **„ECUProgrammingSession" (ECUPS)** an, die implementiert sein müssen, um die Programmierung von Parametern in der VU zu ermöglichen.

Tabelle 1

Übersicht über die SId-Werte

			Diagnosevorgänge		
Name des Diagnosedienstes	Abschnitt Nr.	Wert SId Req.	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Dieses Symbol zeigt an, dass der betreffende Dienst bei diesem Diagnosevorgang obligatorisch ist.

Ein Feld ohne Symbol bedeutet, dass der betreffende Dienst bei diesem Diagnosevorgang nicht zugelassen ist.

3.2. **Antwortcodes**

Für jeden Dienst sind Antwortcodes festgelegt.

4. KOMMUNIKATIONSDIENSTE

Um die Kommunikation aufzubauen und aufrecht zu erhalten, sind einige Dienste erforderlich, die nicht auf der Anwendungsschicht liegen. Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 2

Kommunikationsdienste

Name des Dienstes	Beschreibung
StartCommunication	Client fordert Beginn eines Kommunikationsvorgangs mit einem (mehreren) Server(n) an
StopCommunication	Client fordert Beendigung des laufenden Kommunikationsvorgangs an
TesterPresent	Client teilt dem Server mit, dass die Verbindung noch aktiv ist

CPR_005 Der Dienst StartCommunication wird genutzt, um eine Kommunikation einzuleiten. Für die Ausführung eines Dienstes ist es immer erforderlich, dass die Kommunikation initialisiert und die für die gewünschte Betriebsart geeigneten Kommunikationsparameter verwendet werden.

4.1. **Der Dienst StartCommunication**

CPR_006 Bei Erhalt eines StartCommunication-Primitivs prüft die VU, ob die angeforderte Kommunikationsverbindung unter den gegebenen Bedingungen initialisiert werden kann. Gültige Bedingungen für die Initialisierung einer Kommunikationsverbindung sind im Dokument ISO 14230-2 beschrieben.

CPR_007 Die VU führt daraufhin alle erforderlichen Maßnahmen zur Initialisierung der Kommunikationsverbindung aus und versendet ein StartCommunication-Antwort-Primitiv mit den gewählten Positive Response-Parametern.

CPR_008 Erhält eine bereits initialisierte (und in eine Diagnosesitzung eingetretene) VU die Anforderung StartCommunication (z. B. aufgrund Wiederanlauf des Prüfgeräts nach einer Fehlerbedingung), muss die Anforderung angenommen und die VU neu initialisiert werden.

CPR_009 Falls sich die Kommunikationsverbindung aus irgendeinem Grund nicht initialisieren lässt, setzt die VU den Betrieb in der gleichen Weise wie unmittelbar vor dem Versuch zur Initialisierung der Kommunikationsverbindung fort.

CPR_010 Die Anforderungsnachricht StartCommunication muss an eine physische Adresse erfolgen.

CPR_011 Die Initialisierung der VU für Dienste erfolgt mithilfe einer „Schnellinitialisierung“:

— Jeder Aktivität geht ein Bus-Ruhezustandstakt voraus.

— Das Prüfgerät überträgt anschließend eine Initialisierungssequenz.

— Alle zum Aufbau der Kommunikation benötigten Informationen sind in der Antwort der VU enthalten.

CPR_012 Nach Beendigung der Initialisierung:

— Alle Kommunikationsparameter werden entsprechend den Schlüssel-Bytes auf die Werte in Tabelle 4 gesetzt.

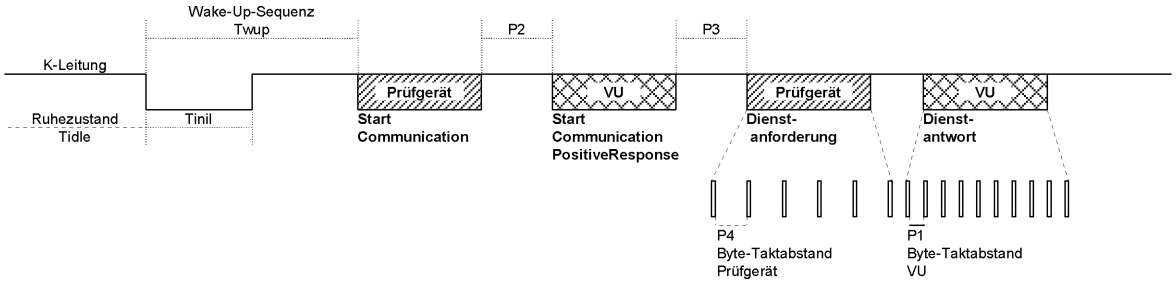
— Die VU wartet auf die erste Anforderung vom Prüfgerät.

— Die VU befindet sich in der Standarddiagnosebetriebsart, d. h. der „StandardDiagnosticSession".

— Die Kalibrierungs-E/A-Signalleitung befindet sich im Standardzustand, d. h. im deaktivierten Zustand.

CPR_014 Die Übertragungsgeschwindigkeit (Baudrate) auf der K-Leitung beträgt 10 400 Baud.

CPR_016 Die Schnellinitialisierung wird ausgelöst, indem das Prüfgerät eine Wake-Up-Sequenz (Wup) auf der K-Leitung überträgt. Diese beginnt nach dem Ruhezustandstakt auf der K-Leitung mit einem L-Takt TInil. Das Prüfgerät sendet das erste Bit des Dienstes StartCommunication im Anschluss an einen TWup-Takt, der nach der ersten fallenden Flanke beginnt.



CPR_017 Die Taktwerte für die Schnellinitialisierung sowie für die Kommunikation generell sind in den nachstehenden Tabellen im Einzelnen aufgeführt. Für den Ruhezustandstakt existieren mehrere Möglichkeiten:

— Erste Übertragung nach Einschalten, Tidle = 300 ms.

— Nach Abschluss eines Dienstes StopCommunication, Tidle = P3 Minimum

— Nach Beendigung der Kommunikation durch Zeitüberschreitung (Time-Out) P3 Maximum, Tidle = 0.

Tabelle 3

Taktwerte zur Schnellinitialisierung

Parameter		Min.	Max.
TInil	25 ± 1 ms	24 ms	26 ms
TWup	50 ± 1 ms	49 ms	51 ms

Tabelle 4

Taktwerte für die Kommunikation

Takt-Parameter	Beschreibung der Parameter	Untere Grenzwerte [in ms]	Obere Grenzwerte [in ms]
		Min.	Max.
P1	Byte-Taktabstand für die VU-Antwort	0	20
P2	Zeit zwischen Prüfgerätanforderung und VU-Antwort bzw. zwei VU-Antworten	25	250
P3	Zeit zwischen Ende der VU-Antworten und Beginn einer neuen Prüfgerätanforderung	55	5 000
P4	Byte-Taktabstand für die Prüfgerätantwort	5	20

CPR_018 Das Nachrichtenformat für die Schnellinitialisierung ist in den nachstehenden Tabellen spezifiziert.

Tabelle 5

Nachricht StartCommunication Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	81	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Prüfsumme	00-FF	CS

Tabelle 6

Nachricht StartCommunication Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**StartCommunication Positive Response Service**	**C1**	**SCRPR**
#6	Schlüsselbyte 1	EA	KB1
#7	Schlüsselbyte 2	8F	KB2
#8	Prüfsumme	00-FF	CS

CPR_019 Eine negative Antwort (Negative Response) auf die Anforderungsnachricht StartCommunication gibt es nicht. Kann keine positive Nachricht (Positive Response) gegeben werden, so erfolgt keine Initialisierung der VU, und diese verbleibt in ihrer normalen Betriebsart.

4.2. **Der Dienst StopCommunication**

4.2.1 *Beschreibung der Nachricht*

Dieser Dienst der Kommunikationssteuerungsschicht hat zum Zweck, einen Kommunikationsvorgang zu beenden.

CPR_020 Bei Erhalt eines StopCommunication-Primitivs prüft die VU, ob die derzeitigen Bedingungen die Beendigung dieser Kommunikation gestatten. Ist dies der Fall, so führt die VU alle erforderlichen Maßnahmen zur Beendigung dieser Kommunikation durch.

CPR_021 Ist die Beendigung der Kommunikation möglich, gibt die VU vor der Beendigung der Kommunikation ein StopCommunication-Antwort-Primitiv mit den gewählten Positive Response-Parametern aus.

CPR_022 Falls sich die Kommunikation aus irgendeinem Grund nicht beenden lässt, gibt die VU ein StopCommunication-Antwort-Primitiv mit den gewählten Parametern für Negative Response aus.

CPR_023 Wird von der VU eine Zeitüberschreitung aufgrund P3max erkannt, muss die Kommunikation ohne Ausgabe eines Antwortelements beendet werden.

4.2.2 *Nachrichtenformat*

CPR_024 Die Nachrichtenformate für die StopCommunication-Primitive sind in den folgenden Tabellen aufgeführt.

Tabelle 7

Nachricht StopCommunication Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	01	LEN
#5	**StopCommunication Request Service**	**82**	**SPR**
#6	Prüfsumme	00-FF	CS

Tabelle 8

Nachricht StopCommunication Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Prüfsumme	00-FF	CS

Tabelle 9

Nachricht StopCommunication Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Prüfsumme	00-FF	CS

4.2.3 *Parameterdefinition*

Dieser Dienst erfordert keine Parameterdefinition.

4.3. **Der Dienst TesterPresent**

4.3.1 *Beschreibung der Nachricht*

Mithilfe des Dienstes TesterPresent teilt das Prüfgerät dem Server mit, dass es sich noch immer in einer aktiven Verbindung mit ihm befindet, um zu verhindern, dass der Server automatisch in die normale Betriebsart zurückkehrt und dadurch möglicherweise die Verbindung beendet. Dieser Dienst sorgt durch regelmäßiges Aussenden einer Anforderung dafür, dass die Diagnosesitzung oder Verbindung aktiv bleibt, indem der P3-Zeitgeber bei jedem Erhalt einer Anforderung für diesen Dienst zurückgesetzt wird.

4.3.2 *Nachrichtenformat*

CPR_079 Die Nachrichtenformate für die TesterPresent-Primitive sind in den folgenden Tabellen aufgeführt.

Tabelle 10

Nachricht TesterPresent Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#6	Sub Function = responseRequired = [yes	01	RESPREQ_Y
	no]	02	RESPREQ_NO
#7	Prüfsumme	00-FF	CS

CPR_080 Ist der Parameter responseRequired auf „yes“ gesetzt, so antwortet der Server mit folgenden positiven Antwortnachrichten. Ist der Parameter auf „no“ gesetzt, sendet der Server keine Antwort.

Tabelle 11

Nachricht TesterPresent Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Prüfsumme	00-FF	CS

CPR_081 Der Dienst verwendet die folgenden negativen Antwort-Codes:

Tabelle 12

Nachricht TesterPresent Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Prüfsumme	00-FF	CS

5. VERWALTUNGSDIENSTE

Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 13

Verwaltungsdienste

Name des Dienstes	Beschreibung
StartDiagnosticSession	Client fordert Beginn eines Diagnosevorgangs mit einer VU an
SecurityAccess	Client ruft Funktionen auf, auf die nur berechtigte Benutzer Zugriff haben.

5.1. **Der Dienst StartDiagnosticSession**

5.1.1 *Beschreibung der Nachricht*

CPR_025 Der Dienst StartDiagnosticSession dient dazu, verschiedene Diagnosevorgänge im Server zu aktivieren. Ein Diagnosevorgang aktiviert bestimmte Dienste nach Maßgabe von Tabelle 17. Mit einem solchen Vorgang kann der Fahrzeughersteller bestimmte Dienste aktivieren, die hier nicht beschrieben werden. Die Implementierungsregeln haben folgenden Festlegungen zu entsprechen:

— Es ist stets genau ein Diagnosevorgang in der VU aktiv.

— Die VU startet die „StandardDiagnosticSession“ bei jedem Einschaltvorgang. Wird kein anderer Diagnosevorgang gestartet, so läuft die „StandardDiagnosticSession“ so lange, wie die VU eingeschaltet ist.

— Wird vom Prüfgerät ein bereits laufender Diagnosevorgang angefordert, sendet die VU eine positive Antwortnachricht (Positive Response).

— Fordert das Prüfgerät einen neuen Diagnosevorgang an, sendet die VU zuerst eine positive Antwortnachricht auf „StartDiagnosticSession“, bevor der neue Diagnosevorgang in der VU aktiviert wird. Kann die VU den angeforderten neuen Diagnosevorgang nicht starten, antwortet sie mit einer negativen Antwortnachricht auf StartDiagnosticSession und setzt den laufenden Diagnosevorgang fort.

CPR_026 Ein Diagnosevorgang darf erst begonnen werden, wenn die Nachrichtenverbindung zwischen dem Client und der VU errichtet wurde.

CPR_027 Nach einer erfolgreichen Anforderung StartDiagnosticSession sind die in Tabelle 4 aufgeführten Taktparameter aktiv, wobei der Parameter diagnosticSession in der Anforderungsnachricht auf „StandardSession“ gesetzt ist, wenn zuvor ein anderer Diagnosevorgang aktiv war.

5.1.2 *Nachrichtenformat*

CPR_028 Die Nachrichtenformate für die StartDiagnosticSession-Primitive sind in den folgenden Tabellen spezifiziert.

Tabelle 14

Nachricht StartDiagnosticSession Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [ein Wert aus Tabelle 17]	xx	DS_…
#7	Prüfsumme	00-FF	CS

Tabelle 15

Nachricht StartDiagnosticSession Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [gleicher Wert wie Byte Nr. 6 in Tabelle 14]	xx	DS_…
#7	Prüfsumme	00-FF	CS

Tabelle 16

Nachricht StartDiagnosticSession Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT

Byte-Nr.	Parameterbezeichnung		Hex-Wert	Symbolform
#3	Quelladress-Byte		EE	SRC
#4	Zusatzlängen-Byte		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	ResponseCode =	[subFunctionNotSupported [a]	12	RC_SFNS
		incorrectMessageLength [b]	13	RC_IML
		conditionsNotCorrect [c]	22	RC_CNC
#8	Prüfsumme		00-FF	CS

[a] — Der in Byte Nr. 6 der Anforderungsnachricht eingetragene Wert wird nicht unterstützt, d. h., er ist nicht in Tabelle 17 definiert.
[b] — Die Nachricht hat eine falsche Länge.
[c] — Die Bedingungen für die angeforderte StartDiagnosticSession sind nicht erfüllt.

5.1.3 *Parameterdefinition*

CPR_029 Der Parameter ***diagnosticSession (DS_)*** dient dem Dienst StartDiagnosticSession dazu, das spezielle Verhalten des Servers bzw. der Server zu wählen. Im vorliegenden Dokument sind folgende Diagnosevorgänge spezifiziert:

Tabelle 17

Definition der Werte für diagnosticSession

Hex	Beschreibung	Symbolform
81	**StandardDiagnosticSession** Dieser Diagnosevorgang aktiviert alle Dienste, die in **Spalte 4 „SD“** von **Tabelle 1** angegeben sind. Diese Dienste ermöglichen das Auslesen der Daten von einem Server (VU). Dieser Diagnosevorgang ist aktiv, nachdem die Initialisierung zwischen Client (Prüfgerät) und Server (VU) erfolgreich abgeschlossen wurde. Dieser Diagnosevorgang kann durch andere in diesem Abschnitt genannte Diagnosevorgänge überschrieben werden.	**SD**
85	**ECUProgrammingSession** Dieser Diagnosevorgang aktiviert alle Dienste, die in **Spalte 6 „ECUPS“** von **Tabelle 1** angegeben sind. Diese Dienste unterstützen die Speicherprogrammierung eines Servers (VU). Dieser Diagnosevorgang kann durch andere in diesem Abschnitt genannte Diagnosevorgänge überschrieben werden.	**ECUPS**
87	**ECUAdjustmentSession** Dieser Diagnosevorgang aktiviert alle Dienste, die in **Spalte 5** „ECUAS“ von **Tabelle 1** angegeben sind. Diese Dienste unterstützen die Eingabe/Ausgabe-Steuerung eines Servers (VU). Dieser Diagnosevorgang kann durch andere in diesem Abschnitt genannte Diagnosevorgänge überschrieben werden.	**ECUAS**

5.2. **Der Dienst SecurityAccess**

Das Schreiben von Kalibrierungsdaten ist nur dann möglich, wenn sich die VU in der Betriebsart KALIBRIERUNG befindet. Der Zugriff auf die Betriebsart KALIBRIERUNG wird erst gewährt, nachdem eine gültige Werkstattkarte in die VU eingesteckt und zusätzlich die richtige persönliche Geheimzahl (PIN) in die VU eingegeben wurde.

Wenn sich die VU in der Betriebsart KALIBRIERUNG oder KONTROLLE befindet, ist der Zugriff auf die Eingabe/Ausgabe-Leitung für die Kalibrierung auch möglich.

Der Dienst SecurityAccess stellt die Möglichkeit zur PIN-Eingabe bereit und zeigt dem Prüfgerät an, ob sich die VU in der Betriebsart KALIBRIERUNG befindet.

Eine PIN-Eingabe durch alternative Methoden ist zulässig.

5.2.1 *Beschreibung der Nachricht*

Der Dienst SecurityAccess besteht aus der Nachricht SecurityAccess „requestSeed", der möglicherweise eine Nachricht SecurityAccess „sendKey" folgt. Der Dienst SecurityAccess muss nach dem Dienst StartDiagnosticSession ausgeführt werden.

CPR_033 Mit der Nachricht SecurityAccess „requestSeed" stellt das Prüfgerät fest, ob die Fahrzeugeinheit zur Annahme einer PIN bereit ist.

CPR_034 Befindet sich die Fahrzeugeinheit bereits in der Betriebsart KALIBRIERUNG, beantwortet sie die Anforderung durch Versenden eines Seed 0x0000 mithilfe des Dienstes auf SecurityAccess Positive Response.

CPR_035 Ist die Fahrzeugeinheit zur Annahme einer PIN zur Verifizierung einer Werkstattkarte bereit, beantwortet sie die Anforderung durch Versenden eines Seed, der größer als 0x0000 ist, mithilfe des Dienstes SecurityAccess Positive Response.

CPR_036 Ist die Fahrzeugeinheit zur Annahme einer PIN vom Prüfgerät nicht bereit, weil entweder die eingesteckte Werkstattkarte ungültig ist, keine Werkstattkarte eingesteckt wurde oder die Fahrzeugeinheit eine andere Methode der PIN-Eingabe erwartet, beantwortet sie die Anforderung mit einer Negative Response, wobei der Antwortcode „conditionsNotCorrectOrRequestSequenceError" lautet.

CPR_037 Das Prüfgerät sendet dann gegebenenfalls eine Nachricht SecurityAccess „sendKey", um eine PIN an die Fahrzeugeinheit zu übergeben. Um ausreichend Zeit für den Prozess der Kartenauthentisierung zu gewähren, sendet die VU den negativen Antwortcode „requestCorrectlyReceived-ResponsePending", mit dem die Antwortzeit verlängert wird. Die längst mögliche Wartezeit darf jedoch 5 Minuten nicht überschreiten. Sobald der angeforderte Dienst abgeschlossen ist, sendet die VU eine positive oder negative Antwortnachricht mit einem anderen Antwortcode als diesem. Der negative Antwortcode „requestCorrectlyReceived-ResponsePending" kann so oft von der VU wiederholt werden, bis der angeforderte Dienst abgeschlossen ist und die abschließende Antwortnachricht gesandt wurde.

CPR_038 Die Fahrzeugeinheit darf diese Anforderung nur dann mit dem Dienst SecurityAccess Positive Response beantworten, wenn sie sich in der Betriebsart KALIBRIERUNG befindet.

CPR_039 In den nachstehenden Fällen muss die Fahrzeugeinheit diese Anforderung mit einer Negative Response bei folgendermaßen gesetzten Antwortcodes quittieren:

— subFunctionNotsupported: ungültiges Format für den Parameter der Unterfunktion (accessType),

— conditionsNotCorrectOrRequestSequenceError: Fahrzeugeinheit ist zur Annahme einer PIN-Eingabe nicht bereit,

— invalidKey: ungültige PIN, Zahl der zulässigen PIN-Prüfversuche jedoch nicht überschritten,

— exceededNumberOfAttempts: ungültige PIN und Zahl der zulässigen PIN-Prüfversuche überschritten,

— generalReject: richtige PIN, gegenseitige Authentisierung mit Werkstattkarte ist jedoch fehlgeschlagen.

5.2.2 *Nachrichtenformat — SecurityAccess — requestSeed*

CPR_040 Die Nachrichtenformate für die SecurityAccess „requestSeed"-Primitive sind in den folgenden Tabellen spezifiziert.

Tabelle 18

Nachricht SecurityAccess Request — requestSeed

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType — requestSeed	7D	AT_RSD
#7	Prüfsumme	00-FF	CS

Tabelle 19

Nachricht SecurityAccess — requestSeed Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	04	LEN
#5	**SecurityAccess Positive Response Service ID**	**67**	**SAPR**
#6	accessType — requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Prüfsumme	00-FF	CS

Tabelle 20

Nachricht SecurityAccess Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#4	Zusatzlängen-Byte	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Prüfsumme	00-FF	CS

5.2.3 *Nachrichtenformat — SecurityAccess — sendKey*

CPR_041 Die Nachrichtenformate für die SecurityAccess „sendKey"-Primitive sind in den folgenden Tabellen spezifiziert.

Tabelle 21

Nachricht SecurityAccess Request — sendKey

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType — sendKey	7E	AT_SK
#7 bis #m +6	Schlüssel #1 (H)	xx	KEY
	…	…	
	Schlüssel #m (N, m muss mindestens 4 und darf höchstens 8 betragen)	xx	
#m+7	Prüfsumme	00-FF	CS

Tabelle 22

Nachricht SecurityAccess — sendKey Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#4	Zusatzlängen-Byte	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType — sendKey	7E	AT_SK
#7	Prüfsumme	00-FF	CS

Tabelle 23

Nachricht SecurityAccess Negative Response

Byte-Nr.	Parameterbezeichnung		Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung		80	FMT
#2	Zieladress-Byte		tt	TGT
#3	Quelladress-Byte		EE	SRC
#4	Zusatzlängen-Byte		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	SecurityAccess Request Service Id		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Prüfsumme		00-FF	CS

6. DATENÜBERTRAGUNGSDIENSTE

Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 24

Datenübertragungsdienste

Name des Dienstes	Beschreibung
ReadDataByIdentifier	Client fordert an, dass der aktuelle Wert eines Datensatzes durch Zugriff von recordDataIdentifier übertragen wird.
WriteDataByIdentifier	Client fordert an, dass ein Datensatz von recordDataIdentifier geschrieben wird.

6.1. **Dienst ReadDataByIdentifier**

6.1.1 *Beschreibung der Nachricht*

CPR_050 Mit dem Dienst ReadDataByIdentifier fordert der Client vom Server die Übertragung von Datensatzwerten an, die durch einen recordDataIdentifier gekennzeichnet sind. Der Fahrzeughersteller muss dafür sorgen, dass die Serverbedingungen zur Abwicklung dieses Dienstes erfüllt sind.

6.1.2 *Nachrichtenformat*

CPR_051 Die Nachrichtenformate für die ReadDataByIdentifier-Primitive sind in den folgenden Tabellen aufgeführt.

Tabelle 25

Nachricht ReadDataByIdentifier Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 bis #7	recordDataIdentifier = [ein Wert aus Tabelle 28]	xxxx	RDI_…
#8	Prüfsumme	00-FF	CS

Tabelle 26

Nachricht ReadDataByIdentifier Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 und #7	recordDataIdentifier = [gleicher Wert wie Bytes 6 und 7 in Tabelle 25]	xxxx	RDI_...
#8 bis #m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Prüfsumme	00-FF	CS

Tabelle 27

Nachricht ReadDataByIdentifier Negative Response

Byte-Nr.	Parameterbezeichnung		Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung		80	FMT
#2	Zieladress-Byte		tt	TGT
#3	Quelladress-Byte		EE	SRC
#4	Zusatzlängen-Byte		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	ReadDataByIdentifier Request Service Id		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Prüfsumme		00-FF	CS

6.1.3 *Parameterdefinition*

CPR_052 Der Parameter ***recordDataIdentifier (RDI_)*** in der Anforderungsnachricht ReadDataByIdentifier kennzeichnet einen Datensatz.

CPR_053 Die hier definierten Werte für recordDataIdentifier sind in der folgenden Tabelle aufgeführt.

Die Tabelle recordDataIdentifier enthält 4 Spalten mit mehreren Zeilen.

— Die **1. Spalte (Hex)** enthält jeweils den hexadezimalen Wert für die in der 3. Spalte angeführte Anforderungsnachricht recordDataIdentifier.

— Die **2. Spalte (Datenelement)** gibt zum jeweiligen recordDataIdentifier das Datenelement gemäß Anlage 1 an (ggf. Umkodierung erforderlich).

— Die **3. Spalte (Beschreibung)** enthält den dazugehörigen Namen des recordDataIdentifier.

— Die **4. Spalte (Symbolform)** gibt die Symbolschreibweise des jeweiligen recordDataIdentifier an.

Tabelle 28

Definition der Werte für recordDataIdentifier

Hex	Datenelement	Name recordDataIdentifier (siehe Format in Abschnitt 8.2)	Symbolform
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Datenelement	Name recordDataIdentifier (siehe Format in Abschnitt 8.2)	Symbolform
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Der Parameter ***dataRecord (DREC_)*** dient der Nachricht Positive Response auf ReadDataByIdentifier dazu, dem Client (Prüfgerät) den durch die recordDataIdentifier gekennzeichneten Datensatz bereitzustellen. Die Datensatzformate werden in Abschnitt 8 definiert. Es können zusätzliche, vom Benutzer wählbare dataRecord-Werte, z. B. VU-abhängige Eingabedaten, interne Daten und Ausgabedaten integriert werden, diese werden jedoch hier nicht definiert.

6.2. **Der Dienst WriteDataByIdentifier**

6.2.1 *Beschreibung der Nachricht*

CPR_056 Der Dienst WriteDataByIdentifier dient dem Client dazu, Datensatzwerte auf einen Server zu schreiben, die durch einen recordDataIdentifier gekennzeichnet sind. Der Fahrzeughersteller muss dafür sorgen, dass die Serverbedingungen zur Abwicklung dieses Dienstes erfüllt sind. Zur Aktualisierung der in Tabelle 28 aufgeführten Parameter muss sich die VU in der Betriebsart KALIBRIERUNG befinden.

6.2.2 *Nachrichtenformat*

CPR_057 Die Nachrichtenformate für die WriteDataByIdentifier-Primitive sind in den folgenden Tabellen aufgeführt.

Tabelle 29

Nachricht WriteDataByIdentifier Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 bis #7	recordDataIdentifier = [ein Wert aus Tabelle 28]	xxxx	RDI_…

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#8 bis m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Prüfsumme	00-FF	CS

Tabelle 30

Nachricht WriteDataByIdentifier Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 bis #7	recordDataIdentifier = [gleicher Wert wie Bytes 6 und 7 in Tabelle 29]	xxxx	RDI_…
#8	Prüfsumme	00-FF	CS

Tabelle 31

Nachricht WriteDataByIdentifier Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI

Byte-Nr.	Parameterbezeichnung		Hex-Wert	Symbolform
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Prüfsumme		00-FF	CS

6.2.3 *Parameterdefinition*

Der Parameter ***recordDataIdentifier (RDI_)*** ist in Tabelle 28 definiert.

Der Parameter ***dataRecord (DREC_)*** dient der Anforderungsnachricht WriteDataByIdentifier dazu, dem Server (VU) den durch die recordDataIdentifier gekennzeichneten Datensatzwerte bereitzustellen. Die Datensatzformate werden in Abschnitt 8 definiert.

7. PRÜFIMPULSSTEUERUNG — FUNKTIONSEINHEIT EINGABE/AUSGABE-STEUERUNG

Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 32

Funktionseinheit Eingabe/Ausgabe-Steuerung

Name des Dienstes	Beschreibung
InputOutputControlByIdentifier	Der Client fordert die Steuerung einer speziellen Eingabe/Ausgabe für den Server an.

7.1. Der Dienst InputOutputControlByIdentifier

7.1.1 *Beschreibung der Nachricht*

Über einen der Steckanschlüsse an der Vorderseite ist es möglich, Prüfimpulse mit einem geeigneten Prüfgerät zu steuern bzw. zu überwachen.

CPR_058 Diese Kalibrierungs-E/A-Signalleitung ist mit einem K-Leitungsbefehl konfigurierbar, wobei mit dem Dienst InputOutputControlByIdentifier die für die Leitung gewünschte Eingabe- bzw. Ausgabefunktion gewählt wird. Es gibt folgende Leitungszustände:

— deaktiviert,

— speedSignalInput: über die Kalibrierungs-E/A-Signalleitung wird ein Geschwindigkeitssignal (Testsignal) eingegeben, das das Geschwindigkeitssignal des Bewegungssensors ersetzt, diese Funktion ist in der Betriebsart KONTROLLE nicht verfügbar,

— realTimeSpeedSignalOutputSensor: über die Kalibrierungs-E/A-Signalleitung wird das Geschwindigkeitssignal des Bewegungssensors ausgegeben,

— RTCOutput: über die Kalibrierungs-E/A-Signalleitung wird das UTC-Zeitsignal ausgegeben, diese Funktion ist in der Betriebsart KONTROLLE nicht verfügbar.

CPR_059 Um den Leitungsstatus zu konfigurieren, muss sich die Fahrzeugeinheit in einem Einstellvorgang befinden und in die Betriebsart KALIBRIERUNG oder KONTROLLE gesetzt sein. Wenn sich die VU in der Betriebsart KALIBRIERUNG befindet, stehen die vier Leitungsstati zur Verfügung (deaktiviert, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Wenn sich die VU in der Betriebsart KONTROLLE befindet, stehen nur zwei Leitungsstati zur Verfügung (deaktiviert, realTimeSpeedOutputSensor). Bei Verlassen des Einstellvorgangs bzw. der Betriebsart KALIBRIERUNG oder KONTROLLE muss die Fahrzeugeinheit die Rückkehr der E/A-Signalleitung in den Status „deaktiviert" (Standardzustand) gewährleisten.

CPR_060 Treffen an der Echtzeit-Eingabeleitung für Geschwindigkeitssignale der VU Geschwindigkeitsimpulse ein, während die E/A-Signalleitung auf Eingabe gesetzt ist, muss die E/A-Signalleitung auf Ausgabe gesetzt werden oder in den deaktivierten Zustand zurückkehren.

CPR_061 Der Ablauf muss wie folgt sein:

— Aufbau der Verbindung durch den Dienst StartCommunication

— Einleiten eines Einstellvorgangs durch den Dienst StartDiagnosticSession und Eintritt in die Betriebsart KALIBRIERUNG oder KONTROLLE (die Reihenfolge dieser beiden Vorgänge ist nicht von Bedeutung).

— Änderung des Ausgabestatus durch den Dienst InputOutputControlByIdentifier.

7.1.2 *Nachrichtenformat*

CPR_062 Die Nachrichtenformate für die InputOutputControlByIdentifier-Primitive sind in den folgenden Tabellen spezifiziert.

Tabelle 33

Nachricht InputOutputControlByIdentifier Request

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	xx	LEN
#5	**InputOutputControlByIdentifier Request SId**	**2F**	**IOCBI**
#6 und #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 oder	ControlOptionRecord = [		COR_…
#8 bis #9	inputOutputControlParameter — ein Wert aus Tabelle 36	xx	IOCP_…
	controlState — ein Wert aus Tabelle 37 (siehe Hinweis unten)]	xx	CS_…
#9 oder #10	Prüfsumme	00-FF	CS

Hinweis: Der Parameter controlState liegt nur in bestimmten Fällen vor (siehe 7.1.3).

Tabelle 34

Nachricht InputOutputControlByIdentifier Positive Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	xx	LEN
#5	**InputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 und #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 oder #8 bis #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (gleicher Wert wie Byte 8 in Tabelle 33)	xx	IOCP_…
	controlState (gleicher Wert wie Byte 9 in Tabelle 33)] (falls zutreffend)	xx	CS_…
#9 oder #10	Prüfsumme	00-FF	CS

Tabelle 35

Nachricht InputOutputControlByIdentifier Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Prüfsumme	00-FF	CS

7.1.3 *Parameterdefinition*

CPR_064 Der Parameter ***inputOutputControlParameter (IOCP_)*** ist in folgender Tabelle beschrieben.

Tabelle 36

Definition der Werte für inputOutputControlParameter

Hex	Beschreibung	Symbolform
00	**ReturnControlToECU** Dieser Wert zeigt dem Server (VU) an, dass das Prüfgerät die Steuerung der Kalibrierungs-E/A-Signalleitung beendet hat.	RCTECU
01	**ResetToDefault** Dieser Wert zeigt dem Server (VU) die Anforderung an, die Kalibrierungs-E/A-Signalleitung in den Standardstatus zurückzusetzen.	RTD
03	**ShortTermAdjustment** Dieser Wert zeigt dem Server (VU) die Anforderung an, die Kalibrierungs-E/A-Signalleitung auf den im Parameter controlState enthaltenen Wert einzustellen.	STA

CPR_065 Der Parameter ***controlState*** liegt nur vor, wenn der inputOutputControlParameter auf ShortTermAdjustment gesetzt ist; folgende Werte sind möglich:

Tabelle 37

Definition der Werte für controlState

Betriebsart	Hex-Wert	Beschreibung
Deaktiviert	00	E/A-Leitung deaktiviert (Ausgangszustand)
Aktiviert	01	Kalibrierungs-E/A-Leitung als speedSignalInput aktiviert
Aktiviert	02	Kalibrierungs-E/A-Leitung als realTimeSpeedSignalOutputSensor aktiviert
Aktiviert	03	Kalibrierungs-E/A-Leitung als RTCOutput aktiviert

8. DATARECORDS-FORMATE

Dieser Abschnitt enthält:

— allgemeine Regeln für die Parameter, die von der Fahrzeugeinheit zum Prüfgerät übertragen werden,

— die Beschreibung der Formate für die in 6 erläuterten Datenübertragungsdienste.

CPR_067 Alle hier angegebenen Parameter müssen von der VU unterstützt werden.

CPR_068 Von der VU an das Prüfgerät aufgrund einer Anforderungsnachricht übertragene Daten müssen dem jeweiligen Messtyp entsprechen (d. h. dem aktuellen Wert des angeforderten Parameters, wie ihn die VU gemessen oder vorgegeben hat).

8.1. **Wertebereiche der übertragenen Parameter**

CPR_069 Tabelle 38 enthält die Wertebereiche, mit deren Hilfe die Gültigkeit der übermittelten Parameter festgestellt wird.

CPR_070 Mit den Werten im Bereich „Fehlerindikator“ kann die Fahrzeugeinheit sofort mitteilen, dass aufgrund eines Fehlers im Fahrtenschreiber derzeit keine gültigen Werte vorhanden sind.

CPR_071 Mit den Werten im Bereich „Nicht verfügbar“ kann die Fahrzeugeinheit eine Nachricht übermitteln, die einen in diesem Modul nicht verfügbaren oder nicht unterstützten Parameter enthält. Die Werte im Bereich „Nicht angefordert“ ermöglichen es der Fahrzeugeinheit, eine Befehlsnachricht zu übermitteln und die Parameter anzugeben, für die es vom anderen Gerät keine Antwort erwartet.

CPR_072 Können wegen eines defekten Bauteils keine gültigen Daten für einen Parameter übermittelt werden, sollte mit dem in Tabelle 38 angegebenen Fehlerindikator anstelle von Daten für den angeforderten Parameter geantwortet werden. Wenn die gemessenen oder errechneten Daten Werte annehmen, die zwar gültig sind, aber außerhalb des festgelegten Wertebereichs für diesen Parameter liegen, ist der Fehlerindikator jedoch nicht zu verwenden. In diesem Fall sollte der jeweilige Mindest- oder Höchstwert für diesen Parameter übertragen werden.

Tabelle 38

Wertebereiche der dataRecords

Wertebereichsname	1 Byte (Hex-Wert)	2 Bytes (Hex-Wert)	4 Bytes (Hex-Wert)	ASCII
Gültiges Signal	00 bis FA	0000 bis FAFF	00000000 bis FAFFFFFF	1 bis 254
Parameterspezifischer Indikator	FB	FB00 bis FBFF	FB000000 bis FBFFFFFF	keiner
Reserviert für zukünftige Indikatorbits	FC bis FD	FC00 bis FDFF	FC000000 bis FDFFFFFF	keiner
Fehlerindikator	FE	FE00 bis FEFF	FE000000 bis FEFFFFFF	0
Nicht verfügbar oder nicht angefordert	FF	FF00 bis FFFF	FF000000 bis FFFFFFFF	FF

CPR_073 Bei den in ASCII dargestellten Parametern ist der Stern „*“ als Trennzeichen reserviert.

8.2. **dataRecords-Formate**

In Tabelle 39 bis Tabelle 42 sind die Datensatzformate für die Dienste ReadDataByIdentifier und WriteDataByIdentifier angegeben.

CPR_074 In Tabelle 39 sind Länge, Auflösung und Betriebsbereich für jeden durch seinen recordDataIdentifier gekennzeichneten Parameter angegeben:

Tabelle 39

dataRecords-Formate

Parameterbezeichnung	Datenlänge (Bytes)	Auflösung	Betriebsbereich
TimeDate	8	siehe Tabelle 40	
HighResolutionTotalVehicleDistance	4	Zuwachs 5 m/Bit, Ausgangswert 0 m	0 bis +21 055 406 km
Kfactor	2	Zuwachs 0,001 Impulse/m/Bit, Ausgangswert 0	0 bis 64,255 Impulse/m
LfactorTyreCircumference	2	Zuwachs 0,125 10^{-3} m/Bit, Ausgangswert 0	0 bis 8,031 m
WvehicleCharacteristicFactor	2	Zuwachs 0,001 Impulse/m/Bit, Ausgangswert 0	0 bis 64,255 Impulse/m
TyreSize	15	ASCII	ASCII

Parameterbezeichnung	Datenlänge (Bytes)	Auflösung	Betriebsbereich
NextCalibrationDate	3	siehe Tabelle 41	
SpeedAuthorised	2	Zuwachs 1/256 km/h/Bit, Ausgangswert 0	0 bis 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	siehe Tabelle 42	
VIN	17	ASCII	ASCII

CPR_075 Tabelle 40 enthält die Formate der verschiedenen Bytes für den Parameter TimeDate:

Tabelle 40

Ausführliches Format des Parameters TimeDate (recordDataIdentifier-Wert F90B)

Byte	Parameterdefinition	Auflösung	Betriebsbereich
1	Sekunden	Zuwachs 0,25 s/Bit, Ausgangswert 0 s	0 bis 59,75 s
2	Minuten	Zuwachs 1 min/Bit, Ausgangswert 0 min	0 bis 59 min
3	Stunden	Zuwachs 1 h/Bit, Ausgangswert 0 h	0 bis 23 h
4	Monat	Zuwachs 1 Monat/Bit, Ausgangswert 0 Monate	1 bis 12 Monate
5	Tag	Zuwachs 0,25 Tag/Bit, Ausgangswert 0 Tage (siehe Hinweis unter Tabelle 41)	0,25 bis 31,75 Tage
6	Jahr	Zuwachs 1 Jahr/Bit, Ausgangswert + 1985 Jahre (siehe Hinweis unter Tabelle 41)	1985 bis 2235 Jahre
7	Lokaler Ausgangswert Minuten	Zuwachs 1 min/Bit, Ausgangswert – 125 h	– 59 bis + 59 min
8	Lokaler Ausgangswert Stunden	Zuwachs 1 h/Bit, Ausgangswert – 125 h	– 23 bis + 23 h

CPR_076 Tabelle 41 enthält die Formate der verschiedenen Bytes für den Parameter NextCalibrationDate.

Tabelle 41

Ausführliches Format des Parameters NextCalibrationDate (recordDataIdentifier-Wert F922)

Byte	Parameterdefinition	Auflösung	Betriebsbereich
1	Monat	Zuwachs 1 Monat/Bit, Ausgangswert 0 Monate	1 bis 12 Monate
2	Tag	Zuwachs 0,25 Tag/Bit, Ausgangswert 0 Tage (siehe Hinweis unten)	0,25 bis 31,75 Tage
3	Jahr	Zuwachs 1 Jahr/Bit, Ausgangswert + 1985 Jahre (siehe Hinweis unten)	1985 bis 2235 Jahre

Hinweis zur Verwendung des Tag-Parameters:

1) Der Datumswert 0 ist ungültig. Die Werte 1, 2, 3 und 4 kennzeichnen den ersten Tag des Monats; die Werte 5, 6, 7 und 8 kennzeichnen den zweiten Tag des Monats usw.

2) Dieser Parameter hat keinen Einfluss auf den Stundenparameter oben.

Hinweis zur Verwendung des Jahr-Parameterbits:

Der Wert 0 für das Jahr kennzeichnet das Jahr 1985; der Wert 1 das Jahr 1986 usw.

CPR_078 Tabelle 42 enthält die Formate der verschiedenen Bytes für den Parameter VehicleRegistrationNumber:

Tabelle 42

Ausführliches Format des Parameters VehicleRegistrationNumber (recordDataIdentifier-Wert F97E)

Byte	Parameterdefinition	Auflösung	Betriebsbereich
1	Codeseite (entsprechend Anlage 1)	ASCII	01 bis 0A
2 bis 14	amtliches Kennzeichen (entsprechend Anlage 1)	ASCII	ASCII

Anlage 9.

TYPGENEHMIGUNG UND MINDESTANFORDERUNGEN AN DIE DURCHZUFÜHRENDEN PRÜFUNGEN

INHALTSVERZEICHNIS

1. EINLEITUNG 309
2. FUNKTIONSPRÜFUNGEN AN DER FAHRZEUGEINHEIT 311
3. FUNKTIONSTESTS AM BEWEGUNGSSENSOR 315
4. FUNKTIONSPRÜFUNGEN AN FAHRTENSCHREIBERKARTEN 318
5. PRÜFUNG EXTERNER GNSS-AUSRÜSTUNG 328
6. PRÜFUNGEN DER AUSRÜSTUNG ZUR FERNKOMMUNIKATION 331
7. PAPIERFUNKTIONSPRÜFUNGEN 333
8. INTEROPERABILITÄTSPRÜFUNGEN 335

1. EINLEITUNG

1.1. **Typgenehmigung**

Die EG-Typgenehmigung von Kontrollgeräten (oder deren Komponenten) oder einer Fahrtenschreiberkarte beruht auf:

— einer **Sicherheitszertifizierung** auf Grundlage der Spezifizierung Allgemeiner Kriterien anhand einer Sicherheitsvorgabe in völliger Übereinstimmung mit Anlage 10 dieses Anhangs (fertigzustellen/zu ändern),

— einer **Funktionszertifizierung** durch die Behörde eines Mitgliedstaates, mit der bestätigt wird, dass das geprüfte Teil hinsichtlich der ausgeführten Funktionen, der Messgenauigkeit und der Umwelteigenschaften die Anforderungen dieses Anhangs erfüllt,

— einer **Interoperabilitätszertifizierung** durch die zuständige Stelle, mit der bestätigt wird, dass das Kontrollgerät (oder die Fahrtenschreiberkarte) mit dem erforderlichen Muster der Fahrtenschreiberkarte (bzw. des Kontrollgeräts) (siehe Kapitel 8 in diesem Anhang) uneingeschränkt interoperabel ist.

In dieser Anlage ist in Form von Mindestanforderungen festgelegt, welche Prüfungen eine Behörde der Mitgliedstaaten während der Funktionsprüfungen und welche Prüfungen eine zuständige Stelle während der Interoperabilitätsprüfungen durchführen muss. Die Verfahren zur Durchführung der Prüfungen bzw. die Art der Prüfungen werden nicht weiter spezifiziert.

Die Aspekte der Sicherheitszertifizierung sind in dieser Anlage nicht enthalten. Werden bestimmte Prüfungen bereits für die Typgenehmigung im Rahmen des Verfahrens zur Sicherheitsbewertung und -zertifizierung durchgeführt, so brauchen diese Prüfungen nicht wiederholt zu werden. In diesem Fall sind lediglich die Ergebnisse dieser Sicherheitsprüfungen nachzuprüfen. Zu Informationszwecken sind in dieser Anlage Anforderungen, bei denen während der Sicherheitszertifizierung die Durchführung einer Prüfung erwartet wird (oder die mit durchzuführenden Prüfungen in einem engen Verhältnis stehen), mit einem „*“ gekennzeichnet.

Die nummerierten Randnummern beziehen sich auf den Hauptteil des Anhangs, während sich die übrigen Anforderungen auf die übrigen Anlagen beziehen (Beispiel: PIC_001 bezieht sich auf Anforderung PIC_001 von Anlage 3 Piktogramme).

In dieser Anlage werden die Typgenehmigungen für den Bewegungssensor, für die Fahrzeugeinheit und für die externe GNSS-Ausrüstung getrennt betrachtet, da es sich dabei um Komponenten des Kontrollgeräts handelt. Jede Komponente enthält eine eigene Typgenehmigung, in der die anderen kompatiblen Komponenten angegeben werden. Die Funktionsprüfung des Bewegungssensors (bzw. der externen GNSS-Ausrüstung) erfolgt zusammen mit der Fahrzeugeinheit und umgekehrt.

Eine Interoperabilität zwischen sämtlichen Bewegungssensormodellen (bzw. externen GNSS-Ausrüstungen) und sämtlichen Fahrzeugeinheitmodellen ist nicht erforderlich. In einem solchen Fall kann die Typgenehmigung für einen Bewegungssensor (bzw. externe GNSS-Ausrüstung) nur in Kombination mit der Typgenehmigung für die relevante Fahrzeugeinheit bzw. umgekehrt erteilt werden.

1.2. **Referenzdokumente**

In dieser Anlage werden folgende Referenzdokumente herangezogen:

IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold (Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte)

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme) (sinusförmig).

IEC 60068-2-6: Environmental testing — Part 2: Tests — Test Fc: Vibration (sinusoidal) (Umgebungseinflüsse — Teil 2-6: Prüfverfahren — Prüfung Fc: Schwingen (sinusförmig)

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature (Umgebungseinflüsse — Teil 2-14: Prüfverfahren — Prüfung N: Temperaturwechsel)

IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock (Umgebungseinflüsse; Teil 2-27: Prüfverfahren — Prüfung Ea und Leitfaden: Schocken)

IEC 60068-2-30: Environmental testing — Part 2-30: Tests — Test Db: Damp heat, cyclic (12 h + 12 h cycle) (Umgebungseinflüsse — Teil 2-30: Prüfverfahren — Prüfung Db: Feuchte Wärme, zyklisch (12 + 12 Stunden))

IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance (Umgebungseinflüsse — Teil 2-64: Prüfverfahren — Prüfung Fh: Schwingen, Breitbandrauschen (digital geregelt) und Leitfaden)

IEC 60068-2-78 Environmental testing — Part 2-78: Tests — Test Cab: Damp heat, steady state (Umgebungseinflüsse — Teil 2-78: Prüfverfahren — Prüfung Cab: Feuchte Wärme, konstant)

ISO 16750-3 — Mechanical loads (2012-12) (Mechanische Beanspruchungen)

ISO 16750-4 — Climatic loads (2010-04) (Klimatische Beanspruchungen).

ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Straßenfahrzeuge — Schutzarten (IP-Code) — Schutz gegen fremde Objekte, Wasser und Kontakt — Elektrische Ausrüstungen)

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles — Test methods for electrical disturbances from electrostatic discharge (Straßenfahrzeuge — Prüfverfahren für elektrische Störungen durch elektrostatische Entladungen)

ISO 7637-1:2002 + AMD1: 2008 Road vehicles — Electrical disturbances from conduction and coupling — Part 1: Definitions and general considerations (Straßenfahrzeuge; Elektrische Störungen durch Leitung und Kopplung — Teil 1: Allgemeines und Definitionen).

ISO 7637-2 Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines only (Straßenfahrzeuge — Elektrische Störungen durch Leitung und Kopplung — Teil 2: Elektrische, leitungsgeführte Störungen auf Versorgungsleitungen).

ISO 7637-3 Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines (Straßenfahrzeuge — Elektrische Störungen durch Leitung und Kopplung — Kapazitiv und induktiv gekoppelte Störungen auf andere als Versorgungsleitungen).

ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics (Identifikationskarten — Chipkarten mit Kontakten — Teil 1: Physikalische Eigenschaften).

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts (Identifikationskarten — Chipkarten — Karten mit Kontakten — Teil 2: Maße und Anordnung der Kontakte).

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol (Chipkarten mit Kontakten — Teil 3: Elektronische Eigenschaften und Übertragungsprotokolle).

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards — Test methods — Part 1: General characteristics (Identifikationskarten — Prüfverfahren — Teil 1: Generelle Eigenschaften).

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices (Identifikationskarten — Prüfverfahren — Teil 3: Chipkarten mit Kontakten und zugehörige Schnittstellen-Geräte)

ISO 16844-3:2004, Cor 1:2006 Road vehicles — Tachograph systems — Part 3: Motion sensor interface (with vehicle units) (Straßenfahrzeuge — Fahrtschreiber (Kontrollgeräte) — Teil 3: Schnittstelle Bewegungssensor).

ISO 16844-4 Road vehicles — Tachograph systems — Part 4: CAN interface (Straßenfahrzeuge — Fahrtschreiber (Kontrollgeräte) — Teil 4: CAN-Schnittstelle).

ISO 16844-6 Road vehicles — Tachograph systems — Part 6: Diagnostics (Straßenfahrzeuge — Fahrtschreiber (Kontrollgeräte) — Teil 6: Diagnose)

ISO 16844-7 Road vehicles — Tachograph systems — Part 7: Parameter

ISO 534 Paper and board – Determination of thickness, density and specific volume (Papier und Pappe — Bestimmung der Dicke, der Dichte und des spezifischen Volumens)

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe) (Regelung der Wirtschaftskommission für Europa bei den Vereinten Nationen über einheitliche technische Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der elektromagnetischen Verträglichkeit

2. FUNKTIONSPRÜFUNGEN AN DER FAHRZEUGEINHEIT

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1	**Administrative Prüfung**		
1.1	Dokumentation	Richtigkeit der Dokumentation	
1.2	Prüfergebnisse des Herstellers	Ergebnisse der beim Einbau vom Hersteller durchgeführten Prüfung. Nachweis auf Papier.	88, 89, 91
2	**Sichtprüfung**		
2.1	Übereinstimmung mit der Dokumentation		
2.2	Kennung/Markierungen		224 bis 226
2.3	Werkstoffe		219 bis 223
2.4	Plombierung		398, 401 bis 405
2.5	Externe Schnittstellen		
3	**Funktionsprüfungen**		
3.1	Mögliche Funktionen		03, 04, 05, 07, 382
3.2	Betriebsarten		09 bis 11*, 132, 133
3.3	Funktionen und Datenzugriffsrechte		12* 13*, 382, 383, 386 bis 389
3.4	Überwachung des Einsteckens und Entnehmens der Karten		15, 16, 17, 18, 19*, 20*, 132
3.5	Geschwindigkeits- und Wegstreckenmessung		21 bis 31
3.6	Zeitmessung (Prüfung bei 20 °C)		38 bis 43
3.7	Überwachung der Fahrertätigkeiten		44 bis 53, 132
3.8	Überwachung des Status der Fahrzeugführung		54, 55, 132

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
3.9	Manuelle Eingabe durch die Fahrer		56 bis 62
3.10	Verwaltung der Unternehmenssperren		63 bis 68
3.11	Überwachung von Kontrollaktivitäten		69, 70
3.12	Feststellung von Ereignissen und Störungen		71 bis 88 132
3.13	Kenndaten der Fahrzeugeinheit		93*, 94*, 97, 100
3.14	Einsteck- und Entnahmedaten der Fahrerkarte		102* bis 104*
3.15	Fahrertätigkeitsdaten		105* bis 107*
3.16	Orts- und Positionsdaten		108* bis 112*
3.17	Kilometerstandsdaten		113* bis 115*
3.18	Detaillierte Geschwindigkeitsdaten		116*
3.19	Ereignisdaten		117*
3.20	Störungsdaten		118*
3.21	Kalibrierungsdaten		119* bis 121*
3.22	Zeiteinstellungsdaten		124*, 125*
3.23	Kontrolldaten		126*, 127*
3.24	Unternehmenssperredaten		128*
3.25	Erfassen des Herunterladens		129*
3.26	Daten zu spezifischen Bedingungen		130*, 131*
3.27	Aufzeichnung und Speicherung von Daten auf Fahrtenschreiberkarten		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Anzeige		90, 132, 149 bis 166, PIC_001, DIS_001
3.29	Drucken		90, 132, 167 bis 179, PIC_001, PRT_001 bis PRT_014
3.30	Warnung		132, 180 bis 189, PIC_001

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
3.31	Herunterladen von Daten auf externe Datenträger		90, 132, 190 bis 194
3.32	Fernkommunikation für gezielte Straßenkontrollen		195 bis 197
3.33	Datenausgabe an zusätzliche externe Geräte		198, 199
3.34	Kalibrierung		202 bis 206*, 383, 384, 386 bis 391
3.35	Kalibrierungskontrolle unterwegs:		207 bis 209
3.36	Zeiteinstellung		210 bis 212*
3.37	Störungsfreiheit zusätzlicher Funktionen		06, 425
3.38	Bewegungssensor-Schnittstelle		02, 122
3.39	Externe GNSS-Ausrüstung		03, 123
3.40	Überprüfen, dass die VU die herstellerdefinierten Ereignisse und/oder Störungen ermittelt, aufzeichnet und speichert, wenn ein gekoppelter Bewegungssensor auf Magnetfelder reagiert, die die Ermittlung von Fahrzeugbewegungsdaten stören		217
3.41	Ziffernfolge und standardisierte Domänenparameter		CSM_48, CSM_50
4	**Umweltprüfungen**		
4.1	Temperatur	Funktionsprüfung durch: Prüfung gemäß ISO 16750-4, Kapitel 5.1.1.2: Betriebsprüfung bei niedrigen Temperaturen (72 h @ – 20 °C) Diese Prüfung bezieht sich auf IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold (Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte) Prüfung gemäß ISO 16750-4, Kapitel 5.1.2.2: Betriebsprüfung bei hohen Temperaturen (72 h @ 70 °C) Diese Prüfung bezieht sich auf IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme) Prüfung gemäß ISO 16750-4, Kapitel 5.3.2: Schnelle Temperaturwechsel mit angegebener Übergangsdauer (– 20 °C/70 °C, 20 Zyklen, Haltezeit 2 h bei jeder Temperatur) In Bezug auf Mindest- und Höchsttemperatur sowie während der Temperaturzyklen ist (für die in Abschnitt 3 dieser Tabelle aufgeführten Prüfungen) eine geringere Anzahl an Prüfungen zulässig	213

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.2	Luftfeuchtigkeit	IEC 60068-2-30, Prüfung Db, zum Nachweis, dass die Fahrzeugeinheit einer zyklischen Feuchtigkeitsprüfung (Wärmeprüfung) von sechs 24-Std.-Zyklen jeweils mit einer Temperaturänderung von + 25 °C bis + 55 °C und einer relativen Luftfeuchtigkeit von 97 % bei + 25 °C bzw. entsprechend 93 % bei + 55 °C standhält	214
4.3	Mechanisch	1. Sinusschwingungen. Nachweis, dass die Fahrzeugeinheit Sinusschwingungen mit folgenden Merkmalen standhält: konstante Verschiebung zwischen 5 und 11 Hz: max. 10 mm konstante Beschleunigung zwischen 11 und 300 Hz: 5 g Nachweis nach IEC 60068-2-6, Prüfung Fc, mit Mindestprüfdauer von 3 × 12 Std. (12 Std. je Achse) ISO 16750-3 schreibt für Geräte, die sich in einer entkoppelten Fahrerkabine befinden, keine Prüfung mit Sinusschwingungen vor. 2. Zufallsschwingungen: Prüfung gemäß ISO 16750-3, Kapitel 4.1.2.8: Prüfung VIII: Nutzfahrzeug, entkoppelte Fahrerkabine Prüfung mit regellosem Schwingen, 10…2 000 Hz, RMS vertikal 21,3 m/s², RMS longitudinal 11,8 m/s², RMS lateral 13,1 m/s², 3 Achsen, 32 Std. je Achse, einschließlich Temperaturzyklus – 20…70 °C. Diese Prüfung bezieht sich auf IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance (Umgebungseinflüsse — Teil 2-64: Prüfverfahren — Prüfung Fh: Schwingen, Breitbandrauschen (digital geregelt) und Leitfaden) 3. Stöße: mechanische Stöße mit 3 g Halbsinus gemäß ISO 16750. Diese Prüfungen werden an zwei unterschiedlichen Proben des zu prüfenden Gerätetyps durchgeführt.	219
4.4	Schutz vor Wasser und vor Fremdkörpern	Prüfung gemäß ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Straßenfahrzeuge — Schutzarten (IP-Code) — Schutz gegen fremde Objekte, Wasser und Kontakt — elektrische Ausrüstungen) (Keine Parameteränderung); Mindestwert IP 40	220, 221
4.5	Überspannungsschutz	Nachweis, dass die Fahrzeugeinheit folgende Versorgungsspannungen aushält: 24-V-Versionen: 34 V bei + 40 °C 1 Stunde 12-V-Versionen: 17 V bei + 40 °C 1 Stunde (ISO 16750-2)	216
4.6	Falschpolungsschutz	Nachweis, dass die Fahrzeugeinheit einer Umkehrung der Polarität der Stromversorgung standhält (ISO 16750-2)	216

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.7	Kurzschlussschutz	Nachweis, dass für Eingangs-/Ausgangssignale Schutz vor Kurzschluss der Stromversorgung und vor Erdschluss besteht (ISO 16750-2)	216
5	**EMV-Prüfungen**		
5.1	Störaussendung und Störanfälligkeit	Einhaltung von ECE-Regelung R10	218
5.2	Elektrostatische Entladung	Einhaltung von ISO 10605:2008 + Technische Korrektur:2010 + AMD1:2014: +/– 4 kV Kontaktentladung und +/– 8 kV Luftentladung	218
5.3	Leitungsgeführte Störgrößen auf Versorgungsleitungen	24-V-Versionen: Einhaltung von ISO 7637-2 + ECE-Verordnung 10 Rev. 3: Impuls 1a: Vs = – 450 V Ri = 50 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 20V Ri = 0,05 Ohm Impuls 3a: Vs = – 150V Ri = 50 Ohm Impuls 3b: Vs = + 150V Ri = 50 Ohm Impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms Impuls 5: Vs = + 120 V Ri = 2,2 Ohm td = 250 ms 12-V-Versionen: Einhaltung von ISO 7637-1 + ECE-Verordnung 10 Rev. 3: Impuls 1: Vs = – 75V Ri = 10 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 10V Ri = 0,05 Ohm Impuls 3a: Vs = – 112V Ri = 50 Ohm Impuls 3b: Vs = + 75V Ri = 50 Ohm Impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms Impuls 5: Vs = + 65 V Ri = 3 Ohm td = 100 ms Impuls 5 ist nur in Fahrzeugeinheiten zu prüfen, die in Fahrzeugen installiert werden sollen, für die keine gemeinsame externe Blindlast vorgesehen ist Blindlastvorschläge siehe ISO 16750-2, 4. Ausgabe, Kapitel 4.6.4.	218

3. FUNKTIONSTESTS AM BEWEGUNGSSENSOR

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1.	**Administrative Prüfung**		
1.1	Dokumentation	Richtigkeit der Dokumentation	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
2.	**Sichtprüfung**		
2.1.	Übereinstimmung mit der Dokumentation		
2.2.	Kennung/Markierungen		225, 226,
2.3	Werkstoffe		219 bis 223
2.4.	Plombierung		398, 401 bis 405
3.	**Funktionsprüfungen**		
3.1	Kenndaten des Sensors		95 bis 97*
3.2	Koppelung des Bewegungssensors mit der Fahrzeugeinheit		122*, 204
3.3	Bewegungserkennung Bewegungsmessgenauigkeit		30 bis 35
3.4	VU-Schnittstelle		02
3.5	Überprüfen, dass der Bewegungssensor gegenüber konstanten Magnetfeldern unempfindlich ist. Andernfalls überprüfen, dass der Bewegungssensor auf konstante Magnetfelder reagiert, die die Ermittlung von Fahrzeugbewegungsdaten stören, sodass eine verbundene VU Sensorstörungen ermitteln, aufzeichnen und speichern kann		217
4.	**Umweltprüfungen**		
4.1	Betriebstemperatur	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) im Temperaturbereich [– 40 °C; + 135 °C] anhand: IEC 60068-2-1, Prüfung Ad, Prüfdauer 96 Std. bei Mindesttemperatur To_{min}, IEC 60068-2-2 Prüfung Bd, Prüfdauer 96 Std. bei Höchsttemperatur To_{max} Prüfung gemäß ISO 16750-4, Kapitel 5.1.1.2: Betriebsprüfung bei niedrigen Temperaturen (24 h @ – 40 °C) Diese Prüfung bezieht sich auf IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold (Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte) IEC 68-2-2 Prüfung Bd, Prüfdauer 96 Std. bei Mindesttemperatur – 40 °C. Prüfung gemäß ISO 16750-4, Kapitel 5.1.2.2: Betriebsprüfung bei hohen Temperaturen (96 h @ 135 °C) Diese Prüfung bezieht sich auf IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme)	213

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.2	Temperaturzyklen	Prüfung gemäß ISO 16750-4, Kapitel 5.3.2: Schneller Temperaturwechsel mit angegebener Übergangsdauer (– 40 °C/135 °C, 20 Zyklen, Haltezeit 30 min bei jeder Temperatur) IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature (Umgebungseinflüsse — Teil 2-14: Prüfverfahren — Prüfung N: Temperaturwechsel)	213
4.3	Luftfeuchtigkeitszyklen	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) anhand IEC 60068-2-30, Prüfung Db, sechs 24-Std.-Zyklen, jeweils mit einer Temperaturänderung von + 25 °C bis + 55 °C und einer relativen Luftfeuchtigkeit von 97 % bei + 25 °C bzw. entsprechend 93 % bei + 55 °C	214
4.4	Schwingungen	ISO 16750-3, Kapitel 4.1.2.6: Prüfung VI: Nutzfahrzeug, Motor, Getriebe Schwingungsprüfung im gemischten Modus einschließlich a) Sinusschwingungsprüfung, 20…520 Hz, 11,4 … 120 m/s^2, <= 0,5 oct/min b) Zufallsschwingungsprüfung, 10…2 000 Hz, RMS 177 m/s^2 94 Std. je Achse, einschließlich Temperaturzyklus – 20…70 °C) Diese Prüfung bezieht sich auf IEC 60068-2-80: Environmental testing — Part 2-80: Tests — Test Fi: Vibration — Mixed mode (Umgebungseinflüsse — Teil 2-80: Prüfverfahren — Prüfung Fi: Schwingungsprüfung im gemischten Modus)	219
4.5	Mechanischer Stoß	ISO 16750-3, Kapitel 4.2.3: Prüfung VI: Prüfung für Geräte in oder auf dem Getriebe Halbsinusstoß, Beschleunigung zu vereinbaren im Bereich 3 000… 15 000 m/s^2, Impulsdauer zu vereinbaren, jedoch < 1 ms, Anzahl an Stößen: zu vereinbaren Diese Prüfung bezieht sich auf IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock (Umgebungseinflüsse; Teil 2-27: Prüfverfahren — Prüfung Ea und Leitfaden: Schocken)	219
4.6	Schutz vor Wasser und vor Fremdkörpern	Prüfung gemäß ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Straßenfahrzeuge — Schutzarten (IP-Code) — Schutz gegen fremde Objekte, Wasser und Kontakt — Elektrische Ausrüstungen) (Zielwert IP 64)	220, 221
4.7	Falschpolungsschutz	Nachweis, dass der Bewegungssensor einer Umkehrung der Polarität der Stromversorgung standhält	216
4.8	Kurzschlussschutz	Nachweis, dass für Eingangs-/Ausgangssignale Schutz vor Kurzschluss der Stromversorgung und vor Erdschluss besteht	216

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
5.	**EMV**		
5.1	Störaussendung und Störanfälligkeit	Überprüfung der Einhaltung von ECE-Regelung R10	218
5.2	Elektrostatische Entladung	Einhaltung von ISO 10605:2008 + Technische Korrektur:2010 + AMD1:2014: +/- 4 kV Kontaktentladung und +/- 8 kV Luftentladung	218
5.3	Anfälligkeit gegenüber leitungsgeführten Störgrößen auf Datenleitungen	24-V-Versionen: Einhaltung von ISO 7637-2 + ECE-Verordnung 10 Rev. 3: Impuls 1a: Vs = – 450 V Ri = 50 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 20V Ri = 0,05 Ohm Impuls 3a: Vs = – 150V Ri = 50 Ohm Impuls 3b: Vs = + 150V Ri = 50 Ohm Impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms Impuls 5: Vs = + 120 V Ri = 2,2 Ohm td = 250 ms 12-V-Versionen: Einhaltung von ISO 7637-1 + ECE-Verordnung 10 Rev. 3: Impuls 1: Vs = – 75V Ri = 10 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 10V Ri = 0,05 Ohm Impuls 3a: Vs = – 112V Ri = 50 Ohm Impuls 3b: Vs = + 75V Ri = 50 Ohm Impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms Impuls 5: Vs = + 65 V Ri = 3 Ohm td = 100 ms Impuls 5 ist nur in Fahrzeugeinheiten zu prüfen, die in Fahrzeugen installiert werden sollen, für die keine gemeinsame externe Blindlast vorgesehen ist Blindlastvorschläge siehe ISO 16750-2, 4. Ausgabe, Kapitel 4.6.4	218

4. FUNKTIONSPRÜFUNGEN AN FAHRTENSCHREIBERKARTEN

Die Prüfungen gemäß diesem Abschnitt 4,

Abschnitt 5 „Protokollprüfungen“,

Abschnitt 6 „Kartenstruktur“ und

Abschnitt 7 „Funktionsprüfungen“

können vom prüfenden oder bescheinigenden Unternehmen während der CC-Sicherheitszertifizierung (Common Criteria bzw. Allgemeine Kriterien für die Bewertung der Sicherheit für Informationstechnologie) für das Chipmodul durchgeführt werden.

Die Prüfungen 2.3 und 4.2 sind identisch. Hierbei handelt es sich um mechanische Prüfungen der Kombination Kartenkörper/Chipmodul. Wenn eine dieser Komponenten (Kartenkörper, Chipmodul) geändert wird, sind diese Prüfungen erforderlich.

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1.	**Administrative Prüfung**		
1.1	Dokumentation	Richtigkeit der Dokumentation	
2	**Kartenkörper**		
2.1	Druckdesign	Gewährleistung, dass sämtliche Schutzanforderungen und die sichtbar anzubringenden Angaben korrekt gedruckt sind und den Vorgaben entsprechen. [Bezeichner] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 227) Die Vorderseite enthält: je nach Kartentyp die großgedruckten Wörter „Fahrerkarte“ oder „Kontrollkarte“ oder „Werkstattkarte“ oder „Unternehmenskarte“ in der Sprache bzw. den Sprachen des ausstellenden Mitgliedstaats; [Name des Mitgliedstaates] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 228) Die Vorderseite enthält: den Namen des Mitgliedstaats, der die Karte ausstellt (fakultativ). [Zeichen] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 229) Die Vorderseite enthält: das Unterscheidungszeichen des ausstellenden Mitgliedstaates im Negativdruck in einem blauen Rechteck, umgeben von zwölf gelben Sternen: [Nummerierung] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 232) Die Rückseite enthält: eine Erläuterung zu den nummerierten Angaben auf der Vorderseite der Karte. [Farbe] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 234) Die Fahrtenschreiberkarten werden mit folgender Hintergrundfarbe gedruckt: — Fahrerkarte: weiß, — Werkstattkarte: rot, — Kontrollkarte: blau, — Unternehmenskarte: gelb.	227 bis 229, 232, 234 bis 236

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Sicherheit] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 235) Zum Schutz vor Fälschung und unbefugten Änderungen weisen die Fahrtenschreiberkarten mindestens folgende Merkmale auf: — ein Sicherheitshintergrunddesign mit feingemustertem Guillochen und Irisdruck, — mindestens eine zweifarbige Mikrodruckzeile.	
		[Markierungen] Anhang 1C, Kapitel 4.1 „Sichtbare Daten“, 236) Die Mitgliedstaaten können Farben oder Markierungen wie Staatssymbole oder Sicherheitsmerkmale hinzufügen.	
		[Prüfzeichen] Die Fahrtenschreiberkarten tragen ein Prüfzeichen. Das Prüfzeichen besteht — aus einem Rechteck, in dem der Buchstabe „e“ platziert ist, gefolgt von der Kennzahl oder dem Kennbuchstaben des Landes, das die Typgenehmigung erteilt hat, — aus einer Typgenehmigungsnummer, die der Nummer des Typgenehmigungsbogens für die Fahrtenschreiberkarte entspricht und an einer beliebigen Stelle in der Nähe des Rechtecks anzubringen ist.	
2.2	Mechanische Prüfungen	[Kartengröße] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.1] Card dimensions and tolererances, card type ID-1 Unused card (Identifikationskarten — Physikalische Eigenschaften, [5] Abmessungen der Karte, [5.1] Kartengröße, [5.1.1] Abmessungen der Karte und Toleranzen, Kartentyp ID-1 Nicht verwendete Karte)	240, 243 ISO/IEC 7810
		[Kartenränder] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.2] Card edges (Identifikationskarten — Physikalische Eigenschaften, [5] Abmessungen der Karte, [5.1] Kartengröße, [5.1.2] Kartenränder)	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Aufbau der Karte] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [6] Card construction (Identifikationskarten — Physikalische Eigenschaften, [6] Aufbau der Karte)	
		[Kartenmaterialien] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [7] Card materials (Identifikationskarten — Physikalische Eigenschaften, [7] [Kartenmaterialien])	
		[Biegesteifigkeit] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.1] Bending stiffness (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.1] Biegesteifigkeit)	
		[Toxizität] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.3] Toxicity (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.3] Toxizität)	
		[Chemikalienbeständigkeit] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.4] Resistance to chemicals (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.4] Chemikalienbeständigkeit)	
		[Stabilität der Karte] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.5] Card dimensional stability and warpage with temperature and humidity (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.5] Stabilität/Verzug der Kartenabmessungen unter Einfluss von Temperatur und Feuchte)	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Licht] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.6] Light (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.6] Licht)	
		[Haltbarkeit] Anhang 1C, Kapitel 4.4 „Spezifikationen für Umgebung und Elektrizität", 241) Fahrtenschreiberkarten müssen bei Verwendung gemäß den Spezifikationen für Umgebung und Elektrizität während einer Dauer von fünf Jahren ordnungsgemäß funktionieren können.	
		[Schälfestigkeit] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.8] Peel strength (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.8] Schälfestigkeit)	
		[Farbhaftung/Blockfestigkeit] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.9] Adhesion or blocking (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.9] Farbhaftung/Blockfestigkeit)	
		[Verzug] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.11] Overall card warpage (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.11] Genereller Verzug der Karte)	
		[Hitzebeständigkeit] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.12] Resistance to heat (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.12] Hitzebeständigkeit)	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Oberflächenverformung] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.13] Surface distortions (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.13] Oberflächenverformung)	
		[Kontaminierung] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.14] Contamination and interaction of card components (Identifikationskarten — Physikalische Eigenschaften, [8] Eigenschaften der Karte, [8.14] Kontaminierung und Interaktion der Kartenkomponenten)	
2.3	Mechanische Prüfungen mit eingebettetem Chipmodul	[Biegung] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810:2003/Änderung 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress (Identifikationskarten — Physikalische Eigenschaften, Änderung 1: Kriterien für Karten mit integrierten Schaltkreisen, [9.2] Dynamische Biegebelastung) Gesamtzahl an Biegezyklen: 4 000.	ISO/IEC 7810
		[Torsion] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810:2003/Änderung 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress (Identifikationskarten — Physikalische Eigenschaften, Änderung 1: Kriterien für Karten mit integrierten Schaltkreisen, [9.3] Dynamische Torsionsbelastung) Gesamtzahl an Torsionszyklen: 4 000.	
3	**Modul**		
3.1	Modul	Das Modul bildet die Kapselung des Chips und die Kontaktplatte.	ISO/IEC 7816
		[Oberflächenprofil] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.2] Surface profile of contacts (Identifikationskarten — Chipkarten — Teil 1: Chipkarten mit Kontakten — Physikalische Eigenschaften, [4.2] Oberflächenprofil der Kontakte)	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Mechanische Stärke] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.3] Mechanical strength (of a card and contacts) (Identifikationskarten — Chipkarten — Teil 1: Chipkarten mit Kontakten — Physikalische Eigenschaften, [4.3] Mechanische Stärke (von Karte und Kontakten)	
		[Elektrischer Widerstand] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.4] Electrical resistance (of contacts) (Identifikationskarten — Chipkarten — Teil 1: Chipkarten mit Kontakten — Physikalische Eigenschaften, [4.4] Elektrischer Widerstand (der Kontakte)	
		[Abmessungen] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [3] Dimension of the contacts (Identifikationskarten — Chipkarten — Teil 2: Chipkarten mit Kontakten — Maße und Anordnung der Kontakte, [3] Maße der Kontakte	
		[Anordnung] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [4] Number and location of the contacts (Identifikationskarten — Chipkarten — Teil 2: Chipkarten mit Kontakten — Maße und Anordnung der Kontakte, [4] Anzahl und Anordnung der Kontakte Im Falle von Modulen mit sechs Kontakten zählen die Kontakte „C4“ und „C8“ nicht zu dieser Prüfanforderung.	
4	**Chip**		
4.1	Chip	[Betriebstemperatur] Der Chip der Fahrtenschreiberkarte muss bei Umgebungstemperaturen in einem Bereich zwischen – 25 °C und + 85 °C funktionieren.	241 bis 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Temperatur und Feuchte] Anhang 1C, Kapitel 4.4 „Spezifikationen für Umgebung und Elektrizität", 241) Die Fahrtenschreiberkarten müssen unter allen klimatischen Bedingungen, die im Gebiet der Gemeinschaft gewöhnlich anzutreffen sind, ordnungsgemäß funktionieren können, mindestens im Temperaturbereich – 25 °C bis + 70 °C mit gelegentlichen Spitzen bis zu + 85 °C, wobei „gelegentlich" jeweils nicht mehr als 4 Stunden und nicht mehr als 100 mal während der Lebensdauer der Karte bedeutet. Die Fahrtenschreiberkarten werden aufeinanderfolgend den folgenden Temperaturen und Feuchtigkeiten für die angegebene Zeitdauer ausgesetzt. Nach jedem Schritt werden die Fahrtenschreiberkarten auf elektrische Funktionsfähigkeit geprüft. 1. Temperatur von – 20 °C für 2 h. 2. Temperatur von +/–0 °C für 2 h. 3. Temperatur von + 20 °C, 50 % RF, für 2 h. 4. Temperatur von 50 °C, 50 % RF, für 2 h. 5. Temperatur von 70 °C, 50 % RF, für 2 h. Die Temperatur wird periodisch auf + 85 °C, 50 % RF, für 60 min erhöht. 6. Temperatur von 70 °C, 85 % RF, für 2 h. Die Temperatur wird periodisch auf + 85 °C, 85 % RF, für 30 min erhöht.	
		[Luftfeuchtigkeit] Anhang 1C, Kapitel 4.4 „Spezifikationen für Umgebung und Elektrizität", 242) Die Fahrtenschreiberkarten müssen bei einer Luftfeuchtigkeit von 10 bis 90 % ordnungsgemäß funktionieren können.	
		[Elektromagnetische Verträglichkeit — EMV] Anhang 1C, Kapitel 4.4 „Spezifikationen für Umgebung und Elektrizität", 244) Während des Betriebs müssen die Fahrtenschreiberkarten ECE R10 bezüglich der elektromagnetischen Verträglichkeit erfüllen.	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		[Statische Elektrizität] Anhang 1C, Kapitel 4.4 „Spezifikationen für Umgebung und Elektrizität“, 244) Während des Betriebs müssen die Fahrtenschreiberkarten gegen elektrostatische Entladungen geschützt sein. Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810:2003/Änderung 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards (Identifikationskarten — Physikalische Eigenschaften, Änderung 1: Kriterien für Karten mit integrierten Schaltkreisen, [9.4] Statische Elektrizität, [9.4.1] Kontakt IS-Karten) Prüfspannung: 4 000 V.	
		[Röntgenstrahlen] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810:2003/Änderung 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] Röntgenstrahlen	
		[Ultraviolettlicht] ISO/IEC 10373-1:2006, Identification cards — Test methods — Part 1: General characteristics [5.11] Ultraviolet light (Identifikationskarten — Physikalische Eigenschaften — Teil 1: Allgemeine Merkmale, [5.11] Ultraviolettlicht)	
		[3-Rad] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 10373-1:2006/Änderung ISO/IEC 103731:2012, Identification cards — Test methods — Part 1: General characteristics, Amendment 1 [5.22] ICC — Mechanical strength: 3 wheel test for ICCs with contacts (Identifikationskarten — Physikalische Eigenschaften — Teil 1: Allgemeine Merkmale, Änderung 1, [5.22] ICC — Mechanische Belastbarkeit: 3-Rad-Prüfung für ICC mit Kontakten)	
		[Umhüllung] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Wrapping Test Robustness (Beständigkeit bei der Umhüllungsprüfung) [13.2.1.32] TM-422: Mechanical Reliability: Wrapping Test (Mechanische Zuverlässigkeit: Umhüllungsprüfung)	

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.2	Mechanische Prüfungen, Chipmodule in Kartenkörper eingebettet -> wie 2.3	[Biegung] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810:2003/Änderung 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress (Identifikationskarten — Physikalische Eigenschaften, Änderung 1: Kriterien für Karten mit integrierten Schaltkreisen, [9.2] Dynamische Biegebelastung) Gesamtzahl an Biegezyklen: 4 000. [Torsion] Die Fahrtenschreiberkarten müssen die folgende Norm erfüllen: ISO/IEC 7810:2003/Änderung 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress (Identifikationskarten — Physikalische Eigenschaften, Änderung 1: Kriterien für Karten mit integrierten Schaltkreisen, [9.3] Dynamische Torsionsbelastung) Gesamtzahl an Torsionszyklen: 4 000.	ISO/IEC 7810
5	**Protokollprüfungen**		
5.1	ATR	Prüfen, dass ATR den Anforderungen entspricht	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Prüfen, dass Protokoll T=0 den Anforderungen entspricht	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Prüfen, dass der Befehl PTS durch Einstellen von T=1 ausgehend von T=0 den Anforderungen entspricht	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Prüfen, dass Protokoll T=1 den Anforderungen entspricht	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Kartenstruktur**		
6.1		Prüfen, dass die Dateistruktur der Karte den Anforderungen entspricht. Hierzu sind das Vorhandensein der obligatorischen Dateien auf der Karte und die Zugriffsbedingungen darauf zu überprüfen	TCS_22 bis TCS_28 TCS_140 bis TCS_179
7	**Funktionsprüfungen**		
7.1	Normale Verarbeitung	Für jeden Befehl ist jede zulässige Ausführung zumindest einmal zu prüfen (z. B.: Prüfung des Befehls UPDATE BINARY mit CLA = '00', CLA = '0C' und mit unterschiedlichen Parametern P1, P2 und Lc). Prüfen, dass die Operationen auf der Karte tatsächlich ausgeführt wurden (z. B.: durch das Lesen der Datei, für die der Befehl ausgeführt wurde)	TCS_29 bis TCS_139

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
7.2	Fehlermeldungen	Für jeden Befehl ist jede Fehlermeldung (entsprechend Anlage 2) zumindest einmal zu prüfen. Jeder generische Fehler ist zumindest einmal zu prüfen (mit Ausnahme von '**6400**'-Integritätsfehlern, die während der Sicherheitszertifizierung geprüft werden)	
7.3	Ziffernfolge und standardisierte Domänenparameter		CSM_48, CSM_50
8	**Personalisierung**		
8.1	Optische Personalisierung	Anhang 1C, Kapitel 4.1 „Sichtbare Daten", 230) Die Vorderseite enthält: Angaben zu der ausgestellten Karte. Anhang 1C, Kapitel 4.1 „Sichtbare Daten", 231) Die Vorderseite enthält: Datumsangaben im Format „TT/MM/JJJJ" oder „TT.MM.JJJJ" (Tag, Monat, Jahr). Anhang 1C, Kapitel 4.1 „Sichtbare Daten", 235) Zum Schutz vor Fälschung und unbefugten Änderungen weisen die Fahrtenschreiberkarten mindestens folgende Merkmale auf: — im Bereich des Lichtbilds eine Überlappung des Sicherheitshintergrunddesigns mit dem Lichtbild.	230, 231, 235

5. PRÜFUNG EXTERNER GNSS-AUSRÜSTUNG

Nein	Prüfung	Beschreibung	Anforderungsentsprechung
1.	**Administrative Prüfung**		
1.1	Dokumentation	Richtigkeit der Dokumentation	
2.	**Sichtprüfung der externen GNSS-Ausrüstung**		
2.1	Übereinstimmung mit der Dokumentation		
2.2	Kennung/Markierungen		224 bis 226
2.3	Werkstoffe		219 bis 223
3.	**Funktionsprüfungen**		
3.1	Kenndaten des Sensors		98,99
3.2	Externes GNSS-Modul — Kopplung mit der Fahrzeugeinheit		123, 205

Nein	Prüfung	Beschreibung	Anforderungsentsprechung
3.3	GNSS-Position		36, 37
3.4	VU-Schnittstelle, wenn es sich beim GNSS-Empfänger der VU um ein externes Gerät handelt.		03
3.5	Ziffernfolge und standardisierte Domänenparameter		CSM_48, CSM_50
4.	**Umweltprüfungen**		
4.1	Temperatur	Funktionsprüfung durch: Prüfung gemäß ISO 16750-4, Kapitel 5.1.1.2: Betriebsprüfung bei niedrigen Temperaturen (72 h @ – 20 °C) Diese Prüfung bezieht sich auf IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold (Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte) Prüfung gemäß ISO 16750-4, Kapitel 5.1.2.2: Betriebsprüfung bei hohen Temperaturen (72 h @ 70 °C) Diese Prüfung bezieht sich auf IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme) Prüfung gemäß ISO 16750-4, Kapitel 5.3.2: Schnelle Temperaturwechsel mit angegebener Übergangsdauer (– 20 °C/70 °C, 20 Zyklen, Haltezeit 1 h bei jeder Temperatur) In Bezug auf Mindest- und Höchsttemperatur sowie während der Temperaturzyklen ist (für die in Abschnitt 3 dieser Tabelle aufgeführten Prüfungen) eine geringere Anzahl an Prüfungen zulässig	213
4.2	Luftfeuchtigkeit	IEC 60068-2-30, Prüfung Db, zum Nachweis, dass die Fahrzeugeinheit einer zyklischen Feuchtigkeitsprüfung (Wärmeprüfung) von sechs 24-Std.-Zyklen jeweils mit einer Temperaturänderung von + 25 °C bis + 55 °C und einer relativen Luftfeuchtigkeit von 97 % bei +25 °C bzw. entsprechend 93 % bei + 55 °C standhält	214
4.3	Mechanisch	1. Sinusschwingungen. Nachweis, dass die Fahrzeugeinheit Sinusschwingungen mit folgenden Merkmalen standhält: konstante Verschiebung zwischen 5 und 11 Hz: max. 10 mm konstante Beschleunigung zwischen 11 und 300 Hz: 5 g Nachweis nach IEC 60068-2-6, Prüfung Fc, mit Mindestprüfdauer von 3 × 12 Std. (12 Std. je Achse) ISO 16750-3 schreibt für Geräte, die sich in einer entkoppelten Fahrerkabine befinden, keine Prüfung mit Sinusschwingungen vor.	219

Nein	Prüfung	Beschreibung	Anforderungsentsprechung
		2. Zufallsschwingungen: Prüfung gemäß ISO 16750-3, Kapitel 4.1.2.8: Prüfung VIII: Nutzfahrzeug, entkoppelte Fahrerkabine Prüfung mit regellosem Schwingen, 10…2 000 Hz, RMS vertikal 21,3 m/s², RMS longitudinal 11,8 m/s², RMS lateral 13,1 m/s², 3 Achsen, 32 Std. je Achse, einschließlich Temperaturzyklus – 20…70 °C. Diese Prüfung bezieht sich auf IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance (Umgebungseinflüsse — Teil 2-64: Prüfverfahren — Prüfung Fh: Schwingen, Breitbandrauschen (digital geregelt) und Leitfaden) 3. Stöße: mechanische Stöße mit 3 g Halbsinus gemäß ISO 16750. Diese Prüfungen werden an zwei unterschiedlichen Proben des zu prüfenden Gerätetyps durchgeführt.	
4.4	Schutz vor Wasser und vor Fremdkörpern	Prüfung gemäß ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Straßenfahrzeuge — Schutzarten (IP-Code) — Schutz gegen fremde Objekte, Wasser und Kontakt (Keine Parameteränderung)	220, 221
4.5	Überspannungsschutz	Nachweis, dass die Fahrzeugeinheit folgende Versorgungsspannungen aushält: 24-V-Versionen: 34V bei + 40 °C 1 Stunde 12-V-Versionen: 17 V bei + 40 °C 1 Stunde (ISO 16750-2, Kapitel 4.3)	216
4.6	Falschpolungsschutz	Nachweis, dass die Fahrzeugeinheit einer Umkehrung der Polarität der Stromversorgung standhält (ISO 16750-2, Kapitel 4.7)	216
4.7	Kurzschlussschutz	Nachweis, dass für Eingangs-/Ausgangssignale Schutz vor Kurzschluss der Stromversorgung und vor Erdschluss besteht (ISO 16750-2, Kapitel 4.10)	216
5	**EMV-Prüfungen**		
5.1	Störaussendung und Störanfälligkeit	Einhaltung von ECE-Regelung R10	218

Nein	Prüfung	Beschreibung	Anforderungsentsprechung
5.2	Elektrostatische Entladung	Einhaltung von ISO 10605:2008 + Technische Korrektur:2010 + AMD1:2014: +/– 4 kV Kontaktentladung und +/– 8 kV Luftentladung	218
5.3	Leitungsgeführte Störgrößen auf Versorgungsleitungen	24-V-Versionen: Einhaltung von ISO 7637-2 + ECE-Verordnung 10 Rev. 3: Impuls 1a: Vs = – 450 V Ri = 50 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 20V Ri = 0,05 Ohm Impuls 3a: Vs = – 150V Ri = 50 Ohm Impuls 3b: Vs = + 150V Ri = 50 Ohm Impuls 4: Vs = – 16 V Va = -12 V t6 = 100 ms Impuls 5: Vs = + 120 V Ri = 2,2 Ohm td = 250 ms 12-V-Versionen: Einhaltung von ISO 7637-1 + ECE-Verordnung 10 Rev. 3: Impuls 1: Vs = – 75V Ri = 10 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 10V Ri = 0,05 Ohm Impuls 3a: Vs = – 112V Ri = 50 Ohm Impuls 3b: Vs = + 75V Ri = 50 Ohm Impuls 4: Vs = – 6 V Va = -5 V t6 = 15 ms Impuls 5: Vs = + 65 V Ri = 3 Ohm td = 100 ms Impuls 5 ist nur in Fahrzeugeinheiten zu prüfen, die in Fahrzeugen installiert werden sollen, für die keine gemeinsame externe Blindlast vorgesehen ist Blindlastvorschläge siehe ISO 16750-2, 4. Ausgabe, Kapitel 4.6.4.	218

6. PRÜFUNGEN DER AUSRÜSTUNG ZUR FERNKOMMUNIKATION

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1.	**Administrative Prüfung**		
1.1	Dokumentation	Richtigkeit der Dokumentation	
2.	**Sichtprüfung**		
2.1	Übereinstimmung mit der Dokumentation		
2.2	Kennung/Markierungen		225, 226
2.3	Werkstoffe		219 bis 223

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.	**Umweltprüfungen**		
4.1	Temperatur	Funktionsprüfung durch: Prüfung gemäß ISO 16750-4, Kapitel 5.1.1.2: Betriebsprüfung bei niedrigen Temperaturen (72 h @ – 20 °C) Diese Prüfung bezieht sich auf IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold (Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte) Prüfung gemäß ISO 16750-4, Kapitel 5.1.2.2: Betriebsprüfung bei hohen Temperaturen (72 h @ 70 °C) Diese Prüfung bezieht sich auf IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme) Prüfung gemäß ISO 16750-4, Kapitel 5.3.2: Schnelle Temperaturwechsel mit angegebener Übergangsdauer (– 20 °C/70 °C, 20 Zyklen, Haltezeit 1 h (?) bei jeder Temperatur) In Bezug auf Mindest- und Höchsttemperatur sowie während der Temperaturzyklen ist (für die in Abschnitt 3 dieser Tabelle aufgeführten Prüfungen) eine geringere Anzahl an Prüfungen zulässig	213
4.4	Schutz vor Wasser und vor Fremdkörpern	Prüfung gemäß ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Straßenfahrzeuge — Schutzarten (IP-Code) — Schutz gegen fremde Objekte, Wasser und Kontakt — Elektrische Ausrüstungen) (Zielwert IP40)	220, 221
5	**EMV-Prüfungen**		
5.1	Störaussendung und Störanfälligkeit	Einhaltung von ECE-Regelung R10	218
5.2	Elektrostatische Entladung	Einhaltung von ISO 10605:2008 + Technische Korrektur:2010 + AMD1:2014: +/– 4 kV Kontaktentladung und +/– 8 kV Luftentladung	218
5.3	Leitungsgeführte Störgrößen auf Versorgungsleitungen	24-V-Versionen: Einhaltung von ISO 7637-2 + ECE-Verordnung 10 Rev. 3: Impuls 1a: Vs = – 450 V Ri = 50 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 20V Ri = 0,05 Ohm Impuls 3a: Vs = – 150V Ri = 50 Ohm Impuls 3b: Vs = + 150V Ri = 50 Ohm Impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms Impuls 5: Vs = + 120 V Ri = 2,2 Ohm td = 250 ms	218

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
		12-V-Versionen: Einhaltung von ISO 7637-1 + ECE-Verordnung 10 Rev. 3: Impuls 1: Vs = – 75V Ri = 10 Ohm Impuls 2a: Vs = + 37V Ri = 2 Ohm Impuls 2b: Vs = + 10V Ri = 0,05 Ohm Impuls 3a: Vs = – 112V Ri = 50 Ohm Impuls 3b: Vs = + 75V Ri = 50 Ohm Impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms Impuls 5: Vs = + 65 V Ri = 3 Ohm td = 100 ms Impuls 5 ist nur in Fahrzeugeinheiten zu prüfen, die in Fahrzeugen installiert werden sollen, für die keine gemeinsame externe Blindlast vorgesehen ist Blindlastvorschläge siehe ISO 16750-2, 4. Ausgabe, Kapitel 4.6.4.	

7. PAPIERFUNKTIONSPRÜFUNGEN

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1.	**Administrative Prüfung**		
1,1	Dokumentation	Richtigkeit der Dokumentation	
2	**Allgemeine Prüfungen**		
2.1	Zeichenzahl pro Zeile	Sichtprüfung der Ausdrucke.	172
2.2	Mindestzeichengröße	Sichtprüfung von Ausdrucken und Zeichen.	173
2.3	Unterstützte Zeichensätze	Der Drucker muss die in Anlage 1 Kapitel 4 „Zeichensätze“ spezifizierten Zeichen unterstützen.	174
2.4	Definition der Ausdrucke	Überprüfung der Typgenehmigung des Fahrtenschreibers und Prüfung der Ausdrucke	174
2.5	Lesbarkeit und Identifizierung der Ausdrucke	Prüfung der Ausdrucke Nachgewiesen durch Prüfberichte und -protokolle des Herstellers. Sämtliche Genehmigungsnummern der Fahrtenschreiber, mit denen das Druckerpapier verwendet werden kann, sind auf dem Papier abgedruckt.	175, 177, 178
2.6	Hinzunahme handschriftlicher Notizen	Sichtprüfung: Unterschriftsfeld für den Fahrer ist verfügbar. Felder für weitere handschriftliche Eintragungen sind verfügbar.	180

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
2.7	Weitere Details auf den Seiten.	Die Vorder- und Rückseiten des Papiers können weitere Einzelheiten und Informationen enthalten. Diese zusätzlichen Einzelheiten und Informationen dürfen die Lesbarkeit der Ausdrucke nicht beeinträchtigen. Sichtprüfung.	177, 178
3	**Lagerprüfung**		
3.1	Trockene Wärme	Vorbehandlung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte Prüfumgebung: 72 Stunden bei + 70 °C ± 2 °C Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ±3 % relative Feuchte	176, 178 IEC 60068-2-2-Bb
3.2	Feuchte Wärme	Vorbehandlung: 16 Stunden bei + 23 °C ± 2 °C/55 % ±3 % relative Feuchte Prüfumgebung: 144 Stunden bei +55 °C ± 2 °C und 93 % ± 3 % RF Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte	176, 178 IEC 60068-2-78-Cab
4	**Betriebsprüfungen Papier**		
4.1	Feuchtigkeitsbeständigkeit Hintergrund (unbedrucktes Papier)	Vorbehandlung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte Prüfumgebung: 144 Stunden bei + 55 °C ± 2 °C und 93 % ± 3 % RF Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte	176, 178 IEC 60068-2-78-Cab
4.2	Bedruckbarkeit	Vorbehandlung: 24 Stunden bei +40 °C ± 2 °C/93 % ± 3 % relative Feuchte Prüfumgebung: Ausdruck erfolgt bei + 23 °C ± 2 °C Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ±3 % relative Feuchte	176, 178
4.3	Wärmebeständigkeit	Vorbehandlung: 16 Stunden bei + 23 °C ± 2 °C/55 % ±3 % relative Feuchte Prüfumgebung: 2 Stunden bei + 70 °C ± 2 °C, trockene Wärme Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ±3 % relative Feuchte	176, 178 IEC 60068-2-2-Bb
4.4	Beständigkeit bei niedrigen Temperaturen	Vorbehandlung: 16 Stunden bei +23 °C ± 2 °C/55 % ± 3 % relative Feuchte Prüfumgebung: 24 Stunden bei – 20 °C ± 3 °C, trockene Kälte Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte	176, 178 ISO 60068-2-1-Ab

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.5	Lichtbeständigkeit	Vorbehandlung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte Prüfumgebung: 100 Stunden unter 5000 Lux Beleuchtung bei + 23 °C ± 2 °C/55 % ± 3 % Relative Feuchte Wiederherstellung: 16 Stunden bei + 23 °C ± 2 °C/55 % ± 3 % relative Feuchte	176, 178

Lesbarkeitskriterien für die Prüfungen 3.x und 4.x:

Lesbarkeit des Ausdrucks ist gewährleistet, wenn die optische Dichte die folgenden Grenzwerte einhält:

Gedruckte Zeichen: min. 1,0

Hintergrund (unbedrucktes Papier): max. 0,2

Optische Dichten der Ausdrucke zu messen gemäß DIN EN ISO 534.

Bei den Ausdrucken dürfen keine Änderungen der Maße auftreten; sie müssen perfekt lesbar bleiben.

8. INTEROPERABILITÄTSPRÜFUNGEN

Nr.	Prüfung	Beschreibung
	9.1 Interoperabilitätsprüfungen zwischen Fahrzeugeinheiten und Fahrtenschreiberkarten	
1	Gegenseitige Authentisierung	Prüfen, dass die gegenseitige Authentisierung zwischen der Fahrzeugeinheit und der Fahrtenschreiberkarte normal abläuft
2	Lese-/Schreib-Prüfungen	Ausführung eines typischen Tätigkeitsszenarios an der Fahrzeugeinheit. Dabei sind in Abhängigkeit von der zu prüfenden Karte so viele Schreibvorgänge wie bei der Karte möglich zu Ereignissen und Störungen durchzuführen Durch Herunterladen von einer Fahrzeugeinheit ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Durch Herunterladen von einer Karte ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Anhand täglicher Ausdrucke ist zu überprüfen, ob alle entsprechenden Aufzeichnungen korrekt zu lesen sind
	9.2 Interoperabilitätsprüfungen zwischen Fahrzeugeinheiten und Bewegungssensoren	
1	Koppelung	Prüfen, dass die Kopplung zwischen den Fahrzeugeinheiten und den Bewegungssensoren normal abläuft
2	Tätigkeitsprüfungen	Ausführung eines typischen Tätigkeitsszenarios am Bewegungssensor. Das Szenario hat eine normale Tätigkeit sowie die Erstellung von so vielen Ereignissen bzw. Störungen wie möglich zu beinhalten. Durch Herunterladen von einer Fahrzeugeinheit ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Durch Herunterladen von einer Karte ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Anhand eines täglichen Ausdrucks ist zu überprüfen, ob alle entsprechenden Aufzeichnungen korrekt zu lesen sind

Nr.	Prüfung	Beschreibung
9.3 Interoperabilitätsprüfungen zwischen Fahrzeugeinheiten und externen GNSS-Ausrüstungen (sofern zutreffend)		
1	Gegenseitige Authentisierung	Prüfen, dass gegenseitige Authentisierung zwischen der Fahrzeugeinheit und dem externen GNSS-Modul normal abläuft.
2	Tätigkeitsprüfungen	Ausführung eines typischen Tätigkeitsszenarios am externen GNSS. Das Szenario hat eine normale Tätigkeit sowie die Erstellung von so vielen Ereignissen bzw. Störungen wie möglich zu beinhalten. Durch Herunterladen von einer Fahrzeugeinheit ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Durch Herunterladen von einer Karte ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Anhand eines täglichen Ausdrucks ist zu überprüfen, ob alle entsprechenden Aufzeichnungen korrekt zu lesen sind

Anlage 10

SICHERHEITSANFORDERUNGEN

In dieser Anlage werden die Anforderungen an die IT-Sicherheit für die Komponenten von intelligenten Fahrtenschreibersystemen (Fahrtenschreiber der zweiten Generation) festgelegt.

SEC_001 Für folgende Komponenten des intelligenten Fahrtenschreibersystems erfolgt eine Sicherheitszertifizierung gemäß dem Common-Criteria-Zertifizierungsverfahren:

— Fahrzeugeinheit,

— Fahrtenschreiberkarte,

— Bewegungssensor,

— externe GNSS-Ausrüstung.

SEC_002 Die von jeder Komponente, für die eine Sicherheitszertifizierung zu erfolgen hat, zu erfüllenden Mindestanforderungen an die IT-Sicherheit werden in einem Schutzprofil gemäß dem Common-Criteria-Zertifizierungsverfahren festgelegt.

SEC_003 Die Europäische Kommission stellt sicher, dass vier mit diesem Anhang konforme Schutzprofile gefördert, entwickelt, von den für die IT-Sicherheitszertifizierung zuständigen staatlichen Stellen, die in der Joint Interpretation Working Group zusammenarbeiten (die die gegenseitige Anerkennung von Zertifikaten im Rahmen des europäischen Abkommens zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates, SOGIS-MRA) unterstützt), genehmigt und registriert werden:

— Schutzprofil für die Fahrzeugeinheit,

— Schutzprofil für die Fahrtenschreiberkarte,

— Schutzprofil für den Bewegungssensor,

— Schutzprofil für die externe GNSS-Ausrüstung.

Das Schutzprofil für die Fahrzeugeinheit gilt für die Fälle, in denen die VU zur Verwendung mit oder ohne eine externe GNSS-Ausrüstung bestimmt ist. Im ersten Fall sind die Sicherheitsanforderungen der externen GNSS-Ausrüstung im spezifischen Schutzprofil festgelegt.

SEC_004 Zur Formulierung der Sicherheitsanforderungen, die bei Beantragung der Sicherheitszertifizierung für die Komponente erfüllt werden müssen, konkretisieren und vervollständigen die Komponentenhersteller erforderlichenfalls das geeignete Schutzprofil, ohne die bestehenden Sicherheitsgefährdungen, Ziele, Verfahrensmöglichkeiten und SEF-Spezifikationen zu ändern bzw. zu streichen.

SEC_005 Während des Bewertungsverfahrens muss die strikte Konformität dieser spezifischen Sicherheitsanforderungen mit dem entsprechenden Schutzprofil festgestellt werden.

SEC_006 Die für jedes Schutzprofil vorgegebene Vertrauenswürdigkeitsstufe ist EAL4, erweitert um die Vertrauenswürdigkeitskomponenten ATE_DPT.2 und AVA_VAN.5.

Anlage 11

GEMEINSAME SICHERHEITSMECHANISMEN

INHALTSVERZEICHNIS

VORWORT		340
TEIL A	FAHRTENSCHREIBERSYSTEM DER 1. GENERATION	341
1.	EINLEITUNG	341
1.1.	Referenzdokumente	341
1.2.	Notationen und Abkürzungen	341
2.	KRYPTOGRAFISCHE SYSTEME UND ALGORITHMEN	343
2.1.	Kryptografische Systeme	343
2.2.	Kryptografische Algorithmen	343
2.2.1	RSA-Algorithmus	343
2.2.2	Hash-Algorithmus	343
2.2.3	Datenverschlüsselungsalgorithmus	343
3.	SCHLÜSSEL UND ZERTIFIKATE	343
3.1.	Erzeugung und Verteilung der Schlüssel	343
3.1.1	Erzeugung und Verteilung der RSA-Schlüssel	343
3.1.2	RSA-Prüfschlüssel	345
3.1.3	Bewegungssensorschlüssel	345
3.1.4	Erzeugung und Verteilung von T-DES-Sitzungsschlüsseln	345
3.2.	Schlüssel	345
3.3.	Zertifikate	345
3.3.1	Inhalt der Zertifikate	346
3.3.2	Ausgestellte Zertifikate	348
3.3.3	Verifizieren und Entpacken der Zertifikate	349
4.	GEGENSEITIGE AUTHENTISIERUNG	349
5.	VERTRAULICHKEITS-, INTEGRITÄTS- UND AUTHENTISIERUNGSMECHANISMEN FÜR DIE DATENÜBERTRAGUNG VU-KARTE	352
5.1.	Secure Messaging	352
5.2.	Behandlung von Secure-Messaging-Fehlern	354
5.3.	Algorithmus zur Berechnung der kryptografischen Prüfsummen	354
5.4.	Algorithmus zur Berechnung von Kryptogrammen für Vertraulichkeits-DOs	355
6.	DIGITALE SIGNATURMECHANISMEN BEIM HERUNTERLADEN VON DATEN	355
6.1.	Erzeugung der Signatur	355
6.2.	Verifizierung der Signatur	356

TEIL B	FAHRTENSCHREIBERSYSTEM DER 2. GENERATION	357
7.	EINLEITUNG	357
7.1.	Referenzdokumente	357
7.2.	Notationen und Abkürzungen	357
7.3.	Begriffsbestimmungen	359
8.	KRYPTOGRAFISCHE SYSTEME UND ALGORITHMEN	359
8.1.	Kryptografische Systeme	359
8.2.	Kryptografische Algorithmen	360
8.2.1	Symmetrische Algorithmen	360
8.2.2	Asymmetrische Algorithmen und standardisierte Domänenparameter	360
8.2.3	Hash-Algorithmen	361
8.2.4	Cipher Suites	361
9.	SCHLÜSSEL UND ZERTIFIKATE	361
9.1.	Asymmetrische Schlüsselpaare und Public-Key-Zertifikate	361
9.1.1	Allgemein	361
9.1.2	Europäische Ebene	362
9.1.3	Mitgliedstaatebene	362
9.1.4	Geräteebene: Fahrzeugeinheiten	363
9.1.5	Geräteebene: Fahrtenschreiberkarten	365
9.1.6	Geräteebene: Externe GNSS-Ausrüstung	366
9.1.7	Überblick Ersatz von Zertifikaten	367
9.2.	Symmetrische Schlüssel	368
9.2.1	Schlüssel für die Sicherung der Kommunikation VU-Bewegungssensor	368
9.2.2	Schlüssel zur Sicherung der DSRC-Kommunikation	372
9.3.	Zertifikate	375
9.3.1	Allgemein	375
9.3.2	Zertifikatsinhalt	375
9.3.3	Beantragen von Zertifikaten	377
10.	GEGENSEITIGE AUTHENTISIERUNG VU-KARTE UND SECURE MESSAGING	378
10.1.	Allgemein	378
10.2.	Gegenseitige Verifizierung der Zertifikatkette	379
10.2.1	Verifizierung der Kartenzertifikatkette durch die VU	379
10.2.2	Verifizierung der VU-Zertifikatkette durch die Karte	381
10.3.	VU-Authentisierung	384
10.4.	Chip-Authentisierung und Vereinbarung des Sitzungsschlüssels	385

10.5. Secure Messaging 387
10.5.1 Allgemein 387
10.5.2 Secure-Message-Struktur 388
10.5.3 Abbruch einer Secure-Messaging-Sitzung 391
11. VU UND EXTERNE GNSS-AUSRÜSTUNG: KOPPELUNG, GEGENSEITIGE AUTHENTISIERUNG UND SECURE MESSAGING 392
11.1. Allgemein 392
11.2. Koppelung von VU und externer GNSS-Ausrüstung 393
11.3. Gegenseitige Verifizierung der Zertifikatkette 393
11.3.1 Allgemein 393
11.3.2 Während der Koppelung VU-EGF 393
11.3.3 Im Normalbetrieb 394
11.4. VU-Authentisierung, Chip-Authentisierung und Vereinbarung des Sitzungsschlüssels 395
11.5. Secure Messaging 395
12. KOPPELUNG UND KOMMUNIKATION VU-BEWEGUNGSSENSOR 396
12.1. Allgemein 396
12.2. Koppelung VU-Bewegungssensor unter Verwendung verschiedener Schlüsselgenerationen 396
12.3. Koppelung und Kommunikation VU-Bewegungssensor mit AES 397
12.4. Koppelung VU-Bewegungssensor bei verschiedenen Gerätegenerationen 399
13. SICHERHEIT FÜR FERNKOMMUNIKATION PER DSRC 399
13.1. Allgemein 399
13.2. Verschlüsselung der Fahrtenschreibernutzdaten und MAC-Generierung 400
13.3. Verifizierung und Entschlüsselung der Fahrtenschreibernutzdaten 401
14. SIGNIEREN VON DATENDOWNLOADS UND VERIFIZIEREN DER SIGNATUREN 401
14.1. Allgemein 401
14.2. Erzeugung der Signatur 402
14.3. Verifizierung der Signatur 402

VORWORT

Diese Anlage enthält die Spezifizierung der Sicherheitsmechanismen zur Gewährleistung

— der gegenseitigen Authentisierung zwischen unterschiedlichen Komponenten im Fahrtenschreibersystem.

— Vertraulichkeit, Integrität, Authentizität und/oder Nichtabstreitbarkeit der zwischen den unterschiedlichen Komponenten des Fahrtenschreibersystems übertragenen oder auf externe Speichermedien heruntergeladenen Daten.

Diese Anlage besteht aus zwei Teilen. In Teil A werden die Sicherheitsmechanismen für das Fahrtenschreibersystem der 1. Generation (digitaler Fahrtenschreiber) definiert. In Teil B werden die Sicherheitsmechanismen für das Fahrtenschreibersystem der 2. Generation (intelligenter Fahrtenschreiber) definiert.

Die in Teil A dieser Anlage angegebenen Mechanismen kommen zur Anwendung, wenn mindestens eine der am Prozess der gegenseitigen Authentisierung und/oder Datenübertragung beteiligten Komponenten des Fahrtenschreibersystems der 1. Generation angehört.

Die in Teil B dieser Anlage angegebenen Mechanismen kommen zur Anwendung, wenn beide am Prozess der gegenseitigen Authentisierung und/oder Datenübertragung beteiligten Komponenten des Fahrtenschreibersystems der 2. Generation angehören.

In Anlage 15 sind weitere Informationen über die Verwendung von Komponenten der 1. Generation zusammen mit Komponenten der 2. Generation aufgeführt.

TEIL A

FAHRTENSCHREIBERSYSTEM DER 1. GENERATION

1. EINLEITUNG

1.1. **Referenzdokumente**

In dieser Anlage werden folgende Referenzdokumente herangezogen:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. April 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. Oktober 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange (Informationstechnik — Identifikationskarten, mit integrierten Schaltkreisen und Kontakten — Teil 4: Interindustrielle Kommandos). Erste Ausgabe: 1995 + Änderung 1: 1997.
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements (Identifikationskarten — Chipkarten — Teil 6: Datenelemente für den interindustriellen Informationsaustausch.) Erste Ausgabe: 1996 + Berichtigung 1: 1998.
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands (Informationstechnik — Identifikationskarten, mit integrierten Schaltkreisen und Kontakten — Teil 8: Interindustrielle sicherheitsbezogene Kommandos). Erste Ausgabe 1999.
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function (Informationstechnik — IT-Sicherheitsverfahren — Digitale Signaturschemata welche die Nachricht wieder herstellen — Teil 2: Mechanismen die eine dedizierte Hash Funktion verwenden). Erste Ausgabe: 1997.
ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm (Informationstechnik — Sicherheitsverfahren — Mechanismen zur Authentifikation von Instanzen — Teil 3: Authentifikation von Instanzen unter Nutzung eines Algorithmus mit öffentlichem Schlüssel). Zweite Ausgabe 1998.
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface (Straßenfahrzeuge — Fahrtenschreibersysteme — Teil 3: Bewegungssensor-Schnittstelle).

1.2. **Notationen und Abkürzungen**

In dieser Anlage werden folgende Notationen und Abkürzungen verwendet:

(K_a, K_b, K_c)	ein Schlüsselbund zur Verwendung durch den Triple Data Encryption Algorithm
CA	Certification Authority (Zertifizierungsstelle)
CAR	Certification Authority Reference (Referenz der Zertifizierungsstelle)
CC	Cryptographic Checksum (kryptografische Prüfsumme)
CG	Cryptogram (Kryptogramm)
CH	Command Header (Befehlskopf)
CHA	Certificate Holder Authorisation (Autorisierung des Zertifikatsinhabers)
CHR	Certificate Holder Reference (Referenz des Zertifikatsinhabers)
D()	Entschlüsselung mit DES

DE	Datenelement
DO	Datenobjekt
d	privater RSA-Schlüssel, privater Exponent
e	öffentlicher RSA-Schlüssel, öffentlicher Exponent
E()	Verschlüsselung mit DES
EQT	Equipment (Gerät)
Hash()	Hash-Wert, ein Ergebnis von *Hash*
Hash	Hash-Funktion
KID	Key Identifier (Schlüsselbezeichner)
Km	T-DES-Schlüssel Hauptschlüssel gemäß ISO 16844-3
Km_{VU}	in Fahrzeugeinheiten integrierter T-DES-Schlüssel
Km_{WC}	in Werkstattkarten integrierter T-DES-Schlüssel
m	Nachrichtenrepräsentant, eine ganze Zahl zwischen 0 und *n*-1
n	RSA-Schlüssel, Modulus
PB	Padding Bytes (Füllbytes)
PI	Padding Indicator-Byte (Verwendung im Kryptogramm für Vertraulichkeits-DO)
PV	Plain Value (Klarwert)
s	Signaturrepräsentant, eine ganze Zahl zwischen 0 und *n*-1
SSC	Send Sequence Counter (Sendesequenzzähler)
SM	Secure Messaging
TCBC	TDEA-Modus Cipher Block Chaining
TDEA	Triple Data Encryption Algorithm (Triple-Datenverschlüsselungsalgorithmus)
TLV	Tag Length Value (Taglängenwert)
VU	Fahrzeugeinheit (Vehicle Unit)
X.C	Zertifikat von Benutzer X, ausgestellt durch eine Zertifizierungsstelle
X.CA	Zertifizierungsstelle von Benutzer X
$X.CA.PK \circ X.C$	Vorgang des Entpackens eines Zertifikats zur Herauslösung eines öffentlichen Schlüssels; es handelt sich um einen Infix-Operator, dessen linker Operand der öffentliche Schlüssel einer Zertifizierungsstelle und dessen rechter Operand das von der Zertifizierungsstelle ausgestellte Zertifikat ist; das Ergebnis ist der öffentliche Schlüssel von Benutzer X, dessen Zertifikat der rechte Operand ist
X.PK	öffentlicher RSA-Schlüssel eines Benutzers X
X.PK[I]	RSA-Chiffrierung einer Information I unter Verwendung des öffentlichen Schlüssels von Benutzer X
X.SK	privater RSA-Schlüssel eines Benutzers X
X.SK[I]	RSA-Chiffrierung einer Information I unter Verwendung des privaten Schlüssels von Benutzer X
‘xx’	ein Hexadezimalwert
||	Verkettungsoperator

2. KRYPTOGRAFISCHE SYSTEME UND ALGORITHMEN

2.1. **Kryptografische Systeme**

CSM_001 Fahrzeugeinheiten und Fahrtenschreiberkarten verwenden ein klassisches RSA-Public-Key-Verschlüsselungssystem, sodass folgende Sicherheitsmechanismen vorliegen:

— Authentisierung zwischen Fahrzeugeinheiten und Karten,

— Übertragung von Triple-DES-Sitzungsschlüsseln zwischen Fahrzeugeinheiten und Fahrtenschreiberkarten,

— digitale Signatur von Daten, die von Fahrzeugeinheiten oder Fahrtenschreiberkarten an externe Medien heruntergeladen werden.

CSM_002 Fahrzeugeinheiten und Fahrtenschreiberkarten verwenden ein symmetrisches Triple-DES-Verschlüsselungssystem, sodass ein Mechanismus für die Datenintegrität während des Benutzerdatenaustauschs zwischen Fahrzeugeinheiten und Fahrtenschreiberkarten und gegebenenfalls die Vertraulichkeit beim Datenaustausch zwischen Fahrzeugeinheiten und Fahrtenschreiberkarten gewährleistet sind.

2.2. **Kryptografische Algorithmen**

2.2.1 *RSA-Algorithmus*

CSM_003 Der RSA-Algorithmus wird durch folgende Beziehungen vollständig definiert:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Eine ausführlichere Beschreibung der RSA-Funktion findet sich im Referenzdokument PKCS1. Der im RSA-Algorithmus verwendete öffentliche Exponent e ist eine Ganzzahl zwischen 3 und n-1, wobei gilt: gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hash-Algorithmus*

CSM_004 Die Mechanismen für die digitale Signatur verwenden den Hash-Algorithmus SHA-1 gemäß Definition im Referenzdokument SHA-1.

2.2.3 *Datenverschlüsselungsalgorithmus*

CSM_005 DES-gestützte Algorithmen werden im Modus Cipher Block Chaining verwendet.

3. SCHLÜSSEL UND ZERTIFIKATE

3.1. **Erzeugung und Verteilung der Schlüssel**

3.1.1 *Erzeugung und Verteilung der RSA-Schlüssel*

CSM_006 Die Erzeugung der RSA-Schlüssel erfolgt auf drei hierarchischen Funktionsebenen:

— auf europäischer Ebene,

— auf Mitgliedstaatebene,

— auf Geräteebene.

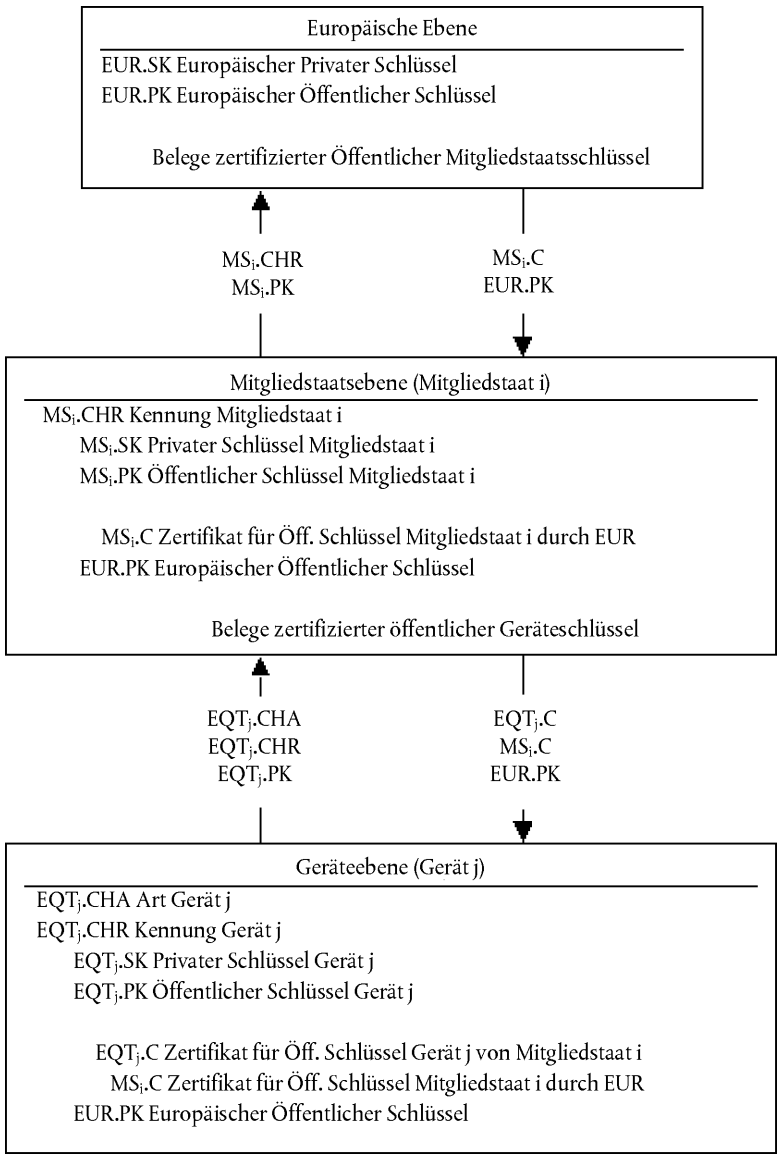
CSM_007 Auf europäischer Ebene wird ein einziges Schlüsselpaar (EUR.SK und EUR.PK) erzeugt. Der europäische private Schlüssel wird zur Zertifizierung der öffentlichen Schlüssel der Mitgliedstaaten verwendet. Über alle zertifizierten Schlüssel sind Belege aufzubewahren. Diese Aufgaben werden von einer Europäischen Zertifizierungsstelle wahrgenommen, die der Europäischen Kommission untersteht.

CSM_008 Auf Mitgliedstaatebene wird ein Mitgliedstaatschlüsselpaar (MS.SK und MS.PK) erzeugt. Öffentliche Mitgliedstaatschlüssel werden von der Europäischen Zertifizierungsstelle zertifiziert. Der private Mitgliedstaatschlüssel wird für die Zertifizierung von öffentlichen Schlüsseln verwendet, die in Geräten (Fahrzeugeinheit oder Fahrtenschreiberkarte) eingefügt sind. Über alle zertifizierten öffentlichen Schlüssel sind Belege zusammen mit der Kennung des Geräts, für das sie bestimmt sind, aufzubewahren. Diese Aufgaben werden von der Zertifizierungsstelle des jeweiligen Mitgliedstaates wahrgenommen. Ein Mitgliedstaat darf sein Schlüsselpaar in regelmäßigen Abständen ändern.

CSM_009 Auf Geräteebene wird ein einziges Schlüsselpaar (EQT.SK und EQT.PK) erzeugt und in jedes Gerät eingefügt. Die öffentlichen Geräteschlüssel werden von der Zertifizierungsstelle des jeweiligen Mitgliedstaates zertifiziert. Diese Aufgaben können von Geräteherstellern, Geräteintegratoren und Behörden der Mitgliedstaaten wahrgenommen werden. Dieses Schlüsselpaar wird zur Authentisierung, für die digitale Signatur sowie zur Chiffrierung verwendet.

CSM_010 Bei der Erzeugung, ggf. bei der Übertragung sowie bei der Speicherung ist die Vertraulichkeit der privaten Schlüssel zu wahren.

Im folgenden Schaubild ist der Datenfluss dieses Prozesses zusammengefasst:



3.1.2 *RSA-Prüfschlüssel*

CSM_011 Zum Zwecke der Geräteprüfung (einschließlich Interoperabilitätsprüfungen) erzeugt die Europäische Zertifizierungsstelle ein anderes einziges europäisches Prüfschlüsselpaar und mindestens zwei Mitgliedstaat-Prüfschlüsselpaare, deren öffentliche Schlüssel mit dem europäischen privaten Prüfschlüssel zertifiziert werden. Von den Herstellern werden in Geräte, die der Typgenehmigungsprüfung unterzogen werden, Prüfschlüssel eingefügt, die durch einen dieser Mitgliedstaatprüfschlüssel zertifiziert sind.

3.1.3 *Bewegungssensorschlüssel*

Die Geheimhaltung der drei genannten T-DES-Schlüssel ist während der Erzeugung, der Übermittlung und ggf. der Aufbewahrung in geeigneter Weise zu gewährleisten.

Um die Unterstützung von Fahrtenschreiberkomponenten, die der ISO 16844 entsprechen, zu gewährleisten, stellen die Europäische Zertifizierungsstelle und die Zertifizierungsstellen der Mitgliedstaaten darüber hinaus Folgendes sicher:

CSM_036 Die Europäische Zertifizierungsstelle erzeugt KmVU und KmWC als zwei voneinander unabhängige und einmalige Triple-DES-Schlüssel sowie Km, wobei gilt: $Km = Km_{VU}$ XOR Km_{WC} . Die Europäische Zertifizierungsstelle übermittelt diese Schlüssel unter geeigneten Sicherheitsvorkehrungen auf deren Anforderung an die Zertifizierungsstellen der Mitgliedstaaten.

CSM_037 Die Zertifizierungsstellen der Mitgliedstaaten:

— verschlüsseln mit Km die von den Herstellern der Bewegungssensoren angeforderten Bewegungssensordaten (die mit Km zu verschlüsselnden Daten sind in ISO 16844-3 festgelegt),

— übermitteln Km_{VU} zum Einbau in die Fahrzeugeinheiten unter geeigneten Sicherheitsvorkehrungen an deren Hersteller,

— stellen sicher, dass Km_{WC} bei der Personalisierung der Karten in alle Werkstattkarten eingefügt wird (`SensorInstallationSecData` in `Sensor_Installation_Data` der Elementardatei).

3.1.4 *Erzeugung und Verteilung von T-DES-Sitzungsschlüsseln*

CSM_012 Im Rahmen des Prozesses der gegenseitigen Authentisierung erzeugen Fahrzeugeinheiten und Fahrtenschreiberkarten die erforderlichen Daten zur Erstellung eines gemeinsamen Triple-DES-Sitzungsschlüssels und tauschen diese Daten aus. Die Vertraulichkeit dieses Datenaustauschs wird durch einen RSA-Verschlüsselungsmechanismus geschützt.

CSM_013 Dieser Schlüssel wird für alle nachfolgenden kryptografischen Operationen unter Anwendung des Secure Messaging benutzt. Seine Gültigkeit erlischt am Ende der Sitzung (Entnahme oder Zurücksetzen der Karte) und/oder nach 240 Benutzungen (eine Benutzung des Schlüssels = ein mittels Secure Messaging an die Karte gesandter Befehl und die dazugehörige Antwort).

3.2. **Schlüssel**

CSM_014 RSA-Schlüssel haben (ungeachtet der Ebene) folgende Länge: Modulus *n* 1 024 Bit, öffentlicher Exponent *e* max. 64 Bit, privater Exponent *d* 1 024 Bit.

CSM_015 Triple-DES-Schlüssel haben die Form (K_a, K_b, K_a), wobei K_a und K_b unabhängige Schlüssel mit einer Länge von 64 Bit sind. Es wird kein Paritätsfehler-Erkennungsbit gesetzt.

3.3. **Zertifikate**

CSM_016 Bei den RSA-Public-Key-Zertifikaten muss es sich um Zertifikate entsprechend der Definition „non self descriptive“ und „card verifiable“ des Referenzdokuments ISO/IEC 7816-8 handeln.

3.3.1 *Inhalt der Zertifikate*

CSM_017 RSA-Public-Key-Zertifikate sind aus den folgenden Daten in folgender Reihenfolge aufgebaut:

Daten	Format	Bytes	Bemerkung
CPI	INTEGER	1	Certificate Profile Identifier (Zertifikatsprofil '01' in dieser Version)
CAR	OCTET STRING	8	Certification Authority Reference (Referenz der Zertifizierungsstelle)
CHA	OCTET STRING	7	Certificate Holder Authorisation (Autorisierung des Zertifikatsinhabers)
EOV	TimeReal	4	Ablauf der Gültigkeit des Zertifikats, bei Nichtverwendung mit 'FF' gefüllt
CHR	OCTET STRING	8	Certificate Holder Reference (Referenz des Zertifikatsinhabers)
n	OCTET STRING	128	Öffentlicher Schlüssel (Modulus)
e	OCTET STRING	8	Öffentlicher Schlüssel (öffentlicher Exponent)
		164	

Hinweise:

1. Mit dem Certificate Profile Identifier (Zertifikatsprofilbezeichner, CPI) wird die genaue Struktur eines Authentisierungszertifikats abgegrenzt. Er kann als interner Gerätebezeichner einer relevanten Kopfliste verwendet werden, die die Verkettung der Datenelemente innerhalb des Zertifikats beschreibt.

   Die Kopfliste für diesen Zertifikatinhalt lautet wie folgt:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Tag für erweiterte Kopfliste	Länge der Kopfliste	CPI-Tag	CPI-Länge	CAR-Tag	CAR-Länge	CHA-Tag	CHA-Länge	EOV-Tag	EOV-Länge	CHR-Tag	CHR-Länge	Tag für öffentlichen Schlüssel (konstruiert)	Länge der folgenden DO	Modulus-Tag	Modulus-Länge	Tag für öffentlichen Exponenten	Länge des öffentlichen Exponenten

2. „Certification Authority Reference" (Referenz der Zertifizierungsstelle, CAR) identifiziert die das Zertifikat ausstellende Zertifizierungsstelle, sodass das Datenelement gleichzeitig als Authority Key Identifier (Schlüsselbezeichner der Stelle) zur Angabe des öffentlichen Schlüssels der Zertifizierungsstelle verwendet werden kann (Kodierung siehe „Key Identifier").

3. Mit „Certificate Holder Authorisation“ (Autorisierung des Zertifikatsinhabers, CHA) wird die Berechtigung des Zertifikatsinhabers ausgewiesen. Sie besteht aus der Kontrollgerätanwendungs-ID sowie aus der Art des Geräts, für das das Zertifikat bestimmt ist (entsprechend dem Datenelement `EquipmentType`, ‘00’ für einen Mitgliedstaat).

4. „Certificate Holder Reference“ (Referenz des Zertifikatsinhabers, CHR) dient der eindeutigen Identifizierung des Zertifikatsinhabers, sodass das Datenelement gleichzeitig als „Subject Key Identifier“ (Schlüsselbezeichner des Subjekts) zur Angabe des öffentlichen Schlüssels des Zertifikatsinhabers verwendet werden kann.

5. „KEY IDENTIFIERS“ (SCHLÜSSELBEZEICHNER, KID) DIENEN DER EINDEUTIGEN IDENTIFIZIERUNG DES ZERTIFIKATSINHABERS ODER DER ZERTIFIZIERUNGSSTELLEN. SIE SIND WIE FOLGT KODIERT:

5.1 Gerät (VU oder Karte):

Daten	Seriennummer Gerät	Datum	Art	Hersteller
Länge	4 Bytes	2 Bytes	1 Byte	1 Byte
Wert	Ganze Zahl	MM JJ BCD-Kod.	Herstellerspezifisch	Herstellercode

Dem Hersteller einer VU ist die Kennung des Geräts, in das die Schlüssel eingefügt werden, bei der Beantragung von Zertifikaten unter Umständen nicht bekannt.

Ist dem Hersteller die Gerätekennung bekannt, sendet er sie mit dem öffentlichen Schlüssel zwecks Zertifizierung an die Zertifizierungsstelle seines Mitgliedstaats. Das Zertifikat enthält dann die Gerätekennung, und der Hersteller muss sicherstellen, dass Schlüssel und Zertifikat in das vorgesehene Gerät eingefügt werden. Der Key Identifier weist die oben genannte Form auf.

Ist dem Hersteller die Gerätekennung nicht bekannt, muss er jeden Antrag auf ein Zertifikat eindeutig kennzeichnen und diese Kennung zusammen mit dem öffentlichen Schlüssel zwecks Zertifizierung an die Zertifizierungsstelle seines Mitgliedstaates senden. Das Zertifikat enthält dann die Antragskennung. Nach dem Einfügen der Schlüssel in das Gerät muss der Hersteller der Zertifizierungsstelle die Zuordnung des Schlüssels zum Gerät mitteilen (d. h. Kennung des Zertifikatsantrags, Gerätekennung). Der Key Identifier (KID) hat folgende Form:

Daten	Seriennummer Zertifikatsantrag	Datum	Art	Hersteller
Länge	4 Bytes	2 Bytes	1 Byte	1 Byte
Wert	Ganze Zahl	MM JJ BCD-Kod.	‘FF’	Herstellercode

5.2 Zertifizierungsstelle:

Daten	Kennung	Seriennr. Schlüssel	Zusatzinfo	Kennung
Länge	4 Bytes	1 Byte	2 Bytes	1 Byte

Wert	1 Byte numerischer Landescode 3 Bytes alphanumerischer Landescode	Ganze Zahl	Zusatzkodierung (CA-spezifisch) 'FF FF' bei Nichtverwendung	'01'

Mit der Seriennummer Schlüssel werden die verschiedenen Schlüssel eines Mitgliedstaates unterschieden, sofern der Schlüssel verändert wird.

6. Den Zertifikatsprüfern ist implizit bekannt, dass es sich bei dem zertifizierten Schlüssel um einen für die Authentisierung, für die Verifizierung der digitalen Signatur und für die vertrauliche Chiffrierung relevanten RSA-Schlüssel handelt (das Zertifikat enthält keine Objektkennung zur entsprechenden Spezifizierung).

3.3.2 *Ausgestellte Zertifikate*

CSM_018 Das ausgestellte Zertifikat ist eine digitale Signatur mit teilweiser Wiederherstellung des Zertifikatsinhalts gemäß ISO/IEC 9796-2 (ausgenommen Anhang A4) mit angefügter „Certification Authority Reference".

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

wobei Zertifikatsinhalt = Cc = C_r || C_n

106 Bytes 58 Bytes

Hinweise:

1. Dieses Zertifikat ist 194 Bytes lang.

2. Die von der Signatur verdeckte CAR wird ebenfalls an die Signatur angefügt, sodass der öffentliche Schlüssel der Zertifizierungsstelle zur Verifizierung des Zertifikats gewählt werden kann.

3. Dem Zertifikatsprüfer ist der von der Zertifizierungsstelle für die Unterzeichnung des Zertifikats verwendete Algorithmus implizit bekannt.

4. Die zu dem ausgestellten Zertifikat gehörende Kopfliste lautet wie folgt:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Tag für CV-Zertifikat (konstruiert)	Länge der folgenden DO	Signatur-Tag	Signatur-Länge	Rest-Tag	Restlänge	CAR-Tag	CAR-Länge

3.3.3 *Verifizieren und Entpacken der Zertifikate*

Das Verifizieren und Entpacken der Zertifikate besteht in der Verifizierung der Signatur entsprechend ISO/IEC 9796-2, wodurch der Zertifikatsinhalt und der enthaltene öffentliche Schlüssel aufgerufen werden: X.PK = X.CA.PK $_o$ X.C, sowie in der Verifizierung der Gültigkeit des Zertifikats.

CSM_019 Dazu gehören folgende Schritte:

Verifizierung der Signatur und Abrufen des Inhalts:

— von X.C Abruf von Sign, C_n' und CAR': X.C = Sign || C_n' || CAR'

128 Bytes 58 Bytes 8 Bytes

— von CAR' Auswahl des entsprechenden öffentlichen Schlüssels der Zertifizierungsstelle (wenn nicht bereits zuvor durch andere Mittel erfolgt),

— Öffnen von Sign mit öffentlichem CA-Schlüssel: Sr'= X.CA.PK [Sign],

— Prüfung Sr' startet mit '6A' und endet mit 'BC'

— Berechnung von C_r' und H' aus: Sr' = '6A' || C_r' || H' || 'BC'

106 Bytes 20 Bytes

— Wiederherstellung des Zertifikatsinhalts C' = C_r' || C_n',

— Prüfung *Hash*(C') = H'

Sind die Prüfungen positiv, ist das Zertifikat echt und sein Inhalt ist C'.

Verifizierung der Gültigkeit. Von C':

— Prüfung des Ablaufdatums der Gültigkeit, wenn zutreffend,

Abruf und Speicherung des öffentlichen Schlüssels, des Key Identifier, der Certificate Holder Authorisation und des Ablaufs der Gültigkeit des Zertifikats von C':

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. GEGENSEITIGE AUTHENTISIERUNG

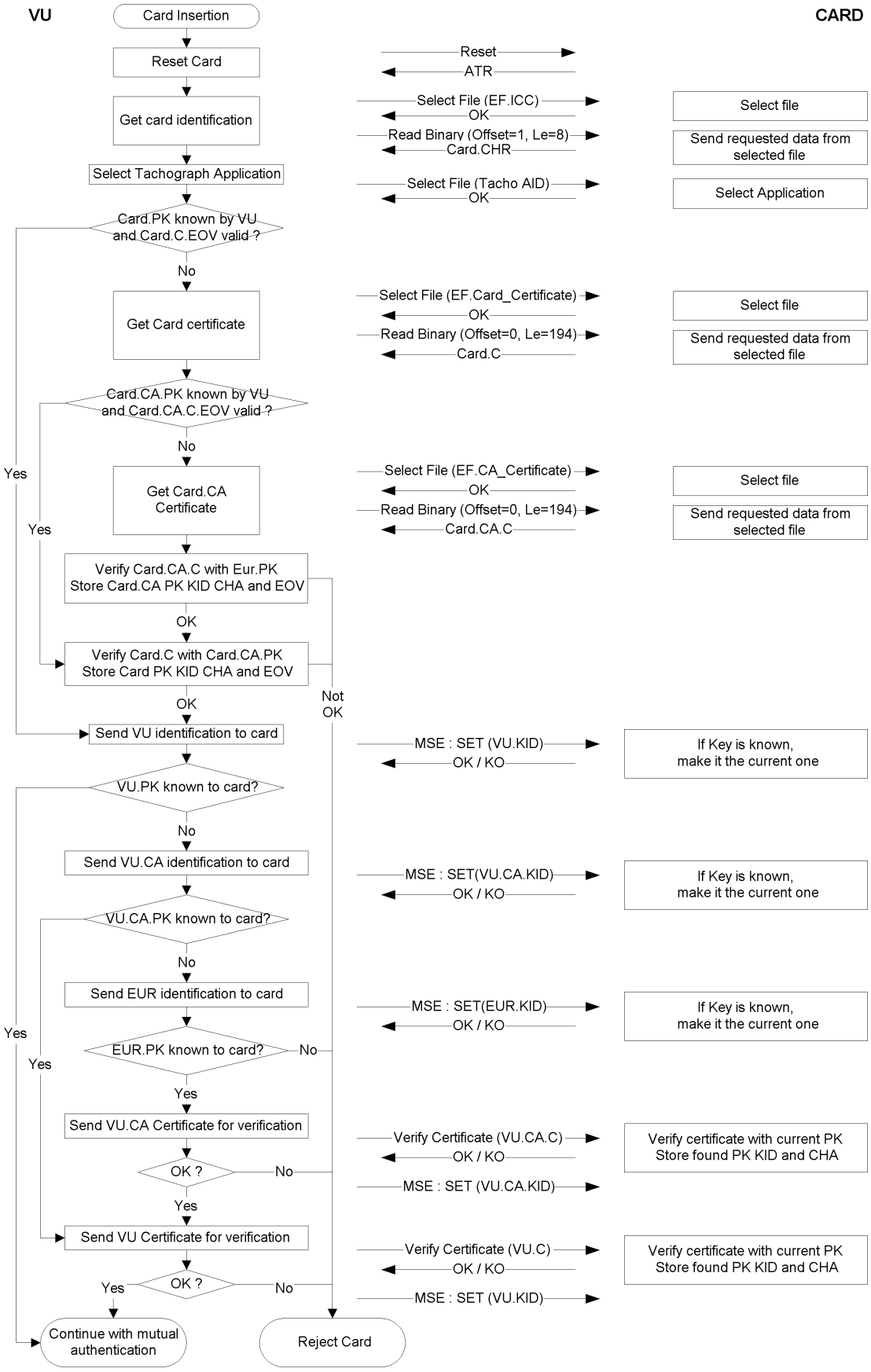
Die gegenseitige Authentisierung zwischen Karten und VU beruht auf dem folgenden Prinzip:

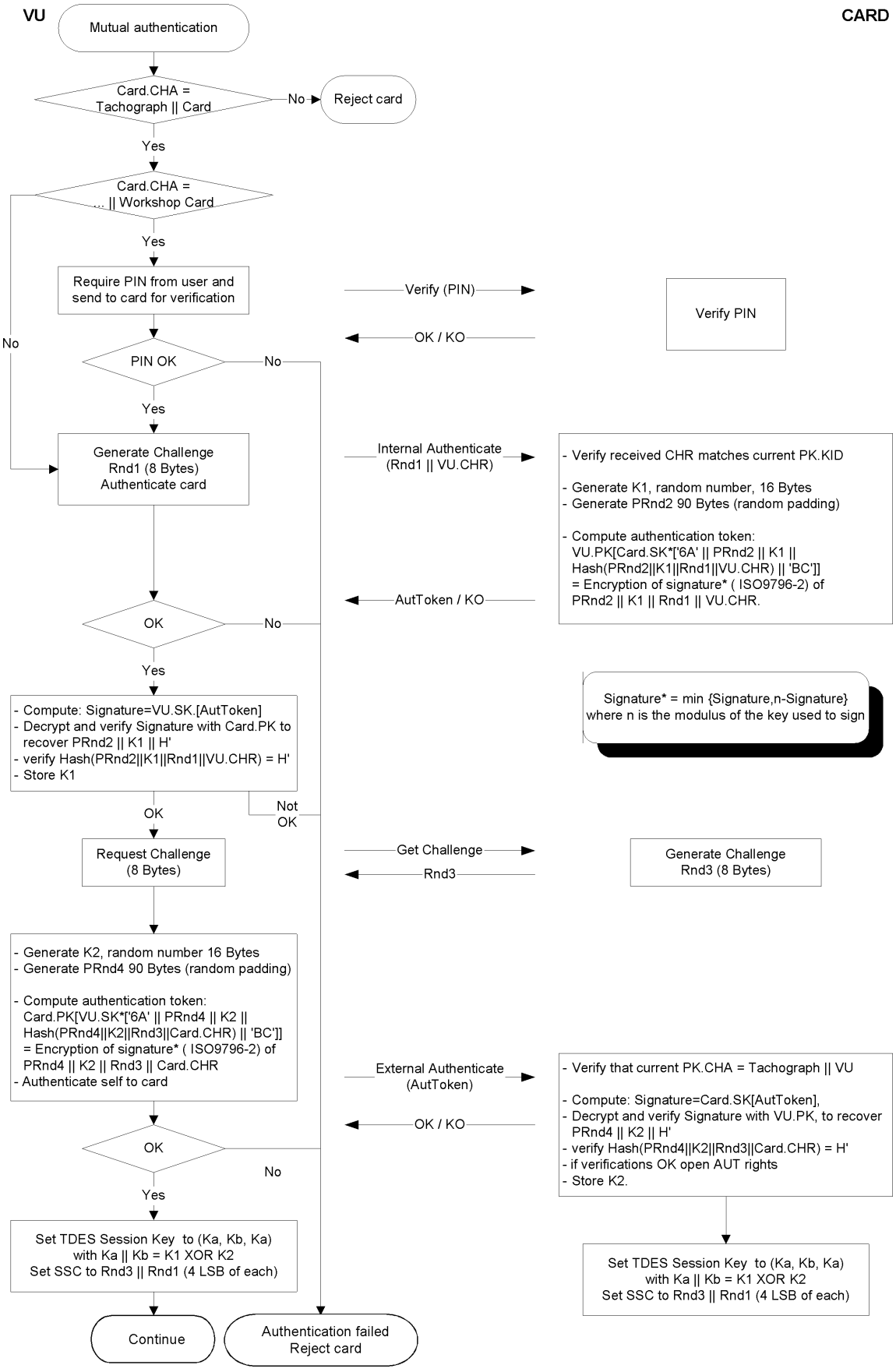
Jede Seite weist der Gegenseite nach, dass sie sich im Besitz eines gültigen Schlüsselpaares befindet, dessen öffentlicher Schlüssel von der Zertifizierungsstelle des jeweiligen Mitgliedstaates zertifiziert worden ist, die wiederum von der europäischen Zertifizierungsstelle zertifiziert wurde.

Der Nachweis wird geführt, indem mit dem privaten Schlüssel eine von der Gegenseite gesandte Zufallszahl signiert wird; die Gegenseite muss bei der Verifizierung dieser Signatur die Zufallszahl wiederherstellen können.

Der Mechanismus wird von der VU beim Einstecken der Karte ausgelöst. Er beginnt mit dem Austausch der Zertifikate und dem Entpacken der öffentlichen Schlüssel und endet mit der Erzeugung eines Sitzungsschlüssels.

CSM_020 Folgendes Protokoll findet Verwendung (Pfeile weisen auf Befehle und ausgetauschte Daten hin, siehe Anlage 2):




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
No
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. VERTRAULICHKEITS-, INTEGRITÄTS- UND AUTHENTISIERUNGSMECHANISMEN FÜR DIE DATENÜBERTRAGUNG VU-KARTE

5.1. **Secure Messaging**

CSM_021 Die Integrität der Datenübertragung zwischen VU und Karte wird durch Secure Messaging entsprechend den Referenzdokumenten ISO/IEC 7816-4 und ISO/IEC 7816-8 geschützt.

CSM_022 Müssen Daten während der Übertragung geschützt werden, wird den innerhalb des Befehls oder der Antwort gesandten Datenobjekten ein Datenobjekt „Cryptographic Checksum" angefügt. Diese kryptografische Prüfsumme wird vom Empfänger verifiziert.

CSM_023 Die kryptografische Prüfsumme der innerhalb eines Befehls gesandten Daten integriert den Befehlskopf sowie alle gesandten Datenobjekte (=>CLA = '0C', und alle Datenobjekte sind mit Tags zu kapseln, bei denen b1=1).

CSM_024 Die Statusinformationsbytes der Antwort sind durch eine kryptografische Prüfsumme zu schützen, wenn die Antwort kein Datenfeld enthält.

CSM_025 Kryptografische Prüfsummen sind 4 Bytes lang.

Somit weisen Befehle und Antworten bei Anwendung von Secure Messaging folgende Struktur auf:

Die DO werden als Teilmenge der in ISO/IEC 7816-4 beschriebenen Secure-Messaging-DO verwendet:

Tag	Symbolform	Bedeutung
'81'	T_{PV}	Klarwert, nicht in BER-TLV kodiert (durch CC zu schützen)
'97'	$\mathbf{T_{LE}}$	Wert von Le im ungesicherten Befehl (durch CC zu schützen)
'99'	T_{SW}	Status-Info (durch CC zu schützen)
'8E'	T_{CC}	Kryptografische Prüfsumme (CC)
'87'	$T_{PI\ CG}$	Padding Indicator Byte || Cryptogram (Klarwert, nicht in BER-TLV kodiert)

Ausgehend von einem ungesicherten Befehl-Antwort-Paar:

Befehlskopf				Befehlskörper		
CLA	INS	P1	P2	[L_c-Feld]	[Datenfeld]	[L_e-Feld]
vier Bytes				L Bytes, bezeichnet als B_1 bis B_L		

Antwortkörper	Antwortendmarke	
[Datenfeld]	SW1	SW2
L_r Datenbytes	zwei Bytes	

lautet das entsprechende gesicherte Befehl-Antwort-Paar:

Gesicherter Befehl:

Befehlskopf (CH)				Befehlskörper										
CLA	INS	P1	P2	[Neues L_c-Feld]	[Neues Datenfeld]									[Neues L_e-Feld]
‘OC’				Länge des neuen Datenfelds	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Datenfeld	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

In die Prüfsumme zu integrierende Daten = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Padding Bytes (80 .. 00) gemäß ISO-IEC 7816-4 und ISO 9797, Methode 2.

Die PV und LE der DO sind nur vorhanden, wenn entsprechende Daten im ungesicherten Befehl vorliegen.

Gesicherte Antwort:

1. Wenn das Antwortdatenfeld nicht leer ist und nicht vertraulichkeitsgeschützt werden muss:

Antwortkörper						Antwortendmarke
[Neues Datenfeld]						SW1 SW2 neu
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Datenfeld	‘8E’	‘04’	CC	

In die Prüfsumme zu integrierende Daten = T_{PV} || L_{PV} || PV || PB

2. Wenn das Antwortdatenfeld nicht leer ist und vertraulichkeitsgeschützt werden muss:

Antwortkörper						Antwortendmarke
[Neues Datenfeld]						SW1 SW2 neu
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI || CG	‘8E’	‘04’	CC	

Daten in CG: nicht-BER-TLV-kodierte Daten und Füllbytes.

In die Prüfsumme zu integrierende Daten = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Wenn das Antwortdatenfeld leer ist:

Antwortkörper						Antwortendmarke
[Neues Datenfeld]						SW1 SW2 neu
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	SW1 SW2 neu	'8E'	'04'	CC	

In die Prüfsumme zu integrierende Daten = T_{SW} || L_{SW} || SW || PB

5.2. **Behandlung von Secure-Messaging-Fehlern**

CSM_026 Erkennt die Fahrtenschreiberkarte beim Interpretieren eines Befehls einen SM-Fehler, müssen die Statusbytes ohne SM zurückgesandt werden. Laut ISO/IEC 7816-4 sind folgende Statusbytes zur Anzeige von SM-Fehlern definiert:

'66 88': Verifizierung der kryptografischen Prüfsumme fehlgeschlagen,

'69 87': erwartete SM-Datenobjekte fehlen,

'69 88': SM-Datenobjekte inkorrekt.

CSM_027 Sendet die Fahrtenschreiberkarte Statusbytes ohne SM-DO oder mit einem fehlerhaften SM-DO zurück, muss die VU den Vorgang abbrechen.

5.3. **Algorithmus zur Berechnung der kryptografischen Prüfsummen**

CSM_028 Kryptografische Prüfsummen werden unter Verwendung eines üblichen MAC gemäß ANSI X9.19 mit DES aufgebaut:

— Ausgangsstufe: Der Ausgangsprüfblock y0 ist E(Ka, SSC).

— Folgestufe: Unter Verwendung von Ka werden die Prüfblöcke y1, …, yn berechnet.

— Endstufe: Die kryptografische Prüfsumme wird aus dem letzten Prüfblock yn wie folgt berechnet: E(Ka, D(Kb, yn)).

E() bedeutet Verschlüsselung mit DES, und D() bedeutet Entschlüsselung mit DES.

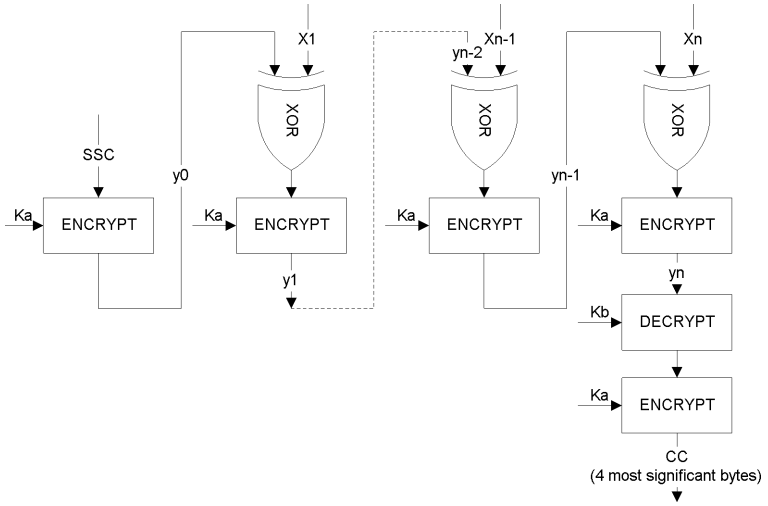
Die vier höchstwertigen Bytes der kryptografischen Prüfsumme werden übertragen.

CSM_029 Während der Schlüsselvereinbarung wird der „Send Sequence Counter" (Sendesequenzzähler, SSC) wie folgt initialisiert:

Anfangs-SSC: Rnd3 (4 niedrigstwertige Bytes) || Rnd1 (4 niedrigstwertige Bytes).

CSM_030 Vor jeder Berechnung eines MAC wird der SSC um 1 erhöht (d. h. der SSC für den ersten Befehl ist Anfangs-SSC + 1, der SSC für die erste Antwort Anfangs-SSC + 2).

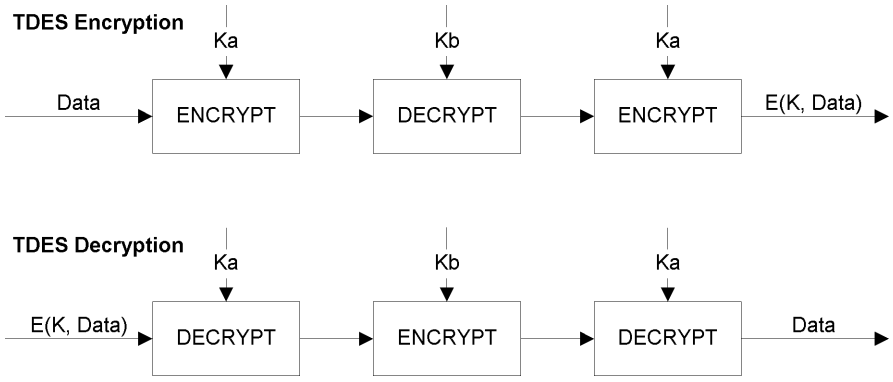
Die folgende Abbildung zeigt die Berechnung des MAC:



5.4. Algorithmus zur Berechnung von Kryptogrammen für Vertraulichkeits-DOs

CSM_031 Kryptogramme werden mit TDEA im Modus TCBC entsprechend den Referenzdokumenten TDES und TDES-OP sowie mit dem Nullvektor als Initial Value-Block berechnet.

Die folgende Abbildung zeigt die Anwendung von Schlüsseln in T-DES:



6. DIGITALE SIGNATURMECHANISMEN BEIM HERUNTERLADEN VON DATEN

CSM_032 Das Intelligent Dedicated Equipment (IDE) speichert die von einem Gerät (VU oder Karte) während eines Übertragungsvorgangs empfangenen Daten in einer Datei ab. Diese Datei muss die Zertifikate MS_i.C und EQT.C enthalten. Die Datei enthält digitale Signaturen von Datenblöcken gemäß Anlage 7, Protokolle zum Herunterladen der Daten.

CSM_033 Für die digitalen Signaturen heruntergeladener Daten wird ein digitales Signatursystem mit Anhang verwendet, sodass die heruntergeladenen Daten auf Wunsch ohne Dechiffrierung lesbar sind.

6.1. Erzeugung der Signatur

CSM_034 Die Erzeugung der Datensignatur durch das Gerät folgt dem in Referenzdokument PKCS1 definierten digitalen Signatursystem mit Anhang und der Hash-Funktion SHA-1:

Signatur = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = Füllstring von Oktetten mit Wert 'FF', sodass die Länge 128 beträgt.

DER(SHA-1(*M*)) ist die Kodierung der Algorithmus-ID für die Hash-Funktion und den Hash-Wert in einen ASN.1-Wert des Typs DigestInfo (Kodierungsregeln):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hash-Wert.

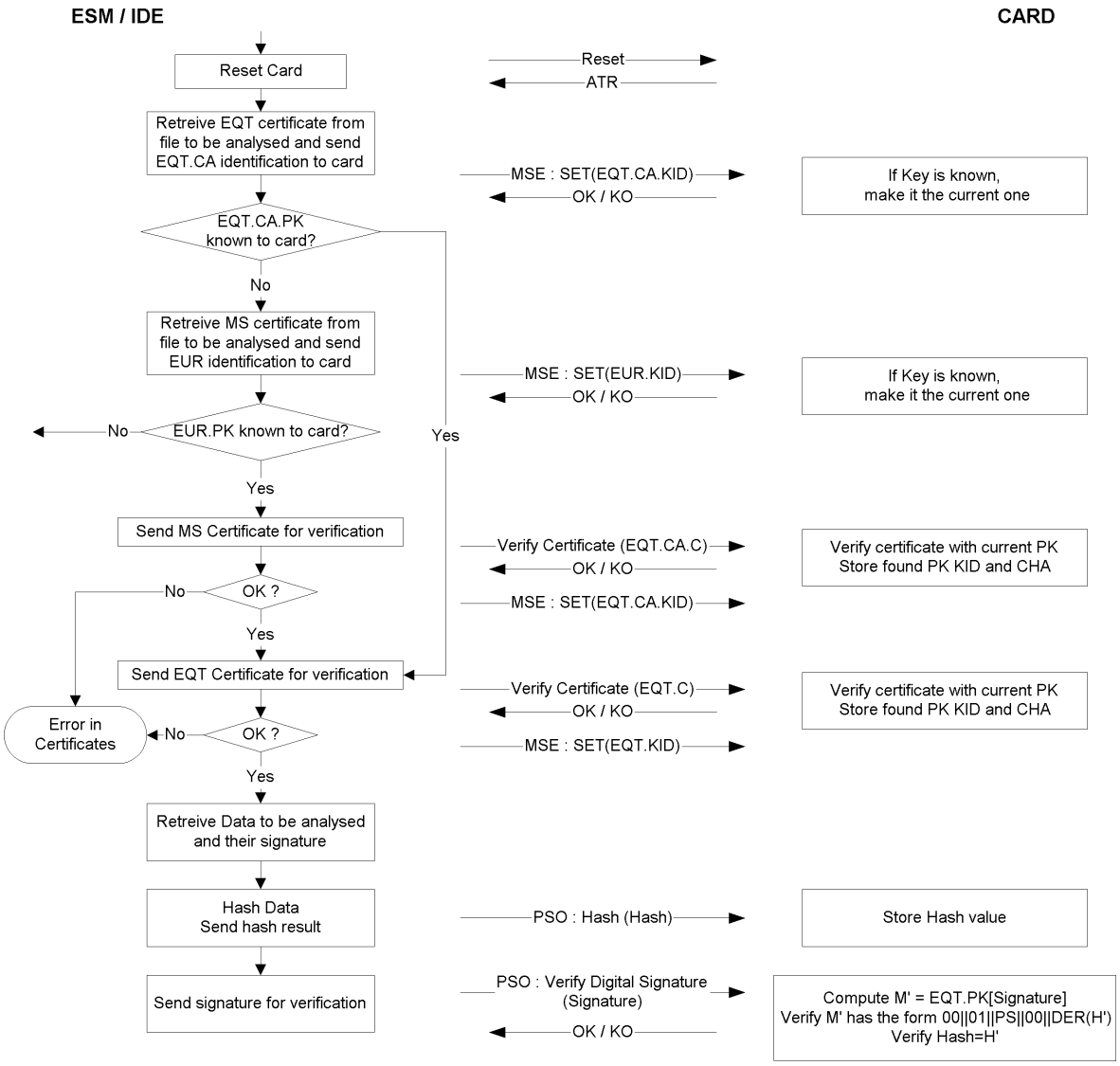
6.2. Verifizierung der Signatur

CSM_035 Die Verifizierung der Datensignatur bei heruntergeladenen Daten folgt dem in Referenzdokument PKCS1 definierten digitalen Signatursystem mit Anhang und der Hash-Funktion SHA-1.

Der europäische öffentliche Schlüssel EUR.PK muss dem Prüfer von unabhängiger Seite her (für ihn verlässlich) bekannt sein.

Die folgende Tabelle veranschaulicht das Protokoll, das von einem IDE mit Kontrollkarte zur Verifizierung der Integrität von heruntergeladenen und in ESM (externen Speichermedien) gespeicherten Daten herangezogen werden kann. Die Kontrollkarte wird zur Dechiffrierung digitaler Signaturen verwendet. Diese Funktion kann in diesem Fall nicht im IDE implementiert sein.

Das Gerät, das die zu analysierenden Daten heruntergeladen und signiert hat, ist mit EQT bezeichnet.



TEIL B

FAHRTENSCHREIBERSYSTEM DER 2. GENERATION

7. EINLEITUNG

7.1. **Referenzdokumente**

Referenzdokumente zu dieser Anlage:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), 26. November 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), Juli 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange (Identifikationskarten — Chipkarten — Teil 4 — Regeln, Sicherheitsfunktionen und Befehle für den Datenaustausch). Dritte Ausgabe 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations (Identifikationskarten — Chipkarten — Teil 8 — Kommandos für Sicherheitsoperationen). Zweite Ausgabe, 2004-06-01.
ISO 8825-1	ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) (Informationstechnik — Codierungsregeln für ASN.1: Spezifikation der Basis-Codierungsregeln (BER), der Kanonischen Codierungsregeln (CER) und der Besonderen Codierungsregeln (DER)). Vierte Ausgabe, 2008-12-15.
ISO 9797-1	ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanismen using a block cipher (Informationstechnik — Sicherheitsverfahren — Message Authentication Codes (MACs) — Teil 1 — Mechanismen, die eine Blockchiffre verwenden). Zweite Ausgabe, 2011-03-01.
ISO 10116	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an *n*-bit block cipher (Informationstechnik — Sicherheitsverfahren — Betriebsarten für n-bit Blockchiffre). Dritte Ausgabe, 2006-02-01.
ISO 16844-3	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface (Straßenfahrzeuge — Fahrtenschreibersysteme — Teil 3: Bewegungssensor-Schnittstelle). Erste Ausgabe 2004, einschließlich Technical Corrigendum 1 2006.
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, März 2009
RFC 5639	Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), Mai 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, März 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.00, 28.6.2012

7.2. **Notationen und Abkürzungen**

In dieser Anlage werden folgende Notationen und Abkürzungen verwendet:

AES	Advanced Encryption Standard
CA	Certification Authority (Zertifizierungsstelle)
CAR	Certification Authority Reference (Referenz der Zertifizierungsstelle)
CBC	Cipher Block Chaining (Betriebsmodus)

CH	Command Header (Befehlskopf)
CHA	Certificate Holder Authorisation (Autorisierung des Zertifikatsinhabers)
CHR	Certificate Holder Reference (Referenz des Zertifikatsinhabers)
CV	Constant Vector (Konstanter Vektor)
DER	Distinguished Encoding Rules (Besondere Codierungsregeln)
DO	Datenobjekt
DSRC	Dedicated Short Range Communication (Dedizierte Nahbereichskommunikation)
ECC	Elliptic Curve Cryptography (Elliptische-Kurven-Kryptografie)
ECDSA	Elliptic Curve Digital Signature Algorithm (auf elliptischen Kurven basierender Algorithmus für digitale Signaturen)
ECDH	Elliptic Curve Diffie-Hellman (Diffie-Hellman-Schlüsselaustausch)
EGF	External GNSS Facility (Externe GNSS-Ausrüstung)
EQT	Equipment (Gerät)
IDE	Intelligent Dedicated Equipment
K_M	Bewegungssensor-Hauptschlüssel, ermöglicht die Koppelung einer Fahrzeugeinheit mit einem Bewegungssensor
$K_{M\text{-}VU}$	In Fahrzeugeinheiten eingesetzter Schlüssel, der es einer VU gestattet, den Bewegungssensor-Hauptschlüssel abzuleiten, wenn eine Werkstattkarte in die VU eingesetzt ist
$K_{M\text{-}VC}$	In Werkstattkarten eingesetzter Schlüssel, der es einer VU gestattet, den Bewegungssensor-Hauptschlüssel abzuleiten, wenn eine Werkstattkarte in die VU eingesetzt ist
MAC	Message Authentication Code
MoS	Bewegungssensor
MSB	Most Significant Bit (höchstwertige Bitposition)
PKI	Public Key Infrastructure (Public-Key-Infrastruktur)
RCF	Remote Communication Facility (Ausrüstung zur Fernkommunikation)
SSC	Send Sequence Counter (Sendesequenzzähler)
SM	Secure Messaging
TDES	Triple Data Encryption Standard (Triple-Datenverschlüsselungsstandard)
TLV	Tag Length Value (Taglängenwert)
VU	Fahrzeugeinheit (Vehicle Unit, VU)
X.C	Zertifikat des öffentlichen Schlüssels von Benutzer X
X.CA	Zertifizierungsstelle, die das Zertifikat von Benutzer X ausgestellt hat
X.CA	die im Zertifikat von Benutzer X erwähnte Referenz der Zertifizierungsstelle
X.CA	die im Zertifikat von Benutzer X erwähnte Referenz des Zertifikatsinhabers
X.PK	öffentlicher Schlüssel von Benutzer X
X.SK	privater Schlüssel von Benutzer X
$X.PK_{eph}$	flüchtiger öffentlicher Schlüssel von Benutzer X
$X.SK_{eph}$	flüchtiger privater Schlüssel von Benutzer X
‘xx’	ein Hexadezimalwert
||	Verkettungsoperator

7.3. **Begriffsbestimmungen**

Die in dieser Anlage verwendeten Begriffsbestimmungen sind in Anhang 1C Abschnitt I aufgeführt.

8. KRYPTOGRAFISCHE SYSTEME UND ALGORITHMEN

8.1. **Kryptografische Systeme**

CSM_38 Fahrzeugeinheiten und Fahrtenschreiberkarten verwenden ein auf elliptischen Kurven basierendes Public-Key-Verschlüsselungssystem, sodass folgende Sicherheitsmechanismen vorliegen:

— gegenseitige Authentisierung zwischen Fahrzeugeinheit und Karte,

— Vereinbarung von AES-Sitzungsschlüsseln zwischen Fahrzeugeinheit und Karte,

— Gewährleistung der Authentizität, Integrität und Nichtabstreitbarkeit der von Fahrzeugeinheiten oder Fahrtenschreiberkarten an externe Medien heruntergeladenen Daten.

CSM_39 Fahrzeugeinheiten und externe GNSS-Ausrüstung verwenden ein auf elliptischen Kurven basierendes Public-Key-Verschlüsselungssystem, sodass folgende Sicherheitsmechanismen vorliegen:

— Koppelung von Fahrzeugeinheit und externer GNSS-Ausrüstung,

— gegenseitige Authentisierung zwischen Fahrzeugeinheit und externer GNSS-Ausrüstung,

— Vereinbarung eines AES-Sitzungsschlüssels zwischen Fahrzeugeinheit und externer GNSS-Ausrüstung.

CSM_40 Fahrzeugeinheiten und Fahrtenschreiberkarten verwenden ein AES-basiertes symmetrisches Verschlüsselungssystem, sodass folgende Sicherheitsmechanismen vorliegen:

— Gewährleistung von Authentizität und Integrität der zwischen Fahrzeugeinheit und Fahrtenschreiberkarte ausgetauschten Daten,

— gegebenenfalls Gewährleistung der Vertraulichkeit der zwischen Fahrzeugeinheit und Fahrtenschreiberkarte ausgetauschten Daten.

CSM_41 Fahrzeugeinheiten und externe GNSS-Ausrüstung verwenden ein AES-basiertes symmetrisches Verschlüsselungssystem, sodass folgende Sicherheitsmechanismen vorliegen:

— Gewährleistung von Authentizität und Integrität der zwischen Fahrzeugeinheit und externer GNSS-Ausrüstung ausgetauschten Daten,

CSM_42 Fahrzeugeinheiten und Bewegungssensoren verwenden ein AES-basiertes symmetrisches Verschlüsselungssystem, sodass folgende Sicherheitsmechanismen vorliegen:

— Koppelung von Fahrzeugeinheit und Bewegungssensor,

— gegenseitige Authentisierung zwischen Fahrzeugeinheit und Bewegungssensor,

— Gewährleistung der Vertraulichkeit der zwischen Fahrzeugeinheit und Bewegungssensor ausgetauschten Daten.

CSM_43 Fahrzeugeinheiten und Kontrollkarten verwenden ein AES-basiertes symmetrisches Verschlüsselungssystem, sodass an der Schnittstelle für die Fernkommunikation folgende Sicherheitsmechanismen vorliegen:

— Gewährleistung von Vertraulichkeit, Authentizität und Integrität der von der Fahrzeugeinheit an die Kontrollkarte übermittelten Daten.

Hinweise:

— Genau genommen werden die Daten von einer Fahrzeugeinheit unter Aufsicht eines Kontrolleurs mithilfe einer VU-internen oder -externen Ausrüstung zur Fernkommunikation an die Fernabfrageeinrichtung übermittelt (siehe Anlage 14). Allerdings sendet die Fernabfrageeinrichtung die erhaltenen Daten zwecks Entschlüsselung und Validierung der Authentizität an eine Kontrollkarte. Im Hinblick auf die Sicherheit sind die Ausrüstung zur Fernkommunikation und die Fernabfrageeinrichtung vollständig transparent.

— Eine Werkstattkarte bietet die gleichen Sicherheitsmechanismen für die DSRC-Schnittstelle wie eine Kontrollkarte. Dadurch kann eine Werkstatt überprüfen, ob die Schnittstelle für die Fernkommunikation einer VU ordnungsgemäß funktioniert und sicher ist. Weitere Informationen siehe Abschnitt 9.2.2.

8.2. **Kryptografische Algorithmen**

8.2.1 *Symmetrische Algorithmen*

CSM_44 Fahrzeugeinheiten, Fahrtenschreiberkarten, Bewegungssensoren und externe GNSS-Ausrüstung unterstützen den in Referenzdokument AES definierten AES-Algorithmus, mit Schlüssellängen von 128, 192 und 256 Bits.

8.2.2 *Asymmetrische Algorithmen und standardisierte Domänenparameter*

CSM_45 Fahrzeugeinheiten, Fahrtenschreiberkarten und externe GNSS-Ausrüstung unterstützen Elliptische-Kurven-Kryptografie mit einer Schlüsselgröße von 256, 384 und 512/521 Bits.

CSM_46 Fahrzeugeinheiten, Fahrtenschreiberkarten und externe GNSS-Ausrüstung unterstützen den ECDSA Signaturalgorithmus gemäß Referenzdokument DSS.

CSM_47 Fahrzeugeinheiten, Fahrtenschreiberkarten und externe GNSS-Ausrüstung unterstützen den ECKA-EG-Algorithmus zur Schlüsselvereinbarung gemäß Referenzdokument TR 03111.

CSM_48 Fahrzeugeinheiten, Fahrtenschreiberkarten und externe GNSS-Ausrüstung unterstützen sämtliche standardisierte Domänenparameter gemäß Tabelle 1 unten für Elliptische-Kurven-Kryptografie.

Tabelle 1

Standardisierte Domänenparameter

Name	Größe (Bits)	Referenzdokument	Objektkennung
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Hinweis: Die in der letzten Spalte von Tabelle 1 genannten Objektkennungen sind in Referenzdokument RFC 5639 für Brainpool-Kurven und in Referenzdokument RFC 5480 für NIST-Kurven angegeben.

Beispiel 1: Die Objektkennung für die Kurve BrainpoolP256r1 lautet

```
{iso(1)
        identified-organization(3) teletrust(36) algorithm(3)
 signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8)
                            ellipticCurve(1) versionOne(1) 7}.
```

Beziehungsweise in Punktnotation: `1.3.36.3.3.2.8.1.1.7.`

Beispiel 2: Die Objektkennung für die Kurve NIST P-384 lautet

```
{iso(1) identified-organization(3) certicom(132) curve(0) 34}.
```

Beziehungsweise in Punktnotation: `1.3.132.0.34.`

8.2.3 *Hash-Algorithmen*

CSM_49 Fahrzeugeinheiten und Fahrtenschreiberkarten unterstützen die Algorithmen SHA-256, SHA-384 und SHA-512 gemäß Referenzdokument SHS.

8.2.4 *Cipher Suites*

CSM_50 Wenn ein symmetrischer Algorithmus, ein asymmetrischer Algorithmus und/oder ein Hash-Algorithmus zusammen ein Sicherheitsprotokoll bilden, haben ihre jeweiligen Schlüssellängen und Hashgrößen (grob) die gleiche Stärke aufzuweisen. Tabelle 2 zeigt die zulässigen Cipher Suites:

Tabelle 2

Zulässige Cipher Suites

Kennung der Cipher Suite	ECC-Schlüsselgröße (Bits)	AES-Schlüssellänge (Bits)	Hash-Algorithmus	MAC-Länge (Bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Hinweis: ECC-Schlüsselgrößen von 512 Bits und 521 Bits gelten im Sinne dieser Anlage als gleich stark.

9. SCHLÜSSEL UND ZERTIFIKATE

9.1. **Asymmetrische Schlüsselpaare und Public-Key-Zertifikate**

9.1.1 *Allgemein*

Hinweis: Die in diesem Abschnitt beschriebenen Schlüssel werden zur gegenseitigen Authentisierung und zum Secure Messaging zwischen den Fahrzeugeinheiten und den Fahrtenschreiberkarten sowie zwischen den Fahrzeugeinheiten und externer GNSS-Ausrüstung verwendet. Diese Vorgänge werden detailliert in den Kapiteln 10 und 11 dieser Anlage beschrieben.

CSM_51 Beim europäischen intelligenten Fahrtenschreibersystem werden die ECC-Schlüsselpaare und die entsprechenden Zertifikate auf drei hierarchischen Funktionsebenen erzeugt und verwaltet:

— auf europäischer Ebene,

— auf Mitgliedstaatebene,

— auf Geräteebene.

CSM_52 Im gesamten europäischen intelligenten Fahrtenschreibersystem werden öffentliche und private Schlüssel sowie Zertifikate mithilfe genormter und sicherer Methoden erzeugt, verwaltet und kommuniziert.

9.1.2 *Europäische Ebene*

CSM_53 Auf europäischer Ebene wird ein einziges ECC-Schlüsselpaar (EUR) erzeugt. Es besteht aus einem privaten (EUR.SK) und einem öffentlichen Schlüssel (EUR.PK). Dieses Schlüsselpaar bildet das Wurzel-Schlüsselpaar der gesamten europäischen intelligenten Fahrtenschreiber-PKI. Diese Aufgabe wird von einer Europäischen Wurzel-Zertifizierungsstelle (ERCA) wahrgenommen, die der Europäischen Kommission untersteht.

CSM_54 Die ERCA verwendet den europäischen privaten Schlüssel, um ein (selbstsigniertes) Wurzelzertifikat des europäischen öffentlichen Schlüssels zu signieren, und übermittelt dieses europäische Wurzelzertifikat an alle Mitgliedstaaten.

CSM_55 Die ERCA verwendet den europäischen privaten Schlüssel, um auf Anfrage die Zertifikate der öffentlichen Schlüssel der Mitgliedstaaten zu signieren. Die ERCA führt ein Verzeichnis aller signierten Public-Key-Zertifikate der Mitgliedstaaten.

CSM_56 Wie in Abbildung 1 (Abschnitt 9.1.7) dargestellt, erzeugt die ERCA alle 17 Jahre ein neues europäisches Wurzel-Schlüsselpaar. Immer, wenn die ERCA ein neues europäisches Wurzel-Schlüsselpaar erzeugt, erstellt es ein neues selbstsigniertes Wurzelzertifikat für den neuen europäischen öffentlichen Schlüssel. Die Gültigkeitsdauer eines europäischen Wurzelzertifikats beträgt 34 Jahre und 3 Monate.

Hinweis: Die Einführung eines neuen Wurzel-Schlüsselpaares bedeutet auch, dass die ERCA einen neuen Bewegungssensor-Hauptschlüssel und einen neuen DSRC-Hauptschlüssel erzeugt, siehe Abschnitte 9.2.1.2 und 9.2.2.2.

CSM_57 Bevor ein neues europäisches Wurzel-Schlüsselpaar erzeugt wird, analysiert die ERCA die für das neue Schlüsselpaar erforderliche kryptografische Stärke, da dieses die kommenden 34 Jahre Sicherheit bieten soll. Wenn nötig, wechselt die ERCA zu einer Cipher Suite, die stärker als die aktuelle ist, wie in CSM_50 festgelegt.

CSM_58 Immer, wenn die ERCA ein neues europäisches Wurzel-Schlüsselpaar erzeugt, muss es ein Linkzertifikat für den neuen europäischen öffentlichen Schlüssel erstellen und dieses mit dem ehemaligen privaten Schlüssel signieren. Die Gültigkeitsdauer des Linkzertifikats beträgt 17 Jahre. Dies wird auch in Abbildung 1 (Abschnitt 9.1.7) gezeigt.

Hinweis: Da ein Linkzertifikat den öffentlichen Schlüssel der Generation *X* von ERCA enthält und mit dem privaten Schlüssel der Generation *X-1* von ERCA signiert ist, bietet ein Linkzertifikat Ausrüstung, die im Laufe der Generation *X-1* herausgegeben wurde, eine Möglichkeit, im Laufe der Generation *X* herausgegebener Ausrüstung zu vertrauen.

CSM_59 Die ERCA darf in keinem Fall den privaten Schlüssel eines Wurzel-Schlüsselpaares verwenden, sobald die neuen Wurzelzertifikate Gültigkeit erlangen.

CSM_60 Die ERCA muss jederzeit über folgende kryptografische Schlüssel und Zertifikate verfügen:

— das aktuelle EUR-Schlüsselpaar samt zugehörigem Zertifikat

— sämtliche vorherigen EUR-Vorgängerzertifikate, die zur Verifizierung noch gültiger MSCA-Zertifikate verwendet werden sollen

— Linkzertifikate aller Generationen von EUR-Linkzertifikaten mit Ausnahme des ersten

9.1.3 *Mitgliedstaatebene*

CSM_61 Auf Mitgliedstaatebene müssen alle Mitgliedstaaten, die zur Signierung von Fahrtenschreiberkarten-zertifikaten verpflichtet sind, eines oder mehrere einzigartige ECC-Schlüsselpaare erzeugen, das mit MSCA_Card bezeichnet wird. Alle Mitgliedstaaten, die zur Signierung von Zertifikaten für Fahrzeugeinheiten oder externe GNSS-Ausrüstung verpflichtet sind, müssen zusätzlich eines oder mehrere einzigartige ECC-Schlüsselpaare erzeugen, das mit MSCA_VU-EGF bezeichnet wird.

CSM_62 Die Aufgabe, Mitgliedstaat-Schlüsselpaare zu erzeugen, wird durch eine Zertifizierungsstelle des jeweiligen Mitgliedstaates (Member State Certificate Authority, MSCA) übernommen. Immer, wenn eine MSCA ein Mitgliedstaat-Schlüsselpaar erzeugt, übermittelt sie den öffentlichen Schlüssel an die ERCA, um ein entsprechendes durch die ERCA signiertes Mitgliedstaatzertifikat zu erhalten.

CSM_63 Die MSCA wählt die Stärke eines Mitgliedstaat-Schlüsselpaars so, dass sie derjenigen des europäischen Wurzel-Schlüsselpaars entspricht, das zur Signierung des zugehörigen Mitgliedstaatzertifikats verwendet wird.

CSM_64 Ein gegebenenfalls vorhandenes MSCA_VU-EGF-Schlüsselpaar besteht aus dem privaten Schlüssel MSCA_VU-EGF.SK und dem öffentlichen Schlüssel MSCA_VU-EGF.PK. Eine MSCA darf den privaten Schlüssel MSCA_VU-EGF.SK ausschließlich dazu nutzen, die Public-Key-Zertifikate von Fahrzeugeinheiten und externer GNSS-Ausrüstung zu signieren.

CSM_65 Ein MSCA_Card-Schlüsselpaar besteht aus einem privaten (MSCA_Card.SK) und einem öffentlichen Schlüssel (MSCA_Card.PK). Eine MSCA darf den privaten Schlüssel MSCA_Card.SK ausschließlich dazu nutzen, die Public-Key-Zertifikate von Fahrtenschreiberkarten zu signieren.

CSM_66 Eine MSCA muss Aufzeichnungen über alle signierten VU-Zertifikate, externen GNSS-Ausrüstungs-Zertifikate und Kartenzertifikate sowie die Kennung der Geräte, für die jedes dieser Zertifikate bestimmt ist, aufbewahren.

CSM_67 Die Gültigkeitsdauer eines MSCA_VU-EGF-Zertifikats beträgt 17 Jahre und 3 Monate. Die Gültigkeitsdauer eines MSCA_Card-Zertifikats beträgt 7 Jahre und 1 Monat.

CSM_68 Wie in Abbildung 1 (Abschnitt 9.1.7) dargestellt, beträgt die Nutzungsdauer eines privaten Schlüssels eines MSCA_VU-EGF-Schlüsselpaares und eines privaten Schlüssels eines MSCA_Card-Schlüsselpaares zwei Jahre.

CSM_69 Das MSCA darf in keinem Fall den privaten Schlüssel eines MSCA_VU-EGF-Schlüsselpaares verwenden, sobald die Nutzungsdauer abgelaufen ist. Ebenso wenig darf das MSCA den privaten Schlüssel eines MSCA_Card-Schlüsselpaares verwenden, sobald die Nutzungsdauer abgelaufen ist.

CSM_70 Das MSCA muss jederzeit über folgende kryptografische Schlüssel und Zertifikate verfügen:

— das aktuelle MSCA_Card-Schlüsselpaar samt zugehörigem Zertifikat

— sämtliche vorherigen MSCA_Card-Vorgängerzertifikate, die zur Verifizierung noch gültiger Zertifikate für Fahrtenschreiberkarten verwendet werden sollen

— das für die Verifizierung des aktuellen MSCA-Zertifikats erforderliche aktuelle EUR-Zertifikat

— sämtliche vorherigen EUR-Vorgängerzertifikate, die zur Verifizierung noch gültiger MSCA-Zertifikate erforderlich sind

CSM_71 Wenn eine MSCA Zertifikate für Fahrzeugeinheiten oder externe GNSS-Ausrüstung signiert, muss sie zusätzlich über folgende Schlüssel und Zertifikate verfügen:

— das aktuelle MSCA_VU-EGF-Schlüsselpaar samt zugehörigem Zertifikat

— sämtliche vorherigen öffentlichen MSCA_VU-EGF-Schlüssel, die zur Verifizierung noch gültiger Zertifikate von VU oder externer GNSS-Ausrüstung verwendet werden sollen

9.1.4 *Geräteebene: Fahrzeugeinheiten*

CSM_72 Für jede Fahrzeugeinheit müssen zwei eindeutige ECC-Schlüsselpaare erzeugt werden, die als VU_MA und VU_Sign bezeichnet werden. Diese Aufgabe wird von den Herstellern der VU übernommen. Immer wenn ein VU-Schlüsselpaar erzeugt wird, übermittelt die erzeugende Partei den öffentlichen Schlüssel an die MSCA des Landes, in dem sie ihren Sitz hat, um das entsprechende durch die MSCA signierte VU-Zertifikat zu erhalten. Der private Schlüssel darf nur durch die Fahrzeugeinheit genutzt werden.

CSM_73 Die Zertifikate VU_MA und VU_Sign jeder gegebenen Fahrzeugeinheit müssen das gleiche Certificate Effective Date aufweisen.

CSM_74 Der VU-Hersteller wählt die Stärke eines VU-Schlüsselpaars so, dass sie derjenigen des MSCA-Schlüsselpaars entspricht, das zur Signierung des zugehörigen VU-Zertifikats verwendet wird.

CSM_75 Fahrzeugeinheiten dürfen ihr aus dem privaten Schlüssel VU_MA.SK und dem öffentlichen Schlüssel VU_MA.PK bestehendes VU_MA-Schlüsselpaar ausschließlich dazu verwenden, die VU-Authentisierung gegenüber Fahrtenschreiberkarten und externer GNSS-Ausrüstung durchzuführen, wie in den Abschnitten 10.3 und 11.4 dieser Anlage beschrieben.

CSM_76 Fahrzeugeinheiten müssen in der Lage sein, flüchtige ECC-Schlüsselpaare, zu erzeugen und dürfen ein flüchtiges Schlüsselpaar ausschließlich dazu nutzen, eine Sitzungsschlüsselvereinbarung mit einer Fahrtenschreiberkarte oder externer GNSS-Ausrüstung durchzuführen, wie in den Abschnitten 10.4 und 11.4 dieser Anlage beschrieben.

CSM_77 Fahrzeugeinheiten nutzen den privaten Schlüssel VU_Sign.SK des VU_Sign-Schlüsselpaars ausschließlich dazu, heruntergeladene Datendateien zu signieren, wie in Kapitel 14 dieser Anlage beschrieben. Der zugehörige öffentliche Schlüssel VU_Sign.PK darf nur dazu genutzt werden, Signaturen, die durch die Fahrzeugeinheit erzeugt wurden, zu verifizieren.

CSM_78 Wie in Abbildung 1 (Abschnitt 9.1.7) dargestellt, beträgt die Gültigkeitsdauer eines VU_MA-Zertifikats 15 Jahre und 3 Monate. Die Gültigkeitsdauer eines VU_Sign-Zertifikats beträgt ebenfalls 15 Jahre und 3 Monate.

Hinweise:

— Die erweiterte Gültigkeitsdauer eines VU_Sign-Zertifikats ermöglicht es einer Fahrzeugeinheit, während der ersten drei Monate nach Ablauf gültige Signaturen für heruntergeladene Daten zu erzeugen, wie in der Verordnung (EU) Nr. 581/2010 vorgeschrieben.

— Die erweiterte Gültigkeitsdauer eines VU_MA-Zertifikats ist erforderlich, um der VU die Authentisierung gegenüber einer Kontroll- oder Unternehmenskarte während der ersten drei Monate nach Ablauf zu ermöglichen, sodass es möglich ist, Daten herunterzuladen.

CSM_79 Nach Ablauf der Gültigkeitsdauer des entsprechenden Zertifikats darf die Fahrzeugeinheit den privaten Schlüssel eines VU-Schlüsselpaars keinesfalls verwenden.

CSM_80 Die VU-Schlüsselpaare (mit Ausnahme flüchtiger Schlüsselpaare) und zugehörigen Zertifikate einer gegebenen Fahrzeugeinheit dürfen nicht bei der Praxisanwendung ausgetauscht oder erneuert werden, sobald das Fahrzeug in Betrieb genommen wurde.

Hinweise:

— Flüchtige Schlüsselpaare sind nicht Teil dieser Anforderung, da eine VU jedes Mal, wenn eine Chip-Authentisierung und eine Sitzungsschlüsselvereinbarung durchgeführt werden, ein neues flüchtiges Schlüsselpaar erzeugt (siehe Abschnitt 10.4). Die flüchtigen Schlüsselpaare verfügen nicht über zugehörige Zertifikate.

— Diese Anforderung verbietet nicht die Möglichkeit, im Rahmen einer Modernisierung oder Reparatur in einer sicheren, vom VU-Hersteller kontrollierten Umgebung statische VU-Schlüsselpaare zu ersetzen.

CSM_81 Im Betrieb müssen die Fahrzeugeinheiten die folgenden kryptografischen Schlüssel und Zertifikate enthalten:

— den privaten VU_MA-Schlüssel samt zugehörigem Zertifikat

— den privaten VU_Sign-Schlüssel samt zugehörigem Zertifikat

— das MSCA_VU-EGF-Zertifikat mit dem öffentlichen MSCA_VU-EGF.PK-Schlüssel zur Verifizierung des VU_MA-Zertifikats und des VU_Sign-Zertifikats

— das EUR-Zertifikat mit dem öffentlichen EUR.PK-Schlüssel zur Verifizierung des MSCA_VU-EGF-Zertifikats

— das EUR-Zertifikat, dessen Gültigkeitsdauer direkt der Gültigkeitsdauer des zur Verifizierung des MSCA_VU-EGF-Zertifikats zu verwendenden EUR-Zertifikats vorausgeht, falls vorhanden

— das Linkzertifikat, das diese beiden EUR-Zertifikate verbindet, sofern vorhanden

CSM_82 Über die in CSM_81 aufgeführten kryptografischen Schlüssel und Zertifikate hinaus müssen die Fahrzeugeinheiten zudem die in Teil A dieser Anlage aufgeführten Schlüssel und Zertifikate enthalten, damit eine Fahrzeugeinheit mit Fahrtenschreiberkarten der 1. Generation interagieren kann.

9.1.5 *Geräteebene: Fahrtenschreiberkarten*

CSM_83 Für jede Fahrtenschreiberkarte wird ein eindeutiges ECC-Schlüsselpaar unter dem Namen Card_MA erzeugt. Zusätzlich wird für jede Fahrerkarte und jede Werkstattkarte ein zweites eindeutiges ECC-Schlüsselpaar unter dem Namen Card_Sign erzeugt. Diese Aufgabe kann von den Kartenherstellern oder -integratoren übernommen werden. Immer wenn ein Kartenschlüsselpaar erzeugt wird, übermittelt die erzeugende Partei den öffentlichen Schlüssel an die MSCA des Landes, in dem sie ihren Sitz hat, um das entsprechende durch die MSCA signierte Kartenzertifikat zu erhalten. Der private Schlüssel darf nur durch die Fahrtenschreiberkarte genutzt werden.

CSM_84 Die Zertifikate Card_MA und Card_Sign jeder gegebenen Fahrer- oder Werkstattkarte müssen das gleiche Certificate Effective Date aufweisen.

CSM_85 Der Kartenhersteller oder -integrator wählt die Stärke eines Kartenschlüsselpaars so, dass sie derjenigen des MSCA-Schlüsselpaars entspricht, das zur Signierung des zugehörigen Kartenzertifikats verwendet wird.

CSM_86 Fahrtenschreiberkarten dürfen ihr aus dem privaten Schlüssel Card_MA.SK und dem öffentlichen Schlüssel Card_MA.PK bestehendes Card_MA-Schlüsselpaar ausschließlich dazu verwenden, die gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung gegenüber Fahrzeugeinheiten durchzuführen, wie in den Abschnitten 10.3 und 10.4 dieser Anlage beschrieben.

CSM_87 Fahrer- oder Werkstattkarten nutzen den privaten Schlüssel Card_Sign.SK des Card_Sign-Schlüsselpaars ausschließlich dazu, heruntergeladene Datendateien zu signieren, wie in Kapitel 14 dieser Anlage beschrieben. Der zugehörige öffentliche Schlüssel Card_Sign.PK darf nur dazu genutzt werden, Signaturen, die durch die Karte erzeugt wurden, zu verifizieren.

CSM_88 Die Gültigkeitsdauer des Card-MA-Zertifikats lautet wie folgt:

— Fahrerkarten: 5 Jahre

— Unternehmenskarten: 2 Jahre

— Kontrollkarten: 2 Jahre

— Werkstattkarten: 1 Jahr

CSM_89 Die Gültigkeitsdauer des Card-Sign-Zertifikats lautet wie folgt:

— Fahrerkarten: 5 Jahre und 1 Monat

— Werkstattkarten: 1 Jahr und 1 Monat

Hinweis: Die erweiterte Gültigkeitsdauer eines Card_Sign-Zertifikats ermöglicht es einer Fahrerkarte, während des ersten Monats nach Ablauf gültige Signaturen für heruntergeladene Daten zu erzeugen. Dies ist aufgrund der Verordnung (EU) Nr. 581/2010 erforderlich, nach der das Herunterladen von Daten einer Fahrerkarte bis 28 Tage nach Aufzeichnung der letzten Tage möglich sein muss.

CSM_90 Die Schlüsselpaare und entsprechenden Zertifikate einer Fahrtenschreiberkarte dürfen nicht mehr ersetzt oder erneuert werden, sobald die Karte ausgegeben ist.

CSM_91 Nach der Ausgabe müssen die Fahrtenschreiberkarten die folgenden kryptografischen Schlüssel und Zertifikate enthalten:

— den privaten Card_MA-Schlüssel samt zugehörigem Zertifikat

— Zusätzlich für Fahrerkarten und Werkstattkarten: der private Card_Sign-Schlüssel und das entsprechende Zertifikat

— das MSCA_Card-Zertifikat mit dem öffentlichen MSCA_Card.PK-Schlüssel zur Verifizierung des Card_MA-Zertifikats und des Card_Sign-Zertifikats

— das EUR-Zertifikat mit dem öffentlichen EUR.PK-Schlüssel zur Verifizierung des MSCA_Card-Zertifikats

— das EUR-Zertifikat, dessen Gültigkeitsdauer direkt der Gültigkeitsdauer des zur Verifizierung des MSCA_Card-Zertifikats zu verwendenden EUR-Zertifikats vorausgeht, falls vorhanden

— das Linkzertifikat, das diese beiden EUR-Zertifikate verbindet, sofern vorhanden.

CSM_92 Über die in CSM_91 aufgeführten kryptografischen Schlüssel und Zertifikate hinaus müssen die Fahrtenschreiberkarten zudem die in Teil A dieser Anlage aufgeführten Schlüssel und Zertifikate enthalten, damit diese Karten mit Fahrzeugeinheiten der 1. Generation interagieren können.

9.1.6 *Geräteebene: Externe GNSS-Ausrüstung*

CSM_93 Für jede externe GNSS-Ausrüstung wird ein eindeutiges ECC-Schlüsselpaar unter dem Namen EGF_MA erzeugt. Diese Aufgabe wird von den Herstellern der externen GNSS-Ausrüstung übernommen. Immer wenn ein EGF-MA-Schlüsselpaar erzeugt wird, wird der öffentliche Schlüssel an die MSCA des jeweiligen Landes übermittelt, um das entsprechende durch die MSCA signierte EGF-MA-Zertifikat zu erhalten. Der private Schlüssel darf nur durch die externe GNSS-Ausrüstung genutzt werden.

CSM_94 Der EGF-Hersteller wählt die Stärke eines EGF_MA-Schlüsselpaars so, dass sie derjenigen des MSCA-Schlüsselpaars entspricht, das zur Signierung des zugehörigen EGF-MA-Zertifikats verwendet wird.

CSM_95 Externe GNSS-Ausrüstung darf ihr aus dem privaten Schlüssel EGF_MA.SK und dem öffentlichen Schlüssel EGF_MA.PK bestehendes EGF_MA-Schlüsselpaar ausschließlich dazu verwenden, die gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung gegenüber Fahrzeugeinheiten durchzuführen, wie in den Abschnitten 11.4 und 11.4 dieser Anlage beschrieben.

CSM_96 Die Gültigkeitsdauer des EGF_MA-Zertifikats beträgt 15 Jahre.

CSM_97 Eine externe GNSS-Ausrüstung darf den privaten Schlüssel ihres EGF_MA Schlüsselpaars nicht zur Koppelung mit einer Fahrzeugeinheit verwenden, wenn das entsprechende Zertifikat abgelaufen ist.

Hinweis: Wie in Abschnitt 11.3.3 erläutert, kann eine externe GNSS-Ausrüstung ihren privaten Schlüssel möglicherweise auch nach Ablauf des entsprechenden Zertifikats gegenüber der VU verwenden, mit der sie bereits gekoppelt ist.

CSM_98 EGF_MA-Schlüsselpaar und zugehöriges Zertifikat einer gegebenen externen GNSS-Ausrüstung dürfen nicht bei der Praxisanwendung ausgetauscht oder erneuert werden, sobald die EGF in Betrieb genommen wurde.

Hinweis: Diese Anforderung verbietet nicht die Möglichkeit, im Rahmen einer Modernisierung oder Reparatur in einer sicheren, vom EGF-Hersteller kontrollierten Umgebung EGF-Schlüsselpaare zu ersetzen.

CSM_99 Im Betrieb muss eine externe GNSS-Ausrüstung die folgenden kryptografischen Schlüssel und Zertifikate enthalten:

— den privaten EGF_MA-Schlüssel samt zugehörigem Zertifikat

— das MSCA_VU-EGF-Zertifikat mit dem öffentlichen MSCA_VU-EGF.PK-Schlüssel zur Verifizierung des EGF_MA-Zertifikats

— das EUR-Zertifikat mit dem öffentlichen EUR.PK-Schlüssel zur Verifizierung des MSCA_VU-EGF-Zertifikats

— das EUR-Zertifikat, dessen Gültigkeitsdauer direkt der Gültigkeitsdauer des zur Verifizierung des MSCA_VU-EGF-Zertifikats zu verwendenden EUR-Zertifikats vorausgeht, falls vorhanden

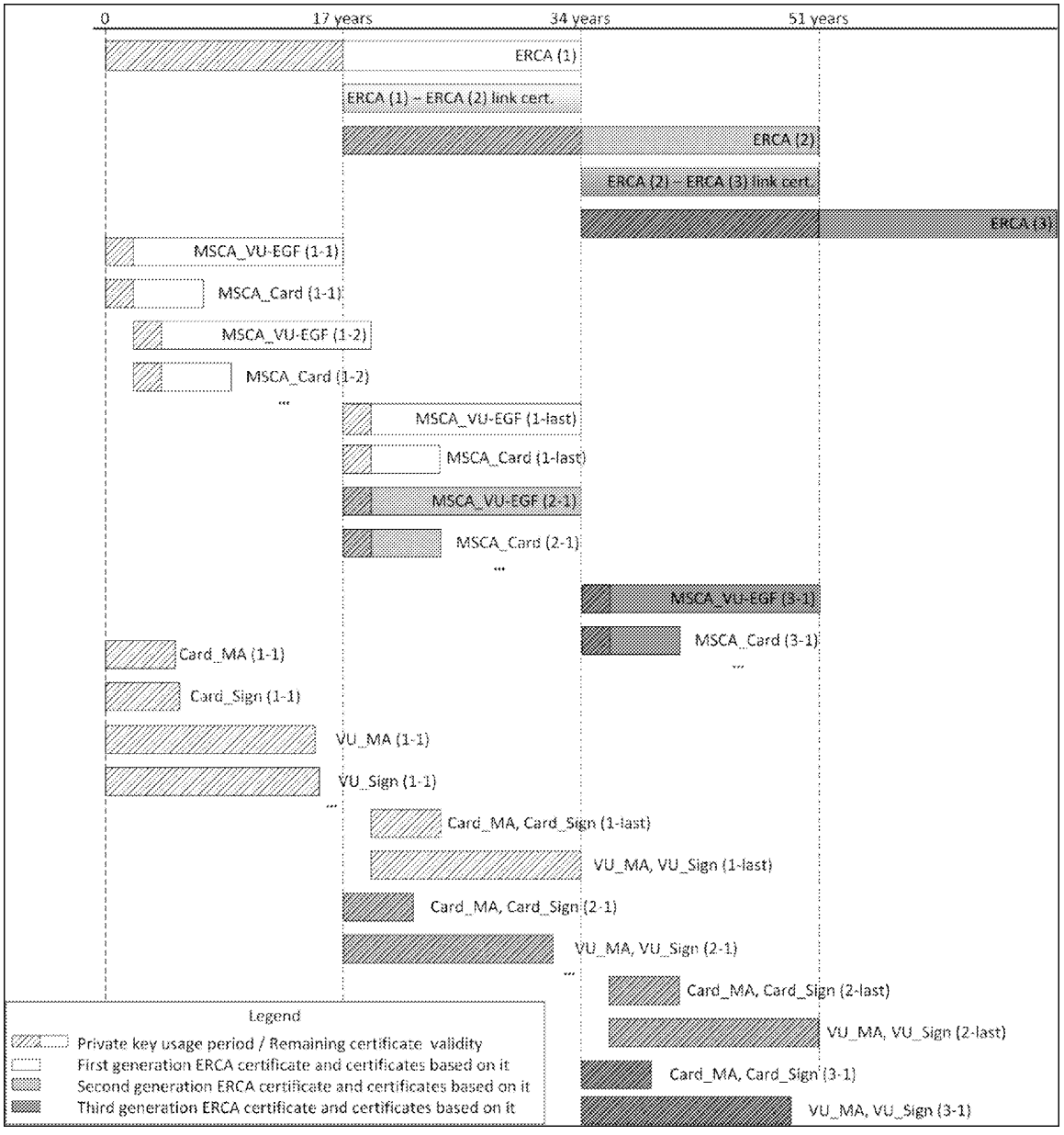
— das Linkzertifikat, das diese beiden EUR-Zertifikate verbindet, sofern vorhanden

9.1.7 *Überblick Ersatz von Zertifikaten*

In der untenstehenden Abbildung 1 ist dargestellt, wie die verschiedenen Generationen von ERCA-Wurzelzertifikaten, ERCA-Linkzertifikaten, MSCA-Zertifikaten und Ausrüstungszertifikaten (VU und Karte) im Laufe der Zeit ausgegeben und genutzt werden:

Abbildung 1

Ausgabe und Nutzung der verschiedenen Generationen von ERCA-Wurzelzertifikaten, ERCA-Linkzertifikaten, MSCA-Zertifikaten und Ausrüstungszertifikaten



Hinweise zu Abbildung 1:

1. Unterschiedliche Generationen des Wurzelzertifikats werden durch eine Zahl in Klammern dargestellt. Beispiel: ERCA (1) gibt die erste Generation des ERCA-Wurzelzertifikats an; ERCA (2) die zweite Generation usw.

2. Sonstige Zertifikate sind durch zwei Zahlen in Klammern dargestellt, wobei die erste Zahl die Generation des Wurzelzertifikats angibt, unter dem sie ausgestellt wurden, und die zweite Zahl die Generation des jeweiligen Zertifikats selbst. MSCA_Card (1-1) ist beispielsweise das erste unter ERCA (1) ausgestellte MSCA_Card-Zertifikat; MSCA_Card (2-1) ist das erste unter ERCA ausgestellte MSCA_Card-Zertifikat (2); MSCA_Card (2-last) ist das letzte unter ERCA (2) ausgestellte MSCA_Card-Zertifikat; Card_MA(2-1) ist das erste unter ERCA (2) ausgestellte Kartenzertifikat für die gegenseitige Authentisierung usw.

3. Die Zertifikate MSCA_Card (2-1) und MSCA_Card (1-last) werden fast, aber nicht exakt am selben Tag ausgestellt. MSCA_Card (2-1) ist das erste unter ERCA (2) ausgestellte MSCA_Card-Zertifikat und wird ein wenig später ausgestellt als MSCA_Card (1-last), dem letzten MSCA_Card-Zertifikat unter ERCA (1).

4. Wie in der Abbildung dargestellt, werden die ersten unter ERCA (2) ausgestellten VU- und Kartenzertifikate fast zwei Jahre, bevor die letzten VU- und Kartenzertifikate unter ERCA (1) ausgegeben werden, verfügbar sein. Grund dafür ist, dass VU- und Kartenzertifikate nicht direkt unter dem ERCA-Zertifikat, sondern unter einem MSCA-Zertifikat ausgestellt werden. Das MSCA (2-1) Zertifikat wird direkt nach Gültigkeitsbeginn von ERCA (2) ausgegeben; das Zertifikat MSCA (1-last) wird hingegen unmittelbar davor ausgestellt, im letzten Moment, zu dem das Zertifikat ERCA (1) noch gültig ist. Aus diesem Grund haben diese beiden MSCA-Zertifikate fast die gleiche Gültigkeitsdauer, gehören aber zu verschiedenen Generationen.

5. Die für Karten angegebene Gültigkeitsdauer entspricht derjenigen von Fahrerkarten (5 Jahre).

6. Aus Platzgründen ist die unterschiedliche Gültigkeitsdauer der Zertifikate Card_MA und Card_Sign sowie der Zertifikate VU_MA und VU_Sign nur für die 1. Generation angegeben.

9.2. **Symmetrische Schlüssel**

9.2.1 *Schlüssel für die Sicherung der Kommunikation VU-Bewegungssensor*

9.2.1.1 *Allgemein*

Hinweis: In diesem Abschnitt wird die Kenntnis des Inhalts von Referenzdokument ISO 16844-3 vorausgesetzt, in dem die Schnittstelle zwischen Fahrzeugeinheit und Bewegungssensor erläutert wird. Die Koppelung zwischen einer VU und einem Bewegungssensor wird in Kapitel 12 dieser Anlage detailliert beschrieben.

CSM_100 Eine Reihe symmetrischer Schlüssel wird zur Koppelung von Fahrzeugeinheiten und Bewegungssensoren, zur gegenseitigen Authentisierung zwischen Fahrzeugeinheiten und Bewegungssensoren sowie zur Verschlüsselung der Kommunikation zwischen Fahrzeugeinheiten und Bewegungssensoren benötigt (siehe Tabelle 3). Bei diesen Schlüsseln muss es sich stets um AES-Schlüssel handeln, deren Schlüssellänge derjenigen des Bewegungssensor-Hauptschlüssels entspricht, die wiederum an die Länge des (vorgesehenen) europäischen Wurzelschlüsselpaars angepasst ist (siehe CSM_50).

Tabelle 3

Schlüssel für die Sicherung der Kommunikation VU-Bewegungssensor

Schlüssel	Symbol	Generiert durch	Generierungsmethode	Gespeichert durch
Bewegungssensor-Hauptschlüssel — VU-Teil	$K_{M\text{-}VU}$	ERCA	Zufall	ERCA, an der Ausgabe von VU-Zertifikaten beteiligte MSCA, VU-Hersteller, Fahrzeugeinheiten

Schlüssel	Symbol	Generiert durch	Generierungsmethode	Gespeichert durch
Bewegungssensor-Hauptschlüssel — Werkstattteil	K_{M-WC}	ERCA	Zufall	ERCA, MSCA, Kartenhersteller, Werkstattkarten
Bewegungssensor-Hauptschlüssel	K_M	Nicht unabhängig generiert	Berechnet als $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, an der Ausgabe von Bewegungssensor-Schlüsseln beteiligte MSCA (fakultativ) (*)
Identifikationsschlüssel	K_{ID}	Nicht unabhängig generiert	Berechnet als $K_{ID} = K_M$ XOR CV (CV angegeben in CSM_106)	ERCA, an der Ausgabe von Bewegungssensor-Schlüsseln beteiligte MSCA (fakultativ) (*)
Koppelungsschlüssel	K_P	Hersteller von Bewegungssensoren	Zufall	Ein Bewegungssensor
Sitzungsschlüssel	K_S	VU (während der Koppelung von VU und Bewegungssensor)	Zufall	Eine VU und ein Bewegungssensor

(*) Die Speicherung von K_M und K_{ID} ist fakultativ, da diese Schlüssel von K_{M-VU}, K_{M-WC} und CV abgeleitet werden können.

CSM_101 Die Europäische Wurzel-Zertifizierungsstelle (ERCA) generiert K_{M-VU} und K_{M-WC}, zwei zufällig erzeugte und eindeutige AES-Schlüssel, aus denen sich der Bewegungssensor-Hauptschlüssel K_M als K_{M-VU} XOR K_{M-WC} berechnen lässt. Die ERCA teilt den Zertifizierungsstellen der Mitgliedstaaten die Schlüssel $K_{M,}$ K_{M-VU} und K_{M-WC} auf Anfrage mit.

CSM_102 Die ERCA weist jedem Bewegungssensor-Hauptschlüssel K_M eine eindeutige Versionsnummer zu, die auch für die zugrunde liegenden Schlüssel K_{M-VU} und K_{M-WC} und für den zugehörigen Identifikationsschlüssel K_{ID} gilt. Wenn die ERCA den MSCA die Schlüssel K_{M-VU} und K_{M-WC} übermittelt, informiert sie diese über die Versionsnummer.

Hinweis: Mithilfe der Versionsnummer können die verschiedenen Generationen dieser Schlüssel unterschieden werden; dies ist in Abschnitt 9.2.1.2 detailliert erläutert.

CSM_103 Die Zertifizierungsstelle des jeweiligen Mitgliedstaates leitet den Schlüssel K_{M-VU} samt Versionsnummer an die VU-Hersteller auf deren Anfrage weiter. Die VU-Hersteller setzen den Schlüssel K_{M-VU} samt Versionsnummer in allen hergestellten VU ein.

CSM_104 Die Zertifizierungsstelle des Mitgliedstaates stellt sicher, dass der Schlüssel K_{M-WC} samt Versionsnummer in jede Werkstattkarte eingefügt wird, die unter ihrer Verantwortung ausgegeben wird.

Hinweise:

— Siehe die Beschreibung des Datentyps `SensorInstallationSecData` in Anlage 2.

— Wie in Abschnitt 9.2.1.2 erläutert, müssen in eine einzelne Werkstattkarte mehrere Generationen von K_{M-WC} eingesetzt werden.

CSM_105 Über den in CSM_104 angegebenen AES-Schlüssel hinaus muss die MSCA sicherstellen, dass der unter Randnummer CSM_037 in Teil A dieser Anlage angegebene T-DES-Schlüssel Km_{WC} in jede Werkstattkarte eingesetzt wird, die unter ihrer Verantwortung ausgegeben wird.

Hinweise:

— Dadurch kann eine Werkstattkarte der 2. Generation zur Koppelung einer VU der 1. Generation verwendet werden.

— Eine Werkstattkarte der 2. Generation umfasst zwei verschiedene Anwendungen: Eine entspricht Teil B dieser Anlage, die andere Teil A. Die Letztgenannte enthält den T-DES-Schlüssel Km_{WC}.

CSM_106 Eine an der Ausgabe von Bewegungssensoren beteiligte MSCA leitet den Identifikationsschlüssel per XOR-Berechnung mit einem konstanten Vektor CV vom Bewegungssensor-Hauptschlüssel ab. Der Wert von CV lautet wie folgt:

— Für 128-Bit-Bewegungssensor-Hauptschlüssel: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— Für 192-Bit-Bewegungssensor-Hauptschlüssel: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— Für 256-Bit-Bewegungssensor-Hauptschlüssel: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Hinweis: Die konstanten Vektoren sind wie folgt zu berechnen:

Pi_10 = die ersten 10 Bytes des Dezimalteils der mathematischen Konstante π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = erste 16 Bytes von SHA-256(Pi_10)

CV_192-bits = erste 24 Bytes von SHA-384(Pi_10)

CV_256-bits = erste 32 Bytes von SHA-512(Pi_10)

CSM_107 Die Hersteller von Bewegungssensoren generieren für jeden Bewegungssensor einen zufälligen, eindeutigen Koppelungsschlüssel K_p und senden jeden einzelnen Koppelungsschlüssel an die Zertifizierungsstelle des Mitgliedstaates. Die MSCA verschlüsselt jeden Koppelungsschlüssel einzeln mit dem Bewegungssensor-Hauptschlüssel K_M und übermittelt den kodierten Schlüssel zurück an den Hersteller des Bewegungssensors. Für jeden kodierten Schlüssel informiert die MSCA den Hersteller von Bewegungssensoren über die Versionsnummer des zugehörigen K_M.

Hinweis: Wie in Abschnitt 9.2.1.2 erläutert, muss ein Hersteller von Bewegungssensoren für einen einzelnen Bewegungssensor unter Umständen mehrere eindeutige Koppelungsschlüssel generieren.

CSM_108 Die Hersteller von Bewegungssensoren generieren für jeden Bewegungssensor eine eindeutige Seriennummer und senden sämtliche Seriennummern an die Zertifizierungsstelle des Mitgliedstaates. Die MSCA verschlüsselt jede Seriennummer einzeln mit dem Identifikationsschlüssel K_{ID} und übermittelt die kodierte Seriennummer zurück an den Hersteller des Bewegungssensors. Für jede kodierte Seriennummer informiert die MSCA den Hersteller von Bewegungssensoren über die Versionsnummer des zugehörigen K_{ID}.

CSM_109 Bezüglich der Randnummern CSM_107 und CSM_108 muss die MSCA den AES-Algorithmus im Modus Cipher Block Chaining gemäß Referenzdokument ISO 10116, mit einem Verschachtelungsparameter *m* = 1 und einem Initialisierungsvektor SV = '00'{16}, d. h. sechzehn Bytes mit dem Binärwert 0, verwenden. Falls erforderlich, muss die MSCA die Auffüllmethode 2 gemäß Referenzdokument ISO 9797-1 verwenden.

CSM_110 Der Hersteller von Bewegungssensoren speichert den kodierten Koppelungsschlüssel und die kodierte Seriennummer im vorgesehenen Bewegungssensor, zusammen mit den entsprechenden Klartextwerten und der Versionsnummer der zur Verschlüsselung verwendeten K_M und K_{ID}.

Hinweis: Wie in Abschnitt 9.2.1.2 erläutert, muss ein Hersteller von Bewegungssensoren für einen einzelnen Bewegungssensor unter Umständen mehrere kodierte Koppelungsschlüssel und mehrere kodierte Seriennummern einfügen.

CSM_111 Über die in CSM_110 erläuterten AES-basierten kryptografischen Elemente hinaus kann der Hersteller von Bewegungssensoren in jedem Bewegungssensor auch die in Teil A dieser Anlage, Randnummer CSM_037, genannten T-DES-basierten kryptografischen Elemente speichern.

Hinweis: Dadurch kann ein Bewegungssensor der 2. Generation mit einer VU der 1. Generation gekoppelt werden.

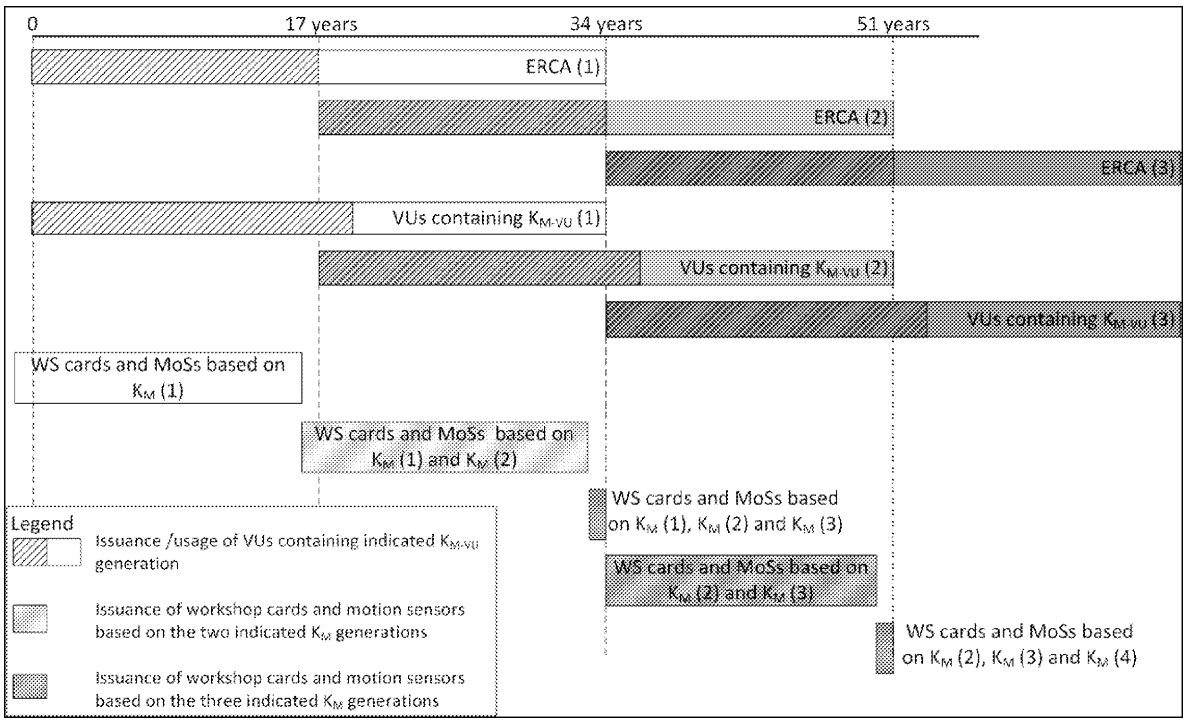
CSM_112 Die Länge des während der Koppelung mit einem Bewegungssensor von einer VU generierten Sitzungsschlüssels K_S muss derjenigen seines K_{M-VU} entsprechen (siehe CSM_50).

9.2.1.2 *Austausch des Bewegungssensor-Hauptschlüssels bei Geräten der zweiten Generation*

CSM_113 Sämtliche Bewegungssensor-Hauptschlüssel und alle zugehörigen Schlüssel (siehe Tabelle 3) sind einer bestimmten Generation des ERCA-Wurzelschlüsselpaars zugeordnet. Diese Schlüssel müssen deshalb alle 17 Jahre ersetzt werden. Die Gültigkeitsdauer jeder Generation von Bewegungssensor-Hauptschlüsseln beginnt ein Jahr, bevor das zugehörige ERCA-Wurzel-Schlüsselpaar gültig wird, und endet, wenn das zugehörige ERCA-Wurzel-Schlüsselpaar ausläuft. Dies ist in Abbildung 2 dargestellt.

Abbildung 2

Ausstellung und Verwendung verschiedener Generationen von Bewegungssensor-Hauptschlüsseln in Fahrzeugeinheiten, Bewegungssensoren und Werkstattkarten



CSM_114 Mindestens ein Jahr, bevor ein neues European Wurzel-Schlüsselpaar erstellt wird (siehe CSM_56), erstellt die ERCA K_M durch Generierung neuer K_{M-VU} und K_{M-WC} einen neuen Bewegungssensor-Hauptschlüssel. Die Länge des Bewegungssensor-Hauptschlüssels muss der vorgesehenen Stärke des neuen europäischen Wurzel-Schlüsselpaars gemäß CSM_50 entsprechen. Die ERCA teilt den MSCA auf Anfrage die neuen K_M, K_{M-VU} und K_{M-WC} samt Versionsnummer mit.

CSM_115 Die MSCA stellt sicher, dass alle gültigen Generationen von K_{M-WC} in jeder unter ihrer Verantwortung ausgegebenen Werkstattkarte samt ihren Versionsnummern gespeichert werden (siehe Abbildung 2).

Hinweis: Dies hat zur Folge, dass im letzten Jahr der Gültigkeitsdauer eines ERCA-Zertifikats Werkstattkarten mit drei verschiedenen Generationen von K_{M-WC} ausgegeben werden (siehe Abbildung 2).

CSM_116 Bezüglich des unter CSM_107 und CSM_108 oben genannten Verfahrens: Die MSCA kodiert jeden Koppelungsschlüssel K_P, den sie von einem Hersteller von Bewegungssensoren erhält, separat mit jeder gültigen Generation des Bewegungssensor-Hauptschlüssels K_M. Weiterhin kodiert die MSCA jede Seriennummer, die sie von einem Hersteller von Bewegungssensoren erhält, separat mit jeder gültigen Generation des Identifizierungsschlüssels K_{ID}. Der Hersteller von Bewegungssensoren speichert sämtliche Kodierungen des Koppelungsschlüssels sowie sämtliche Kodierungen der Seriennummern im vorgesehenen Bewegungssensor, zusammen mit den entsprechenden Klartextwerten und der Versionsnummer der zur Verschlüsselung verwendeten K_M und K_{ID}.

Hinweis: Dies hat zur Folge, dass im letzten Jahr der Gültigkeitsdauer eines ERCA-Zertifikats Bewegungssensoren mit kodierten Daten ausgegeben werden, die auf drei verschiedenen K_M-Generationen basieren (siehe Abbildung 2).

CSM_117 Bezüglich des unter CSM_107 oben genannten Verfahrens: Da die Länge des Koppelungsschlüssels K_P an der Länge von K_M auszurichten ist (siehe CSM_100), muss ein Hersteller von Bewegungssensoren für einen Bewegungssensor unter Umständen bis zu drei verschiedene Koppelungsschlüssel (unterschiedlicher Länge) für den Fall generieren, dass nachfolgende K_M-Generationen unterschiedliche Längen aufweisen. In einem solchen Fall sendet der Hersteller sämtliche Koppelungsschlüssel an die MSCA. Die MSCA stellt sicher, dass jeder Koppelungsschlüssel mit der richtigen Generation des Bewegungssensor-Hauptschlüssels kodiert ist, also derjenigen gleicher Länge.

Hinweis: Wenn der Hersteller von Bewegungssensoren entscheidet, einen T-DES-basierten Koppelungsschlüssel für einen Bewegungssensor der 2. Generation zu generieren (siehe CSM_111), muss der Hersteller die MSCA darauf hinweisen, dass der T-DES-basierte Bewegungssensor-Hauptschlüssel zur Dekodierung dieses Koppelungsschlüssels verwendet werden muss. Grund dafür ist, dass die Länge eines T-DES-Schlüssels mit derjenigen eines AES-Schlüssels identisch sein kann; die MSCA kann die Unterscheidung deshalb nicht alleine anhand der Schlüssellänge treffen.

CSM_118 Die VU-Hersteller dürfen in jede Fahrzeugeinheit nur eine K_{M-VU}-Generation samt Versionsnummer einsetzen. Diese K_{M-VU}-Generation ist an das ERCA-Zertifikat zu binden, auf dem die Zertifikate der VU basieren.

Anmerkungen:

— Eine Fahrzeugeinheit, die auf dem ERCA-Zertifikat der Generation *X* basiert, darf nur den K_{M-VU} der Generation *X* enthalten, selbst wenn dieser erst nach Beginn der Gültigkeitsdauer des ERCA-Zertifikats der Generation *X+1* ausgestellt wurde. Dies ist in Abbildung 2 dargestellt.

— Eine VU der Generation *X* kann nicht mit einem Bewegungssensor der Generation *X-1* gekoppelt werden.

— Da Werkstattkarten eine Gültigkeitsdauer von einem Jahr aufweisen, bewirken CSM_113 — CSM_118, dass alle Werkstattkarten dann, wenn der neue K_{M-VU} ausgegeben werden wird, den neuen K_{M-WC} enthalten werden. Somit wird eine solche VU immer in der Lage sein, den neuen K_M zu berechnen. Zudem werden dann die meisten neuen Bewegungssensoren ebenfalls kodierte Daten enthalten, die auf dem neuen K_M beruhen.

9.2.2 *Schlüssel zur Sicherung der DSRC-Kommunikation*

9.2.2.1 *Allgemein*

CSM_119 Die Authentizität und Vertraulichkeit der von einer Fahrzeugeinheit per DSRC-Fernkommunikationskanal an eine Kontrollbehörde übermittelten Daten kann mithilfe einer Reihe VU-spezifischer AES-Schlüssel sichergestellt werden, die von einem einzigen DSRC-Hauptschlüssel, KM_{DSRC}, abgeleitet sind.

CSM_120 Beim DSRC-Hauptschlüssel KM_{DSRC} muss es sich um einen AES-Schlüssel handeln, der von der ERCA sicher generiert, gespeichert und verteilt wird. Die Schlüssellänge kann 128, 192 oder 256 Bits betragen und orientiert sich an der Länge des europäischen Wurzel-Schlüsselpaars (siehe CSM_50).

CSM_121 Die ERCA übermittelt auf Anfrage den Zertifizierungsstellen der Mitgliedstaaten den DSRC-Hauptschlüssel in sicherer Form, damit diese Stellen VU-spezifische DSRC-Schlüssel ableiten und somit sicherstellen können, dass der DSRC-Hauptschlüssel in alle unter ihrer Verantwortung ausgegebenen Kontrollkarten und Werkstattkarten eingesetzt ist.

CSM_122 Die ERCA weist jedem DSRC-Hauptschlüssel eine eindeutige Versionsnummer zu. Wenn die ERCA den MSCA den DSRC-Hauptschlüssel übermittelt, informiert sie diese über die Versionsnummer.

Hinweis: Mithilfe der Versionsnummer können die verschiedenen Generationen des DSRC-Hauptschlüssels unterschieden werden; dies ist in Abschnitt 9.2.2.2 detailliert erläutert.

CSM_123 Für jede Fahrzeugeinheit erstellt der Hersteller der Fahrzeugeinheit eine eindeutige VU-Seriennummer und sendet diese an die Zertifizierungsstelle des Mitgliedstaates, um eine Gruppe von zwei VU-spezifischen DSRC-Schlüsseln zu beantragen. Die VU-Seriennummer verfügt über den Datentyp `VuSerialNumber`; zur Kodierung sind die Distinguished Encoding Rules (DER) gemäß Referenzdokument ISO 8825-1 zu verwenden.

CSM_124 Nach Erhalt des Antrags auf VU-spezifische DSRC-Schlüssel leitet die MSCA für die Fahrzeugeinheit zwei AES-Schlüssel namens K_VU_{DSRC}_ENC und K_VU_{DSRC}_MAC ab. Diese VU-spezifischen Schlüssel sind genauso lang wie der DSRC-Hauptschlüssel. Die MSCA verwendet die in Referenzdokument RFC 5869 definierte Schlüsselableitungsfunktion. Die zum Instanzieren der HMAC-Hashfunktion erforderliche Hashfunktion ist an der Länge des DSRC-Hauptschlüssels auszurichten (siehe CSM_50). Die in RFC 5869 dargelegte Schlüsselableitungsfunktion ist wie folgt zu verwenden:

Schritt 1 (Extrahieren):

— *PRK* = HMAC-Hash (*salt, IKM*) wobei *salt* einen leeren String '' darstellt und *IKM* KM_{DSRC} entspricht

Schritt 2 (Expandieren):

— *OKM* = *T(1)*, wobei

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01') mit

— *T(0)* = leerer String ('')

— *info* = VU-Seriennummer gemäß CSM_123

— K_VU_{DSRC}_ENC = erste *L*-Oktette von *OKM* und

K_VU_{DSRC}_MAC = letzte *L*-Oktette von *OKM*;

dabei ist *L* die erforderliche Länge von K_VU_{DSRC}_ENC und K_VU_{DSRC}_MAC in Oktetten.

CSM_125 Die MSCA verteilt K_VU_{DSRC}_ENC und K_VU_{DSRC}_MAC in sicherer Form an die VU-Hersteller, damit diese sie in die vorgesehene Fahrzeugeinheit einsetzen.

CSM_126 Bei der Ausgabe müssen im geschützten Speicher einer Fahrzeugeinheit K_VU_{DSRC}_ENC und K_VU_{DSRC}_MAC abgelegt sein, um die Integrität, Authentizität und Vertraulichkeit der über den Fernkommunikationskanal gesendeten Daten gewährleisten zu können. Außerdem muss in einer Fahrzeugeinheit die Versionsnummer des zum Ableitung dieser VU-spezifischen Schlüssel verwendeten DSRC-Hauptschlüssels gespeichert sein.

CSM_127 Bei der Ausgabe muss im geschützten Speicher von Kontrollkarten und Werkstattkarten KM_{DSRC} abgelegt sein, um die Integrität und Authentizität der von einer VU über den Fernkommunikationskanal gesendeten Daten zu überprüfen und diese Daten zu entschlüsseln. Auch in den Kontrollkarten und Werkstattkarten muss die Versionsnummer des DSRC-Hauptschlüssels abgelegt sein.

Hinweis: Wie in Abschnitt 9.2.2.2 erläutert, müssen unter Umständen in eine einzelne Werkstatt- oder Kontrollkarte mehrere Generationen von K_{MDSRC} eingesetzt werden.

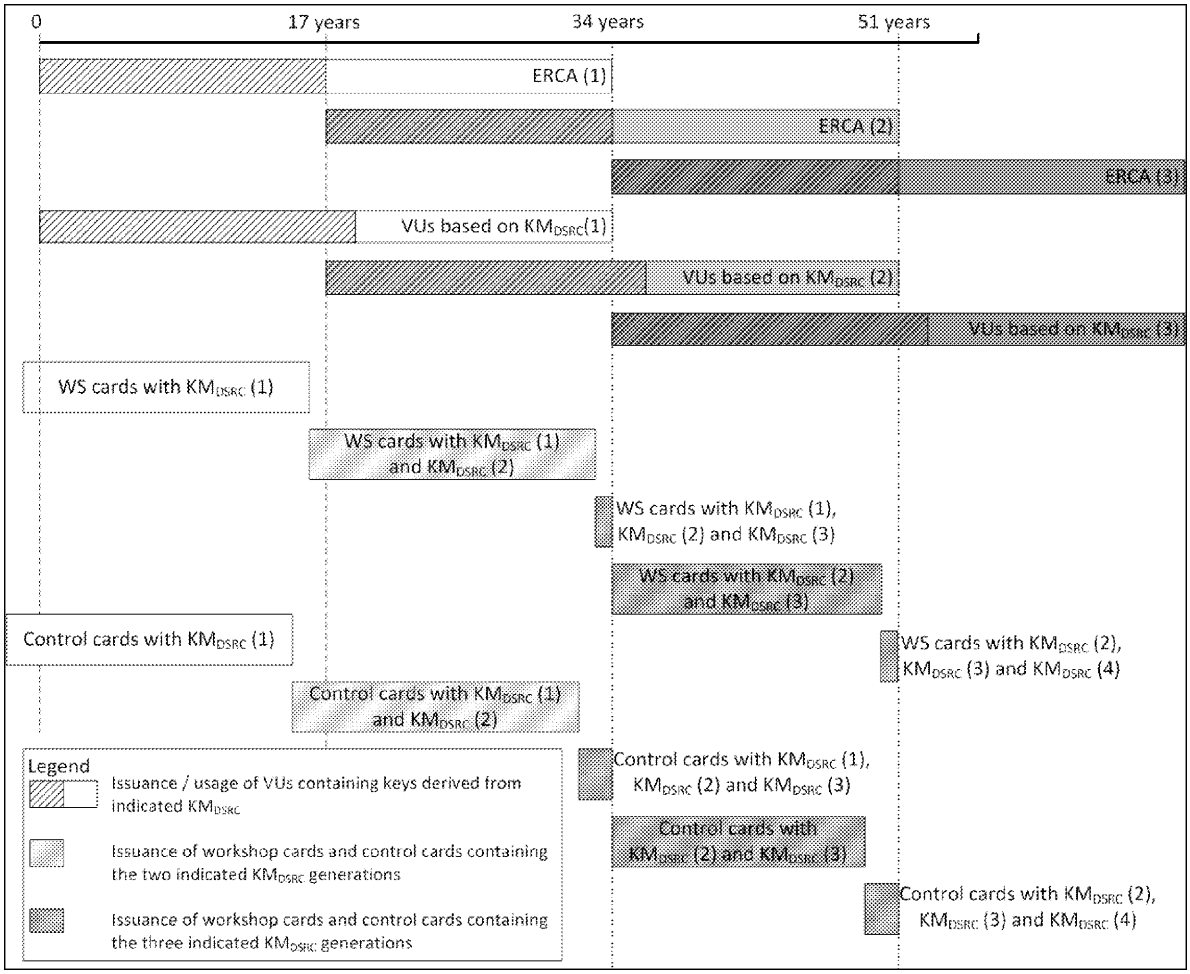
CSM_128 Die MSCA muss Aufzeichnungen aller von ihr erzeugten VU-spezifischen DSRC-Schlüssel samt Versionsnummer und Kennung der VU, für die jede Schlüsselreihe vorgesehen ist, führen.

9.2.2.2 *Austausch des DSRC-Hauptschlüssels*

CSM_129 Sämtliche DSRC-Hauptschlüssel sind einer bestimmten Generation des ERCA-Wurzelschlüsselpaars zugeordnet. Die ERCA tauscht den DSRC-Hauptschlüssel deshalb alle 17 Jahre aus. Die Gültigkeitsdauer jeder Generation von DSRC-Hauptschlüsseln beginnt zwei Jahre, bevor das zugehörige ERCA-Wurzel-Schlüsselpaar gültig wird, und endet, wenn das zugehörige ERCA-Wurzel-Schlüsselpaar ausläuft. Dies ist in Abbildung 3 dargestellt.

Abbildung 3

Ausstellung und Verwendung verschiedener Generationen von DSRC-Hauptschlüsseln in Fahrzeugeinheiten, Werkstatt- und Kontrollkarten



CSM_130 Spätestens zwei Jahre vor dem Erstellen eines neuen europäischen Wurzel-Schlüsselpaars (siehe CSM_56) erstellt die ERCA einen neuen DSRC-Hauptschlüssel. Die Länge des DSRC-Hauptschlüssels muss der vorgesehenen Stärke des neuen europäischen Wurzel-Schlüsselpaars gemäß CSM_50 entsprechen. Die ERCA teilt den MSCA auf Anfrage den neuen DSRC-Hauptschlüssel samt Versionsnummer mit.

CSM_131 Die MSCA stellt sicher, dass alle gültigen Generationen von K_{MDSRC} in jeder unter ihrer Verantwortung ausgegebenen Kontrollkarte samt Versionsnummern gespeichert werden (siehe Abbildung 3).

Hinweis: Dies hat zur Folge, dass in den letzten beiden Jahren der Gültigkeitsdauer eines ERCA-Zertifikats Kontrollkarten mit drei verschiedenen Generationen von K_{MDSRC} ausgegeben werden (siehe Abbildung 3).

CSM_132 Die MSCA stellt sicher, dass alle Generationen von K_{MDSRC}, die seit mindestens einem Jahr und auch noch weiter gültig sind, in jeder unter ihrer Verantwortung ausgegebenen Werkstattkarte samt ihren Versionsnummern gespeichert werden (siehe Abbildung 3).

Hinweis: Dies hat zur Folge, dass im letzten Jahr der Gültigkeitsdauer eines ERCA-Zertifikats Werkstattkarten mit drei verschiedenen Generationen von K_{MDSRC} ausgegeben werden (siehe Abbildung 3).

CSM_133 Die VU-Hersteller dürfen in jede Fahrzeugeinheit nur eine Gruppe VU-spezifischer DSRC-Schlüssel samt Versionsnummer einsetzen. Diese Schlüsselgruppe ist von der KM_{DSRC}-Generation abzuleiten, die an das ERCA-Zertifikat gebunden ist, auf dem die Zertifikate der VU basieren.

Hinweise:

— Dies bedeutet, dass eine Fahrzeugeinheit, die auf dem ERCA-Zertifikat der Generation *X* basiert, nur die K_VU_ENC und K_VU_{DSRC}_MAC der Generation enthalten darf, selbst wenn die VU erst nach Beginn der Gültigkeitsdauer des ERCA-Zertifikats der Generation *X+1* ausgestellt wurde. Dies ist in Abbildung 3 dargestellt.

— Da Werkstattkarten eine Gültigkeitsdauer von einem Jahr und Kontrollkarten eine Gültigkeitsdauer von zwei Jahren aufweisen, bewirken CSM_131 — CSM_133, dass alle Werkstatt- und Kontrollkarten dann, wenn die erste VU mit VU-spezifischen Schlüsseln auf Grundlage dieses Hauptschlüssels ausgegeben werden wird, den neuen DSRC-Hauptschlüssel enthalten werden.

9.3. **Zertifikate**

9.3.1 *Allgemein*

CSM_134 Bei allen Zertifikaten im europäischen intelligenten Fahrtenschreibersystem muss es sich um selbstbeschreibende, kartenverifizierbare (CV) Zertifikate gemäß ISO 7816-4 und ISO 7816-8 handeln.

CSM_135 Zur Kodierung der ASN.1-Datenstrukturen und (anwendungsspezifischen) Datenobjekte innerhalb der Zertifikate sind die Distinguished Encoding Rules (DER) gemäß ISO 8825-1 zu verwenden.

Hinweis: Diese Kodierung bewirkt folgende TLV-Struktur (Tag-Length-Value, Tag-Längen-Wert):

Tag: Der Tag ist in ein oder zwei Oktette verschlüsselt und gibt den Inhalt an.

Länge: Die Länge ist als unsignierte Ganzzahl in ein, zwei oder drei Oktette verschlüsselt, was zu einer Länge von maximal 65 535 Oktetten führt. Es ist die Mindestzahl an Oktetten zu verwenden.

Wert: Der Wert ist in null oder mehr Oktette verschlüsselt.

9.3.2 *Zertifikatsinhalt*

CSM_136 Alle Zertifikate weisen die Struktur des Zertifikatprofils in Tabelle 4 auf.

Tabelle 4

Zertifikatprofil Version 1

Feld	Feldkennung	Tag	Länge (Bytes)	ASN.1-Datentyp (siehe Anlage 1)
ECC-Zertifikat	C	'7F 21'	var	
ECC Certificate Body	B	'7F 4E'	var	

Feld	Feldkennung	Tag	Länge (Bytes)	ASN.1-Datentyp (siehe Anlage 1)
Certificate Profile Identifier	CPI	'5F 29'	'01'	INTEGER(0..255)
Certificate Authority Reference	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorisation	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Public Key	PK	'7F 49'	var	
Domain Parameters	DP	'06'	var	OBJECT IDENTIFIER
Public Point	PP	'86'	var	OCTET STRING
Certificate Holder Reference	CHR	'5F 20'	'08'	KeyIdentifier
Certificate Effective Date	CEfD	'5F 25'	'04'	TimeReal
Certificate Expiration Date	CExD	'5F 24'	'04'	TimeReal
ECC Certificate Signature	S	'5F 37'	var	OCTET STRING

Hinweis: Mit der Feldkennung werden in späteren Abschnitten dieser Anlage einzelne Felder eines Zertifikats angegeben — X.CAR ist beispielsweise die im Zertifikat von Benutzer X angegebene Certificate Authority Reference.

9.3.2.1 Certificate Profile Identifier

CSM_137 Die Zertifikate müssen mit einem Certificate Profile Identifier das verwendete Zertifikatprofil angeben. Version 1 (siehe Tabelle 4) ist durch einen Wert von '00' anzugeben.

9.3.2.2 Certificate Authority Reference

CSM_138 Mit der Certificate Authority Reference wird der öffentliche Schlüssel angegeben, mit dem die Zertifikatsignatur verifiziert wird. Die Certificate Authority Reference muss deshalb mit der Certificate Holder Reference im Zertifikat der entsprechenden Zertifizierungsstelle übereinstimmen.

CSM_139 Ein ERCA-Wurzelzertifikat muss selbstsigniert sein, d. h. Certificate Authority Reference und Certificate Holder Reference im Zertifikat müssen übereinstimmen.

CSM_140 Bei einem ERCA-Linkzertifikat muss die Certificate Holder Reference der CHR des neuen ERCA-Wurzelzertifikats entsprechen. Die Certificate Holder Reference eines Linkzertifikats muss der CHR des vorherigen ERCA-Wurzelzertifikats entsprechen.

9.3.2.3 Certificate Holder Authorisation

CSM_141 Mit „Certificate Holder Authorisation" wird die Zertifikatart angegeben. Sie besteht aus den sechs höchstwertigen Bytes der Fahrtenschreiberanwendungs-ID, verkettet mit der Geräteart, für die das Zertifikat vorgesehen ist.

9.3.2.4 Public Key

Public Key verschachtelt zwei Datenelemente: den mit dem öffentlichen Schlüssel im Zertifikat zu verwendenden standardisierten Domänenparameter und den Wert des öffentlichen Punktes.

CSM_142 Das Datenelement Domain Parameters muss eine der in Tabelle 1 angegebenen Objektkennungen enthalten, um auf eine Gruppe standardisierter Domänenparameter zu verweisen.

CSM_143 Das Datenelement Public Point enthält den öffentlichen Punkt. Öffentliche Punkte auf elliptischen Kurven sind gemäß TR-03111 in Oktettstrings umzuwandeln. Dabei ist das unkomprimierte Verschlüsselungsformat zu verwenden. Beim Wiederherstellen eines Punktes auf einer elliptischen Kurve aus seinem verschlüsselten Format sind stets die in TR-03111 genannten Validierungen durchzuführen.

9.3.2.5 Certificate Holder Reference (Referenz des Zertifikatinhabers)

CSM_144 Certificate Holder Reference ist eine Kennung für den im Zertifikat angegebenen öffentlichen Schlüssel. Mit dieser Kennung wird in anderen Zertifikaten auf diesen öffentlichen Schlüssel verwiesen.

CSM_145 Bei Kartenzertifikaten und Zertifikaten externer GNSS-Ausrüstung muss Certificate Holder Reference den in Anlage 1 angegebenen Datentyp `ExtendedSerialNumber` aufweisen.

CSM_146 Bei Fahrzeugeinheiten ist dem Hersteller bei der Beantragung eines Zertifikats die herstellerspezifische Seriennummer der VU, für die das Zertifikat und der zugehörige private Schlüssel vorgesehen sind, unter Umständen nicht bekannt. Wenn sie ihm bekannt ist, muss Certificate Holder Reference den in Anlage 1 angegebenen Datentyp `ExtendedSerialNumber` aufweisen. Wenn sie ihm nicht bekannt ist, muss Certificate Holder Reference den in Anlage 1 angegebenen Datentyp `CertificateRequestID` aufweisen.

CSM_147 Bei ERCA- und MSCA-Zertifikaten muss Certificate Holder Reference den in Anlage 1 angegebenen Datentyp CertificationAuthorityKID `CertificationAuthorityKID` aufweisen.

9.3.2.6 Certificate Effective Date

CSM_148 Certificate Effective Date gibt Anfangsdatum und -uhrzeit der Gültigkeitsdauer des Zertifikats an. Certificate Effective Date entspricht dem Datum, zu dem das Zertifikat generiert wurde.

9.3.2.7 Certificate Expiration Date

CSM_149 Certificate Expiration Date gibt Enddatum und -uhrzeit der Gültigkeitsdauer des Zertifikats an.

9.3.2.8 Certificate Signature

CSM_150 Die Signatur des Zertifikats wird anhand des kodierten Zertifikatkörpers erstellt, einschließlich Tag und Länge des Zertifikatkörpers. Als Signaturalgorithmus wird ECDSA gemäß DSS verwendet; dabei ist der an die Schlüsselgröße der signierenden Stelle gebundene Hash-Algorithmus zu verwenden (siehe CSM_50). Das Signaturformat ist Klartext, wie in TR-03111 angegeben.

9.3.3 *Beantragen von Zertifikaten*

CSM_151 Beim Beantragen eines Zertifikats muss der Antragsteller der Zertifizierungsstelle die folgenden Daten übermitteln:

— den Certificate Profile Identifier des beantragten Zertifikats

— die Certificate Authority Reference, die zum Signieren des Zertifikats voraussichtlich verwendet werden soll

— den zu signierenden Public Key

CSM_152 Über die in CSM_151 genannten Angaben hinaus muss die MSCA der ERCA in einem Zertifikatsantrag die folgenden Daten übermitteln, damit Letztgenannte die Certificate Holder Reference des neuen MSCA-Zertifikats erstellen kann:

— den numerischen Landescode der Zertifizierungsstelle (der in Anlage 1 definierte Datentyp `NationNumeric`)

— den alphanumerischen Landescode der Zertifizierungsstelle (der in Anlage 1 definierte Datentyp `NationAlpha`)

— die 1-Byte-Seriennummer zur Unterscheidung der verschiedenen Schlüssel der Zertifizierungsstelle für den Fall des Wechsels von Schlüsseln

— das 2-Byte-Feld mit weiteren Informationen zur Zertifizierungsstelle

CSM_153 Über die in CSM_151 genannten Angaben hinaus muss der Gerätehersteller der MSCA in einem Zertifikatsantrag die folgenden Daten übermitteln, damit Letztgenannte die Certificate Holder Reference des neuen Gerätezertifikats erstellen kann:

— eine herstellerspezifische Kennung der Geräteart

— falls bekannt (siehe CSM_154), die Seriennummer des Geräts in Bezug auf den Hersteller, den Gerätetyp und den Herstellungsmonat Andernfalls eine eindeutige Kennung für den Zertifikatsantrag.

— Monat und Jahr der Geräteherstellung oder des Zertifikatsantrags.

Der Hersteller muss sicherstellen, dass diese Angaben richtig sind und dass das von der MSCA übermittelte Zertifikat in die vorgesehene Ausrüstung eingesetzt wird.

CSM_154 Bei Fahrzeugeinheiten ist dem Hersteller bei der Beantragung eines Zertifikats die herstellerspezifische Seriennummer der VU, für die das Zertifikat und der zugehörige private Schlüssel vorgesehen sind, unter Umständen nicht bekannt. Wenn bekannt, übermittelt der VU-Hersteller die Seriennummer der MSCA. Wenn nicht bekannt, kennzeichnet der Hersteller jeden Zertifikatsantrag eindeutig und übermittelt diese Seriennummer der MSCA. Das ausgestellte Zertifikat enthält dann die Seriennummer des Zertifikatsantrags. Sobald das Zertifikat in eine bestimmte VU eingesetzt ist, übermittelt der Hersteller der MSCA den Zusammenhang zwischen der Seriennummer des Zertifikatsantrags und der VU-Kennung.

10. GEGENSEITIGE AUTHENTISIERUNG VU-KARTE UND SECURE MESSAGING

10.1. **Allgemein**

CSM_155 Generell wird die sichere Kommunikation zwischen Fahrzeugeinheit und Fahrtenschreiberkarte durch die folgenden Schritte gewährleistet:

— Im ersten Schritt zeigt jede Partei der jeweils anderen, dass sie über ein gültiges Public-Key-Zertifikat verfügt, signiert durch die Zertifizierungsstelle des Mitgliedstaats. Das Public-Key-Zertifikat der MSCA wiederum muss durch die Europäische Wurzel-Zertifizierungsstelle signiert sein. Dieser Schritt, die Verifizierung der Zertifikatkette, wird in Abschnitt 10.2 detailliert erläutert.

— Im zweiten Schritt weist die Fahrzeugeinheit der Karte nach, dass sie über den privaten Schlüssel verfügt, der dem öffentlichen Schlüssel im vorgelegten Zertifikat entspricht. Dazu signiert sie eine von der Karte übermittelte Zufallszahl. Die Karte verifiziert die Signatur anhand der Zufallszahl. Wenn diese Verifizierung erfolgreich verläuft, ist die VU authentisiert. Dieser Schritt, die VU-Authentisierung, wird in Abschnitt 10.3 detailliert erläutert.

— Im dritten Schritt berechnen beide Parteien unabhängig voneinander mithilfe eines asymmetrischen Algorithmus zur Schlüsselvereinbarung zwei AES-Sitzungsschlüssel. Mit einem dieser Sitzungsschlüssel erstellt die Karte anhand einiger von der Karte gesendeter Daten einen Code für die Nachrichtenauthentisierung (MAC). Die VU verifiziert den MAC. Wenn diese Verifizierung erfolgreich verläuft, ist die Karte authentisiert. Dieser Schritt, die Kartenauthentisierung, wird in Abschnitt 10.4 detailliert erläutert.

— Im vierten Schritt gewährleisten VU und Karte mithilfe der vereinbarten Sitzungsschlüssel die Vertraulichkeit, Integrität und Authentizität aller ausgetauschten Nachrichten. Dieser Schritt namens Secure Messaging wird in Abschnitt 10.5 detailliert erläutert.

CSM_156 Der in CSM_155 beschriebene Mechanismus wird von der Fahrzeugeinheit ausgelöst, sobald in einen ihrer Steckplätze eine Karte eingesetzt wird.

10.2. **Gegenseitige Verifizierung der Zertifikatkette**

10.2.1 *Verifizierung der Kartenzertifikatkette durch die VU*

CSM_157 Die Fahrzeugeinheiten verifizieren mithilfe des in Abbildung 4 dargestellten Protokolls die Zertifikatkette einer Fahrtenschreiberkarte.

Hinweise zu Abbildung 4:

— Bei den in der Abbildung erwähnten Kartenzertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur gegenseitigen Authentisierung. In Abschnitt 9.1.5 werden sie als Card_MA bezeichnet.

— Bei den in der Abbildung erwähnten Card.CA-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur Signierung der Kartenzertifikate, die in der CAR des Card-Zertifikats angegeben sind. In Abschnitt 9.1.3 werden sie als MSCA_Card bezeichnet.

— Bei dem in der Abbildung erwähnten Card.CA.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des Card.CA-Zertifikats angegeben ist.

— Das in der Abbildung erwähnte Card.Link-Zertifikat ist das Linkzertifikat der Karte, sofern vorhanden. Wie in Abschnitt 9.1.2 angegeben, handelt es sich hierbei um ein Linkzertifikat für ein neues europäisches Wurzel-Schlüsselpaar, das durch die ERCA erstellt und mithilfe des zuvor erwähnten europäischen privaten Schlüssels signiert wird.

— Bei dem Card.Link.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des Card.Link-Zertifikats angegeben ist.

CSM_158 Wie in Abbildung 4 dargestellt, beginnt beim Einsetzen der Karte die Verifizierung ihrer Zertifikatkette. Die Fahrzeugeinheit liest aus der EF-ECC die Kennung des Karteninhabers (`cardExtendedSerialNumber`) aus. Die VU muss überprüfen, ob sie die Karte kennt — ob sie also in der Vergangenheit die Zertifikatkette der Karte erfolgreich überprüft und zur späteren Referenz abgelegt hat. Wenn dies der Fall und das Zertifikat der Karte weiterhin gültig ist, wird nun die Zertifikatkette der VU verifiziert. Andernfalls muss die VU das MSCA_Card-Zertifikat zur Verifizierung des Kartenzertifikats, das Card.CA.EUR-Zertifikat zur Verifizierung des MSCA_Card-Zertifikats und eventuell das Linkzertifikat nacheinander aus der Karte auslesen, bis sie auf ein bekanntes Zertifikat stößt. Wenn sie ein solches Zertifikat findet, verifiziert die VU mit diesem die zugrunde liegenden Kartenzertifikate, die sie der Karte entnommen hat. Wenn diese Überprüfung erfolgreich verläuft, wird nun die Zertifikatkette der VU verifiziert. Andernfalls ignoriert die VU die Karte.

Hinweis: Der VU kann das Card.CA.EUR-Zertifikat auf drei Arten bekannt sein:

— es handelt sich um das gleiche Zertifikat wie das EUR-Zertifikat der VU selbst;

— das Card.EUR-Zertifikat ist ein Vorgänger des EUR-Zertifikats der VU und die VU enthielt dieses Zertifikat bereits ab Ausgabe (siehe CSM_81);

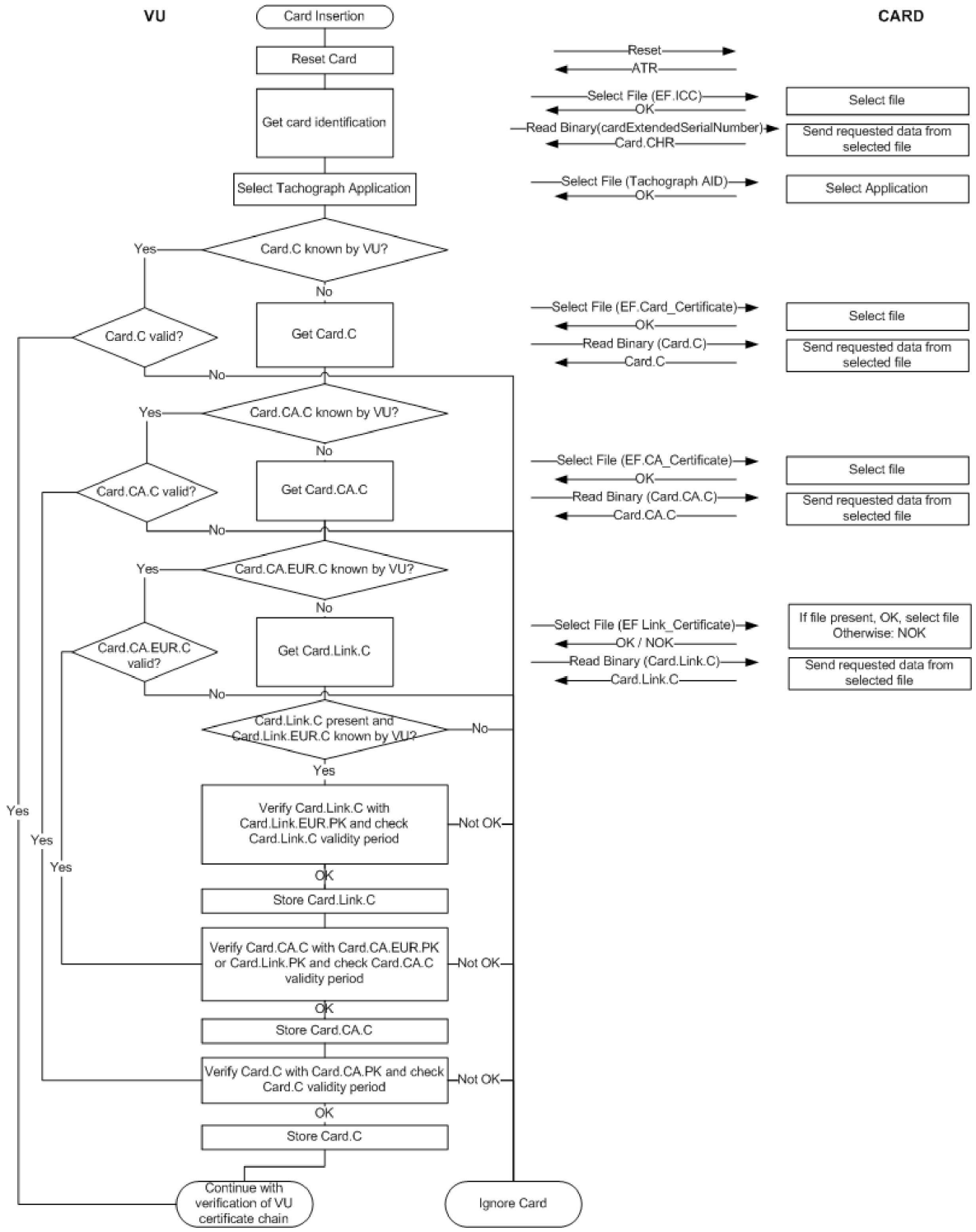
— das Card.CA.EUR-Zertifikat ist ein Nachfolger des EUR-Zertifikat der VU und die VU hat in der Vergangenheit von einer anderen Fahrtenschreiberkarte ein Linkzertifikat erhalten, verifiziert und zur zukünftigen Referenz abgespeichert.

CSM_159 Wie in Abbildung 4 angegeben, kann die VU, sobald sie die Authentizität und Gültigkeit eines zuvor unbekannten Zertifikats überprüft hat, dieses Zertifikat zur zukünftigen Referenz abspeichern. Sie braucht dann die Authentizität dieses Zertifikats nicht ein weiteres Mal zu prüfen, wenn es ihr erneut vorgelegt wird. Die VU braucht nicht das gesamte Zertifikat zu speichern, sondern lediglich den Inhalt des Zertifikatkörpers (siehe Abschnitt 9.3.2).

CSM_160 Die VU überprüft die temporäre Gültigkeit aller Zertifikate, die sie aus der Karte ausliest oder gespeichert hat, und lehnt abgelaufene Zertifikate ab. Die VU überprüft die temporäre Gültigkeit eines von einer Karte vorgelegten Zertifikats mithilfe ihrer Systemuhr.

Abbildung 4

Protokoll zur Verifizierung der Kartenzertifikatkette durch die VU

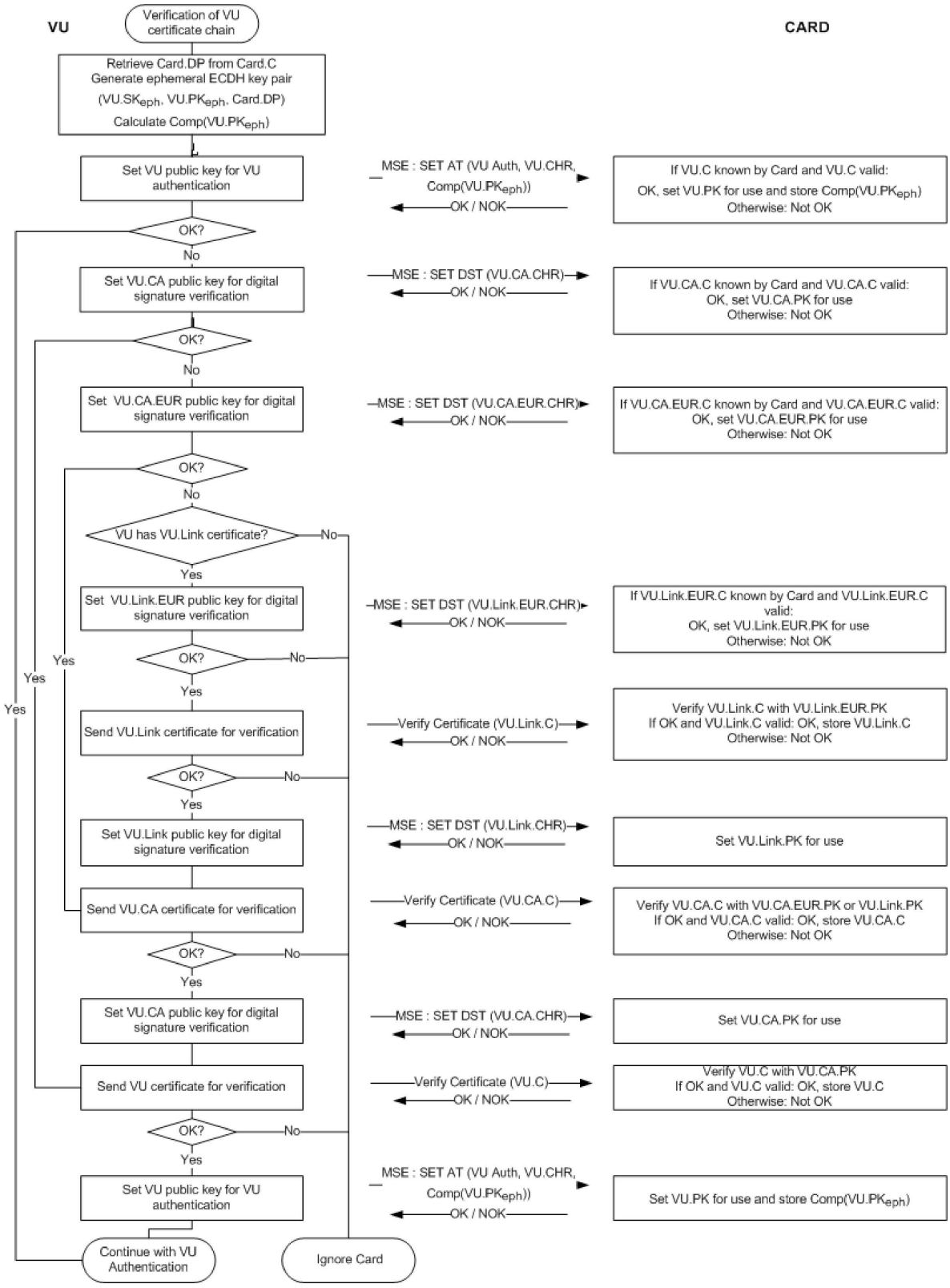


10.2.2 *Verifizierung der VU-Zertifikatkette durch die Karte*

CSM_161 Die Fahrtenschreiberkarten verifizieren mithilfe des in Abbildung 5 dargestellten Protokolls die Zertifikatkette einer VU.

Abbildung 5

Protokoll zur Verifizierung der VU-Zertifikatkette durch Card



Hinweise zu Abbildung 5:

— Bei den in der Abbildung erwähnten VU-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur gegenseitigen Authentisierung. In Abschnitt 9.1.4 werden sie als VU_MA bezeichnet.

— Bei den in der Abbildung erwähnten VU.CA-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur Signierung der Zertifikate von VU und externer GNSS-Ausrüstung. In Abschnitt 9.1.3 werden sie als MSCA_VU-EGF bezeichnet.

— Bei dem in der Abbildung erwähnten VU.CA.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des VU.CA-Zertifikats angegeben ist.

— Das in der Abbildung erwähnte VU.Link-Zertifikat ist das Linkzertifikat der VU, sofern vorhanden. Wie in Abschnitt 9.1.2 angegeben, handelt es sich hierbei um ein Linkzertifikat für ein neues europäisches Wurzel-Schlüsselpaar, das durch die ERCA erstellt und mithilfe des zuvor erwähnten europäischen privaten Schlüssels signiert wird.

— Bei dem VU.Link.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des VU.Link-Zertifikats angegeben ist.

CSM_162 Wie in Abbildung 5 dargestellt, versucht die Fahrzeugeinheit bei der Verifizierung der Zertifikatkette der Fahrzeugeinheit zunächst, ihren eigenen öffentlichen Schlüssel zur Verwendung in der Fahrtenschreiberkarte anzugeben. Wenn dies erfolgreich verläuft, bedeutet dies, dass die Karte zu einem früheren Zeitpunkt die Zertifikatkette der VU erfolgreich verifiziert und das VU-Zertifikat zur späteren Referenz abgelegt hat. In einem solchen Fall wird das VU-Zertifikat verwendet, und es schließt sich die VU-Authentisierung an. Wenn der Karte das VU-Zertifikat nicht bekannt ist, präsentiert die VU nacheinander das VU.CA-Zertifikat zur Verifizierung ihres VU-Zertifikats, das VU.CA.EUR-Zertifikat zur Verifizierung ihres VU.CA-Zertifikats und eventuell das Linkzertifikat, um festzustellen, ob die Karte eines dieser Zertifikate kennt oder verifizieren kann. Wenn sie ein solches Zertifikat findet, verifiziert die Karte mit diesem die ihr präsentierten zugrunde liegenden VU-Zertifikate. Im Erfolgsfall legt die VU schließlich ihren öffentlichen Schlüssel zur Verwendung in der Fahrtenschreiberkarte fest. Andernfalls ignoriert die VU die Karte.

Hinweis: Der VU kann das VU.CA.EUR-Zertifikat auf drei Arten bekannt sein:

— es handelt sich um das gleiche Zertifikat wie das EUR-Zertifikat der Karte selbst;

— das VU.CA.EUR-Zertifikat ist ein Vorgänger des EUR-Zertifikats der Karte und die Karte enthielt dieses Zertifikat bereits ab Ausgabe (siehe CSM_91);

— das VU.CA.EUR-Zertifikat ist ein Nachfolger des EUR-Zertifikat der Karte und die Karte hat in der Vergangenheit von einer anderen Fahrzeugeinheit ein Linkzertifikat erhalten, verifiziert und zur zukünftigen Referenz abgespeichert.

CSM_163 Die VU legt mithilfe des Befehls MSE: Set AT ihren öffentlichen Schlüssel zur Verwendung in der Fahrtenschreiberkarte fest. Wie in Anlage 2 erläutert, gibt dieser Befehl das kryptografische Verfahren an, das zusammen mit dem festgelegten Schlüssel verwendet wird. Hierbei handelt es sich um eine VU-Authentisierung unter Verwendung des ECDSA-Algorithmus in Kombination mit dem Hash-Algorithmus, der an die Schlüsselgröße des VU_MA-Schlüsselpaars der VU gebunden ist (siehe CSM_50).

CSM_164 Der Befehl MSE: Set AT beinhaltet zudem die Angabe des flüchtigen Schlüsselpaars, das die VU während der Vereinbarung des Sitzungsschlüssels verwendet (siehe Abschnitt 10.4). Vor dem Senden des Befehls MSE: Set AT generiert die VU deshalb ein flüchtiges ECC-Schlüsselpaar. Zur Generierung des flüchtigen Schlüsselpaars verwendet die VU die im Kartenzertifikat angegebenen standardisierten Domänenparameter. Das flüchtige Schlüsselpaar wird dargestellt als ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Die VU wählt die x-Koordinate des flüchtigen öffentlichen Punkts des ECDH-Verfahrens als Schlüsselkennung; dies ist eine komprimierte Darstellung des öffentlichen Schlüssels und wird in der Form Comp($VU.PK_{eph}$) dargestellt.

CSM_165 Wenn der Befehl MSE: Set AT erfolgreich ausgeführt wird, legt die Karte den angegebenen VU.PK zur weiteren Verwendung im Rahmen der VU-Authentisierung fest und speichert Comp($VU.PK_{eph}$) temporär. Wenn vor der Vereinbarung des Sitzungsschlüssels zwei oder mehr erfolgreiche Befehle MSE: Set AT gesendet werden, speichert die Karte lediglich den letzten erhaltenen Comp($VU.PK_{eph}$).

CSM_166 Die Karte überprüft die temporäre Gültigkeit aller von der VU präsentierten oder von der VU als Referenz verwendeten Zertifikate, die im Speicher der Karte abgelegt sind, und lehnt abgelaufene Zertifikate ab.

CSM_167 Um die temporäre Gültigkeit eines von der VU präsentierten Zertifikats zu überprüfen, speichert jede Fahrtenschreiberkarte intern gewisse Daten, die den aktuellen Zeitpunkt darstellen. Diese Daten dürfen von einer VU nicht direkt aktualisiert werden können. Im Moment der Ausgabe wird die aktuelle Uhrzeit einer Karte auf das Effective Date des Card_MA-Zertifikats der Karte gesetzt. Eine Karte darf dann ihre aktuelle Uhrzeit aktualisieren, wenn das Effective Date eines authentischen, von einer VU präsentierten Zertifikats einer „gültigen Zeitquelle" jünger ist als die aktuelle Uhrzeit der Karte. In diesem Fall setzt die Karte ihre aktuelle Uhrzeit auf das Effective Date dieses Zertifikats. Die Karte darf nur die folgenden Zertifikate als gültige Zeitquelle akzeptieren:

— ERCA-Linkzertifikate der 2. Generation

— MSCA-Zertifikate der 2. Generation

— VU-Zertifikate der 2. Generation, die vom selben Land ausgestellt sind wie das bzw. die Kartenzertifikat(e) der Karte selbst.

Hinweis: Die letzte Anforderung impliziert, dass eine Karte die CAR des VU-Zertifikats, d. h. das MSCA_VU-EGF-Zertifikat, erkennen muss. Diese ist mit der CAR ihres eigenen Zertifikats, dem MSCA_Card-Zertifikat, nicht identisch.

CSM_168 Wie in Abbildung 5 angegeben, kann die Karte, sobald sie die Authentizität und Gültigkeit eines zuvor unbekannten Zertifikats überprüft hat, dieses Zertifikat zur zukünftigen Referenz abspeichern. Sie braucht dann die Authentizität dieses Zertifikats nicht ein weiteres Mal zu prüfen, wenn es ihr erneut vorgelegt wird. Die Karte braucht nicht das gesamte Zertifikat zu speichern, sondern lediglich den Inhalt des Zertifikatkörpers (siehe Abschnitt 9.3.2).

10.3. **VU-Authentisierung**

CSM_169 Fahrzeugeinheiten und Karten verwenden zur Authentisierung der VU gegenüber der Karte das VU-Authentisierungsprotokoll Abbildung 6. Durch die VU-Authentisierung kann die Fahrtenschreiberkarte explizit verifizieren, dass die VU authentisch ist. Dazu verwendet die VU ihren privaten Schlüssel, um eine von der Karte erzeugte Zufallszahl zu signieren.

CSM_170 Neben der Zufallszahl enthält die Signatur der VU die dem Kartenzertifikat entnommene Kennung des Karteninhabers.

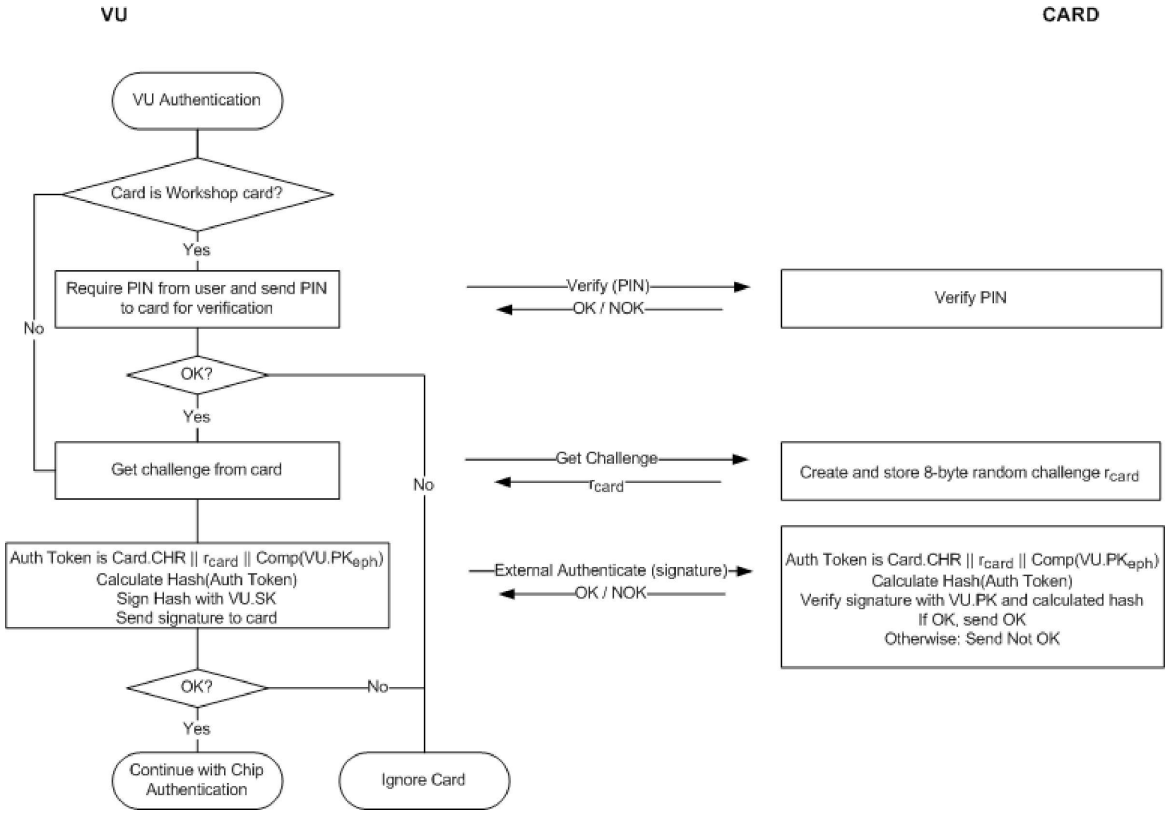
Hinweis: Dadurch lässt sich sicherstellen, dass es sich bei der Karte, gegenüber der die VU sich authentisiert, um dieselbe Karte handelt, deren Zertifikatkette die VU zuvor verifiziert hat.

CSM_171 Außerdem nimmt die VU in die Signatur die Kennung des flüchtigen öffentlichen Schlüssels Comp ($VU.PK_{eph}$) auf, mit dem die VU während der Chip-Authentisierung das Secure Messaging konfiguriert (siehe Abschnitt 10.4).

Hinweis: Dadurch wird sichergestellt, dass es sich bei der VU, mit der die Karte während einer Secure-Messaging-Sitzung kommuniziert, um die von der Karte authentisierte VU handelt.

Abbildung 6

VU-Authentisierungsprotokoll



CSM_172 Wenn die VU während der VU-Authentisierung mehrere Befehle GET CHALLENGE sendet, gibt die Karte jedes Mal einen neue 8-Byte-Zufallszahl zurück, speichert aber nur die letzte Zufallszahl.

CSM_173 Die VU verwendet zur VU-Authentisierung den Signaturalgorithmus ECDSA gemäß DSS; dabei wird der an die Schlüsselgröße des VU_MA-Schlüsselpaars der VU gebundene Hash-Algorithmus verwendet (siehe CSM_50). Das Signaturformat ist Klartext, wie in TR-03111 angegeben. Die VU sendet die resultierende Signatur an die Karte.

CSM_174 Nach Erhalt der VU-Signatur in einem Befehl EXTERNAL AUTHENTICATE führt die Karte Folgendes durch:

— Sie berechnet den Authentisierungstoken, indem sie Card.CHR, den r_{card} der Kartenzufallszahl und die Kennung des flüchtigen öffentlichen Schlüssels der VU, Comp(VU.PK_{eph}), verkettet,

— sie berechnet den Hash anhand des Authentisierungstokens, wobei sie den an die Schlüsselgröße des VU_MA-Schlüsselpaars der VU gebundenen Hash-Algorithmus verwendet (siehe CSM_50),

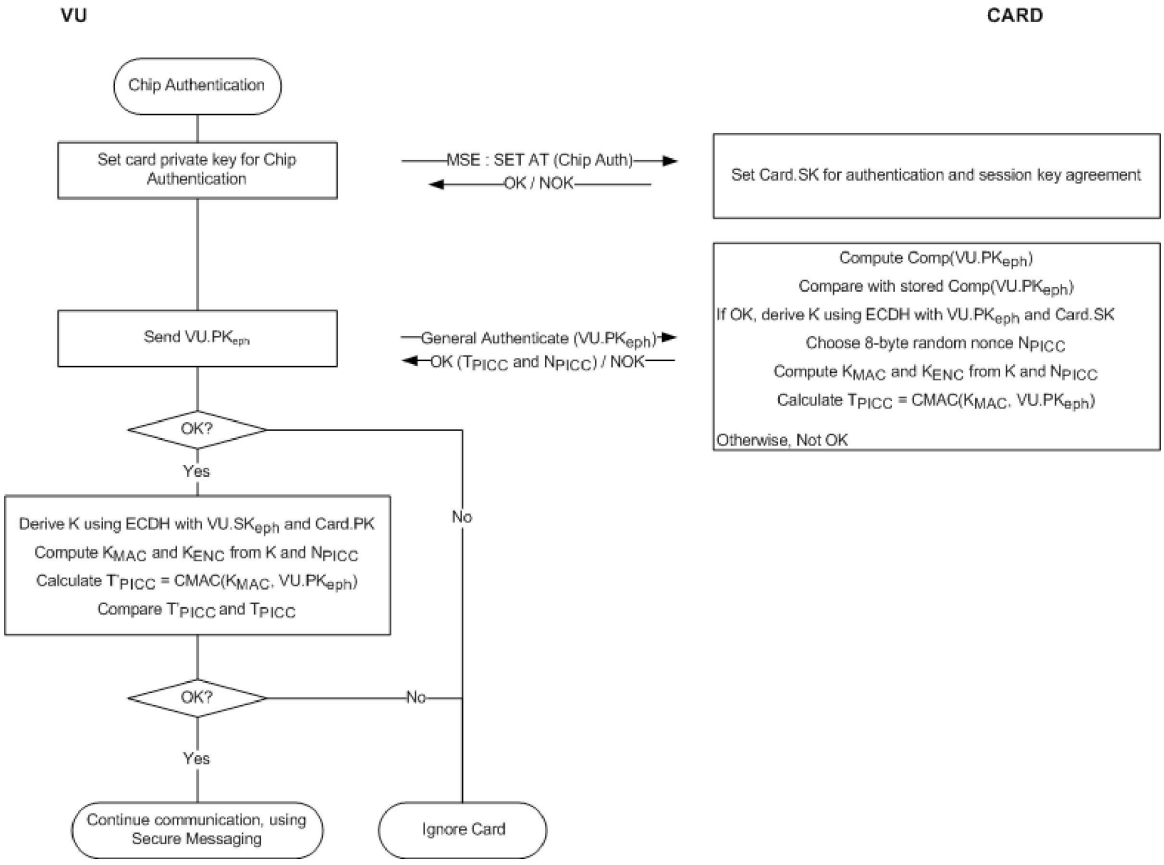
— sie überprüft die Signatur der VU unter Verwendung des ECDSA-Algorithmus in Kombination mit VU.PK und dem berechneten Hash.

10.4. Chip-Authentisierung und Vereinbarung des Sitzungsschlüssels

CSM_175 Fahrzeugeinheiten und Karten verwenden zur Authentisierung der Karte gegenüber der VU das Chip-Authentisierungsprotokoll **Abbildung 7**. Durch die Chip-Authentisierung kann die Fahrzeugeinheit explizit verifizieren, dass die Karte authentisch ist.

Abbildung 7

Chip-Authentisierung und Vereinbarung des Sitzungsschlüssels



CSM_176 VU und Karte gehen wie folgt vor:

1. Die Fahrzeugeinheit leitet die Chip-Authentisierung durch Senden des Befehls MSE: Set AT ein. Dieser zeigt eine Chip-Authentisierung unter Verwendung des ECDH-Algorithmus an; die Länge des AES-Sitzungsschlüssels ist an die Schlüsselgröße des Card_MA-Schlüsselpaars der Karte gebunden (siehe CSM_50). Die VU ermittelt aus dem Kartenzertifikat die Schlüsselgröße des Schlüsselpaars der Karte.

2. Die VU sendet den öffentlichen Punkt $VU.PK_{eph}$ ihres flüchtigen Schlüsselpaars an die Karte. Wie in CSM_164 erläutert, hat die VU dieses flüchtige Schlüsselpaar bereits vor der Verifizierung der VU-Zertifikatkette generiert. Dabei sendete die VU die Kennung des flüchtigen öffentlichen Schlüssels $Comp(VU.PK_{eph})$ an die Karte, die diese Kennung speicherte.

3. Die Karte berechnet nun $Comp(VU.PK_{eph})$ anhand von $VU.PK_{eph}$ und vergleicht diesen mit dem gespeicherten Wert von $Comp(VU.PK_{eph})$.

4. Mithilfe des ECDH-Algorithmus in Kombination mit dem statischen privaten Schlüssel der Karte und dem flüchtigen öffentlichen Schlüssel der VU berechnet die Karte einen geheimen Wert K.

5. Die Karte wählt eine zufällige 8-Byte-Nonce N_{PICC} und leitet mit dieser zwei AES-Sitzungsschlüssel K_{MAC} und K_{ENC} von K ab. Siehe CSM_179.

6. Mithilfe von K_{MAC} berechnet die Karte anhand der Kennung des flüchtigen öffentlichen Schlüssels der VU einen Authentisierungstoken: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Die Karte übermittelt N_{PICC} und T_{PICC} an die Fahrzeugeinheit.

7. Mithilfe des ECDH-Algorithmus in Kombination mit dem statischen privaten Schlüssel der Karte und dem flüchtigen privaten Schlüssel der VU berechnet die VU den geheimen Wert K auf die gleiche Weise, wie die Karte dies in Schritt 4 durchführte.

8. Die VU leitet die Sitzungsschlüssel K_{MAC} und K_{ENC} von K und N_{PICC} ab, siehe CSM_179.

9. Die VU verifiziert den Authentisierungstoken T_{PICC}.

CSM_177 In Schritt 3 oben berechnet die Karte Comp(VU.PKeph) als x-Koordinate des öffentlichen Punkts in VU.PKeph.

CSM_178 In den Schritten 4 und 7 oben verwenden Karte und Fahrzeugeinheit den ECKA-EG Algorithmus gemäß TR-03111.

CSM_179 In den Schritten 5 und 8 oben verwenden Karte und Fahrzeugeinheit die Schlüsselableitungsfunktion für AES-Sitzungsschlüssel gemäß TR-03111, mit den folgenden Präzisierungen und Änderungen:

— Der Zählerwert beträgt '00 00 00 01' für K_{ENC} und '00 00 00 02' für $K_{MAC.}$

— Es wird die optionale Nonce *r* verwendet, die mit N_{PICC} identisch ist.

— Zum Ableiten von 128-Bits-AES-Schlüsseln ist der Hash-Algorithmus SHA-256 zu verwenden.

— Zum Ableiten von 192-Bits-AES-Schlüsseln ist der Hash-Algorithmus SHA-384 zu verwenden.

— Zum Ableiten von 256-Bits-AES-Schlüsseln ist der Hash-Algorithmus SHA-512 zu verwenden.

Die Länge des Sitzungsschlüssels (d. h. die Länge, nach der der Hash abgeschnitten wird) ist an die Größe des Card_MA-Schlüsselpaars zu binden, siehe CSM_50.

CSM_180 In den Schritten 6 und 9 oben verwenden Karte und Fahrzeugeinheit den AES-Algorithmus im CMAC-Modus, wie in SP 800-38B festgelegt. Die Länge von T_{PICC} ist an die Länge des AES-Sitzungsschlüssels gemäß CSM_50 zu binden.

10.5. **Secure Messaging**

10.5.1 *Allgemein*

CSM_181 Alle zwischen Fahrzeugeinheit und Fahrtenschreiberkarte im Anschluss an eine erfolgreiche Chip-Authentisierung bis zum Sitzungsende ausgetauschten Befehle und Antworten sind durch den Secure-Messaging-Modus zu schützen.

CSM_182 Außer beim Lesen aus einer Datei mit Zugriffsbedingung SM-R-ENC-MAC-G2 (siehe Anlage 2 Abschnitt 4) muss das Secure Messaging im reinen Authentisierungsmodus stattfinden. In diesem Modus werden sämtliche Befehle und Antworten um eine kryptografische Prüfsumme (MAC) ergänzt, um die Authentizität und Integrität der Nachricht zu gewährleisten.

CSM_183 Beim Lesen von Daten aus einer Datei mit Zugriffsbedingung SM-R-ENC-MAC-G2 ist Secure Messaging im Modus Verschlüsseln-dann-Authentisieren zu verwenden. Das bedeutet, dass die Antwort zunächst verschlüsselt wird, um die Vertraulichkeit der Nachricht zu gewährleisten. Anschließend wird anhand der formatierten verschlüsselten Daten ein MAC berechnet, um Authentizität und Integrität sicherzustellen.

CSM_184 Beim Secure Messaging muss AES gemäß Definition im Referenzdokument AES mit den während der Chip-Authentisierung vereinbarten Sitzungsschlüsseln K_{MAC} und K_{ENC} verwendet werden.

CSM_185 Als Sendesequenzzähler (Send Sequence Counter, SSC) ist eine unsignierte Ganzzahl zu verwenden, um Replay-Angriffe zu verhindern. Die Größe des SSC muss mit derjenigen des AES-Blocks übereinstimmen, d. h. 128 Bits. Der SSC muss im Format MSB-first vorliegen. Beim Start von Secure Messaging ist der SSC auf null zu setzen (d. h. '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). Der SSC ist jedes Mal hochzusetzen, bevor eine Befehls- oder Antwort-APDU generiert wird: Da der SSC-Anfangswert in einer SM-Sitzung 0 beträgt, wird er im ersten Befehl auf 1 gesetzt. Der SSC-Wert der ersten Antwort lautet 2.

CSM_186 Zur Nachrichtenverschlüsselung ist K_{ENC} mit AES im CBC-Modus (Cipher Block Chaining) gemäß ISO 10116 zu verwenden, mit einem Verschachtelungsparameter m = 1 und einem Initialisierungsvektor SV = E(K_{ENC}, SSC), d. h. dem aktuellen SSC verschlüsselt mit K_{ENC}.

CSM_187 Zur Nachrichtenauthentisierung ist K_{MAC} mit AES in CMAC-Modus gemäß SP 800-38B zu verwenden. Die Länge des MAC ist an die Länge des AES-Sitzungsschlüssels gemäß CSM_50 zu binden. Der SSC ist im MAC vor dem zu authentisierenden Datenpaket einzufügen.

10.5.2 *Secure-Message-Struktur*

CSM_188 Beim Secure Messaging dürfen nur die in Tabelle 5 aufgeführten Secure-Messaging-Datenobjekte (siehe ISO 7816-4) verwendet werden. In allen Nachrichten sind diese Datenobjekte in der in dieser Tabelle angegebenen Reihenfolge zu verwenden.

Tabelle 5

Secure-Messaging-Datenobjekte

Datenobjektname	Tag	Vorgeschrieben (V), an Bedingungen geknüpft (B) oder untersagt (U) in	
		Befehlen	Antworten
Klarwert, nicht in BER-TLV kodiert	'81'	B	B
Klarwert, in BER-TLV kodiert, jedoch ohne SM DO	'B3'	B	B
Padding Indicator, gefolgt von Kryptogramm, Klarwert nicht in BER-TLV kodiert	'87'	B	B
Geschütztes Le	'97'	B	U
Verarbeitungsstatus	'99'	U	V
Kryptografische Prüfsumme (CC)	'8E'	V	V

Hinweis: Wie in Anlage 2 angegeben, können Fahrtenschreiberkarten die Befehle READ BINARY und UPDATE BINARY mit ungeradem INS-Byte ('B1' bzw. 'D7') unterstützen. Die Befehlsvarianten sind erforderlich, um Dateien mit 32 768 Bytes oder mehr zu lesen und zu aktualisieren. Falls eine Variante verwendet wird, ist anstelle eines Objekts mit Tag '81' ein Datenobjekt mit Tag 'B3' zu verwenden. Weitere Informationen siehe Anlage 2.

CSM_189 Alle SM-Datenobjekte sind gemäß ISO 8825-1 in DER TLV zu kodieren. Diese Kodierung bewirkt folgende TLV-Struktur (Tag-Length-Value, Tag-Längen-Wert):

Tag: Der Tag ist in ein oder zwei Oktette verschlüsselt und gibt den Inhalt an.

Länge: Die Länge ist als unsignierte Ganzzahl in ein, zwei oder drei Oktette verschlüsselt, was zu einer Länge von maximal 65 535 Oktetten führt. Es ist die Mindestzahl an Oktetten zu verwenden.

Wert: Der Wert ist in null oder mehr Oktette verschlüsselt.

CSM_190 Durch Secure Messaging geschützte APDU sind wie folgt zu erstellen:

— Der Befehlskopf ist in der MAC-Berechnung zu berücksichtigen, deshalb ist für das Klassenbyte CLA der Wert '0C' zu verwenden.

— Wie in Anlage 2 angegeben, müssen sämtliche INS-Bytes gerade sein, mit der möglichen Ausnahme ungerader INS-Bytes für die Befehle READ BINARY und UPDATE BINARY.

— Der tatsächliche Wert von Lc wird nach Anwendung von Secure Messaging in Lc' geändert.

— Das Datenfeld muss aus SM-Datenobjekten bestehen.

— Im geschützten APDU-Befehl ist das neue Le-Byte auf '00' zu setzen. Gegebenenfalls ist ein Datenobjekt '97' in das Datenfeld aufzunehmen, um den Originalwert von Le zu übertragen.

CSM_191 Sämtliche zu verschlüsselnde Datenobjekte sind gemäß ISO 7816-4 mithilfe von Padding Indicator '01' aufzufüllen. Zur Berechnung des MAC muss zudem jedes Datenobjekt im APDU separat gemäß ISO 7816-4 aufgefüllt werden.

Hinweis: Bei Secure Messaging erfolgt das Auffüllen immer durch die Secure-Messaging-Schicht, nicht durch die CMAC- oder CBC-Algorithmen.

Zusammenfassung und Beispiele

Ein APDU-Befehl mit angewandtem Secure Messaging besitzt die folgende Struktur, je nach dem jeweiligen ungesicherten Befehl (DO ist Datenobjekt):

Fall 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Fall 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Fall 3 (gerades INS-Byte):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Fall 3 (ungerades INS-Byte):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Fall 4 (gerades INS-Byte):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Fall 4 (ungerades INS-Byte):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

Dabei ist Le = '00' oder '00 00', je nachdem, ob kurze Längenfelder oder erweiterte Längenfelder verwendet werden; siehe ISO 7816-4.

Eine APDU-Antwort mit angewandtem Secure Messaging besitzt die folgende Struktur, je nach dem jeweiligen ungesicherten Befehl (DO ist Datenobjekt):

Fall 1 oder 3:	DO '99' || DO '8E' || SW1SW2
Fall 2 oder 4 (gerades INS-Byte) mit Verschlüsselung:	DO '81' || DO '99' || DO '8E' || SW1SW2
Fall 2 oder 4 (gerades INS-Byte) ohne Verschlüsselung:	DO '87' || DO '99' || DO '8E' || SW1SW2
Fall 2 oder 4 (ungerades INS-Byte) ohne Verschlüsselung:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Hinweis: Fall 2 oder 4 (ungerades INS-Byte) mit Verschlüsselung kommt in der Kommunikation zwischen VU und Karte nie zum Einsatz.

Im Folgenden sind drei APDU-Transformationen für Befehle mit geradem INS-Code beispielhaft aufgeführt. Abbildung 8 zeigt einen authentisierten APDU-Befehl für Fall 4, Abbildung 9 zeigt eine authentisierte APDU-Antwort für Fall 2/Fall 4, und Abbildung 10 zeigt eine verschlüsselte und authentisierte APDU-Antwort für Fall 2/Fall 4.

Abbildung 8

Transformation eines authentisierten APDU-Befehls für Fall 4

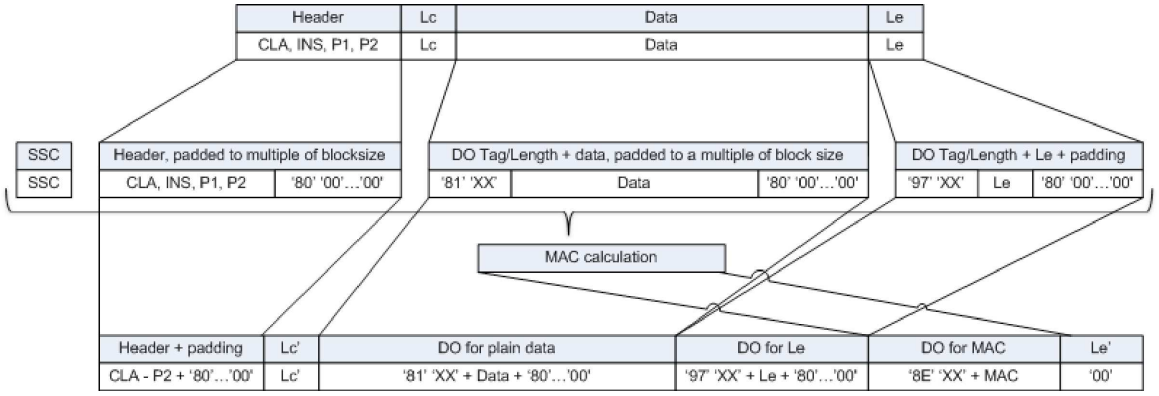


Abbildung 9

Transformation einer authentisierten Antwort-APDU für Fall 1/Fall 3

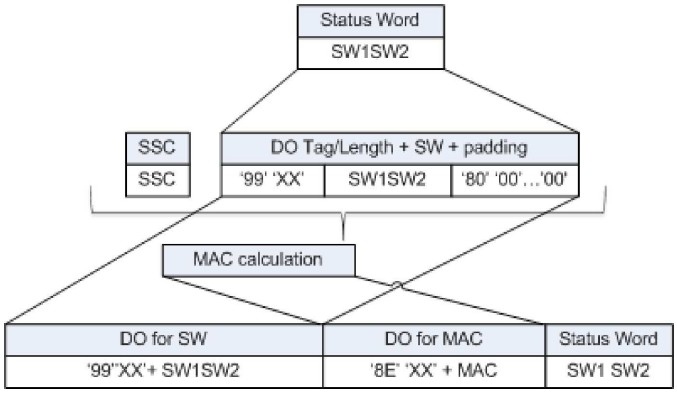
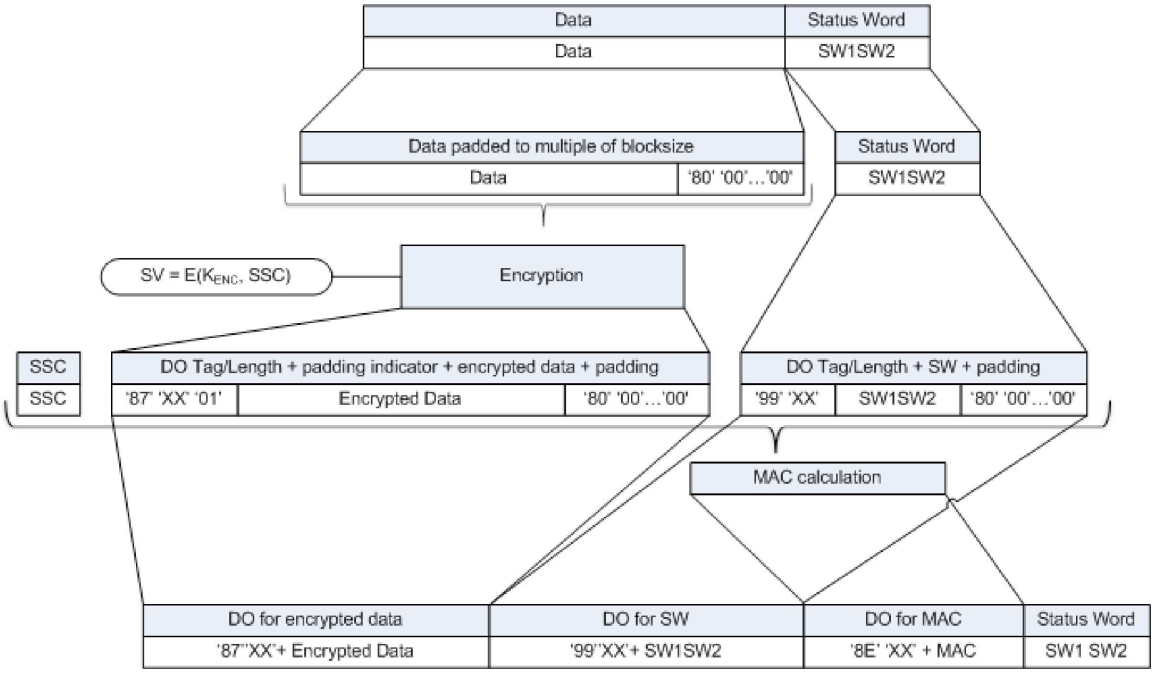


Abbildung 10

Transformation einer verschlüsselten und authentisierten Antwort-APDU für Fall 2/Fall 4



10.5.3 *Abbruch einer Secure-Messaging-Sitzung*

CSM_192 Eine Fahrzeugeinheit muss eine laufende Secure-Messaging-Sitzung abbrechen, wenn (und nur wenn) eine der folgenden Bedingungen eintritt:

— Sie erhält eine APDU-Antwort in Klartext.

— Sie entdeckt in einer APDU-Antwort einen Secure-Messaging-Fehler:

— Ein erwartetes Secure-Messaging-Datenobjekt fehlt, die Reihenfolge der Datenobjekte ist falsch, oder ein unbekanntes Datenobjekt ist vorhanden.

— Ein Secure-Messaging-Datenobjekt ist falsch, z. B. der MAC-Wert ist falsch, die TLV-Struktur ist fehlerhaft, oder der Padding Indicator in Tag '87' ist nicht gleich '01'.

— Die Karte sendet ein Statusbyte, laut dem sie einen SM-Fehler entdeckt hat (siehe CSM_194).

— Der Grenzwert für die innerhalb der aktuellen Sitzung zulässige Anzahl an Befehlen und zugehörigen Antworten ist erreicht. Dieser Grenzwert wird für eine VU von ihrem Hersteller festgelegt, der dabei die Sicherheitsanforderungen der verwendeten Hardware berücksichtigt; der Höchstwert beträgt 240 SM-Befehle und zugehörige Antworten pro Sitzung.

CSM_193 Eine Fahrtenschreiberkarte muss eine laufende Secure-Messaging-Sitzung abbrechen, wenn (und nur wenn) eine der folgenden Bedingungen eintritt:

— Sie erhält einen APDU-Befehl in Klartext.

— Sie entdeckt in einem APDU-Befehl einen Secure-Messaging-Fehler:

— Ein erwartetes Secure-Messaging-Datenobjekt fehlt, die Reihenfolge der Datenobjekte ist falsch, oder ein unbekanntes Datenobjekt ist vorhanden.

— Ein Secure-Messaging-Datenobjekt ist fehlerhaft, beispielsweise ist der MAC-Wert oder die TLV-Struktur fehlerhaft.

— Sie ist ohne Stromversorgung oder wurde zurückgesetzt.

— Die VU wählt eine Anwendung auf der Karte.

— Die VU leitet die VU-Authentisierung ein.

— Der Grenzwert für die innerhalb der aktuellen Sitzung zulässige Anzahl an Befehlen und zugehörigen Antworten ist erreicht. Dieser Grenzwert wird für eine Karte von ihrem Hersteller festgelegt, der dabei die Sicherheitsanforderungen der verwendeten Hardware berücksichtigt; der Höchstwert beträgt 240 SM-Befehle und zugehörige Antworten pro Sitzung.

CSM_194 SM-Fehlerbehandlung durch eine Fahrtenschreiberkarte:

— Wenn in einem APDU-Befehl erwartete Secure-Messaging-Datenobjekte fehlen, die Reihenfolge der Datenobjekte falsch ist oder unbekannte Datenobjekte vorhanden sind, antwortet die Fahrtenschreiberkarte mit den Statusbytes '69 87'.

— Wenn ein Secure-Messaging-Datenobjekt in einem APDU-Befehl falsch ist, antwortet die Fahrtenschreiberkarte mit Statusbytes '69 88'.

In einem solchen Fall werden die Statusbytes ohne SM zurückgesendet.

CSM_195 Wenn eine Secure-Messaging-Sitzung zwischen VU und Fahrtenschreiberkarte abgebrochen wird, führen VU und Fahrtenschreiberkarte Folgendes durch:

— Sie zerstören die gespeicherten Sitzungsschlüssel auf sichere Weise.

— Sie leiten sofort eine neue Secure-Messaging-Sitzung ein, wie in den Abschnitten 10.2 — 10.5 beschrieben.

CSM_196 Wenn die VU aus beliebigem Grund entscheidet, die gegenseitige Authentisierung mit einer eingesetzten Karte neu zu starten, beginnt der Prozess mit der Verifizierung der Zertifikatkette der Karte (siehe Abschnitt 10.2) und geht dann gemäß den Abschnitten 10.2 — 10.5 weiter.

11. VU UND EXTERNE GNSS-AUSRÜSTUNG: KOPPELUNG, GEGENSEITIGE AUTHENTISIERUNG UND SECURE MESSAGING

11.1. **Allgemein**

CSM_197 Bei der von einer VU zur Ermittlung ihrer Position genutzten GNSS-Ausrüstung kann es sich um ein internes (d. h. in das VU-Gehäuse fest integriertes) oder externes Modul handeln. Im ersten Fall ist es nicht nötig, die interne Kommunikation zwischen GNSS-Ausrüstung und VU zu standardisieren; die Anforderungen dieses Kapitels gelten deshalb nicht. Im zweiten Fall muss die Kommunikation zwischen VU und externer GNSS-Ausrüstung nach den Beschreibungen in diesem Kapitel standardisiert und geschützt werden.

CSM_198 Die sichere Kommunikation zwischen Fahrzeugeinheit und externer GNSS-Ausrüstung erfolgt genauso wie die sichere Kommunikation zwischen Fahrzeugeinheit und Fahrtenschreiberkarte, wobei die externe GNSS-Ausrüstung (EGF) die Rolle der Karte einnimmt. Die externe GNSS-Ausrüstung muss alle in Kapitel 10 für Fahrtenschreiberkarten erwähnten Anforderungen erfüllen, wobei die in diesem Kapitel genannten Abweichungen, Klärungen und Ergänzungen zu berücksichtigen sind. Insbesondere müssen gegenseitige Verifizierung der Zertifikatkette, VU-Authentisierung und Chip-Authentisierung gemäß den Abschnitten 11.3 und 11.4 erfolgen.

CSM_199 Die Kommunikation zwischen Fahrzeugeinheit und EGF unterscheidet sich von der Kommunikation zwischen Fahrzeugeinheit und Karte insofern, als Fahrzeugeinheit und EGF einmal in einer Werkstatt gekoppelt werden müssen, damit VU und EGF im Normalbetrieb GNSS-basierte Daten austauschen können. Die Koppelung wird in Abschnitt 11.2 beschrieben.

CSM_200 Zur Kommunikation zwischen Fahrzeugeinheit und EGF sind APDU-Befehle und -Antworten gemäß ISO 7816-4 und ISO 7816-8 zu verwenden. Die genaue Struktur dieser APDU ist in Anlage 2 dieses Anhangs festgelegt.

11.2. **Koppelung von VU und externer GNSS-Ausrüstung**

CSM_201 Fahrzeugeinheit und EGF in einem Fahrzeug müssen durch eine Werkstatt gekoppelt werden. Nur gekoppelte Fahrzeugeinheiten und EGF dürfen im Normalbetrieb kommunizieren.

CSM_202 Die Koppelung von Fahrzeugeinheit und EGF darf nur möglich sein, wenn sich die Fahrzeugeinheit im Kalibrierungsmodus befindet. Die Koppelung ist durch die Fahrzeugeinheit einzuleiten.

CSM_203 Eine Werkstatt kann eine Fahrzeugeinheit jederzeit mit einer anderen oder derselben EGF neu koppeln. Während der Neukoppelung muss die VU das in ihrem Speicher vorhandene EGF_MA-Zertifikat auf sichere Weise zerstören und das EGF_MA-Zertifikat der EGF, mit der sie gekoppelt wird, im Speicher ablegen.

CSM_204 Eine Werkstatt kann eine externe GNSS-Ausrüstung jederzeit mit einer anderen oder derselben VU neu koppeln. Während der Neukoppelung muss die EGF das in ihrem Speicher vorhandene VU_MA-Zertifikat auf sichere Weise zerstören und das VU_MA-Zertifikat der VU, mit der sie gekoppelt wird, im Speicher ablegen.

11.3. **Gegenseitige Verifizierung der Zertifikatkette**

11.3.1 *Allgemein*

CSM_205 Die gegenseitige Verifizierung der Zertifikatkette zwischen VU und EGF kann nur während der Koppelung von VU und EGF durch eine Werkstatt erfolgen. Im Normalbetrieb gekoppelter VU und EGF werden keine Zertifikate verifiziert. Stattdessen vertrauen VU und EGF den während der Koppelung gespeicherten Zertifikaten, überprüfen allerdings deren temporäre Gültigkeit. Um im Normalbetrieb die Kommunikation zwischen VU und EGF zu schützen, vertrauen VU und EGF lediglich diesen Zertifikaten.

11.3.2 *Während der Koppelung VU-EGF*

CSM_206 Während der Koppelung an eine EGF verwendet die Fahrzeugeinheit das in Abbildung 4 (Abschnitt 10.2.1) dargestellte Protokoll, um die Zertifikatkette der externen GNSS-Ausrüstung zu verifizieren.

Hinweise zu Abbildung 4 in diesem Kontext:

— Die Kommunikationskontrolle ist nicht Gegenstand dieser Anlage. Allerdings handelt es sich bei einer EGF nicht um eine Chipkarte, weshalb die VU vermutlich kein Reset zum Einleiten der Kommunikation senden und kein ATR erhalten wird.

— Die in der Abbildung genannten Zertifikate und öffentlichen Schlüssel der Karte sind als Zertifikate und öffentlichen Schlüssel der EGF zur gegenseitigen Authentisierung zu verstehen. In Abschnitt 9.1.6 werden sie als EGF_MA bezeichnet.

— Die in der Abbildung genannten Card.CA-Zertifikate und öffentlichen Schlüssel sind als Zertifikate und öffentlichen Schlüssel der MSCA zum Signieren der EGF-Zertifikate zu verstehen. In Abschnitt 9.1.3 werden sie als MSCA_VU-EGF bezeichnet.

— Das in der Abbildung erwähnte Card.CA.EUR-Zertifikat ist als das europäische Wurzelzertifikat zu verstehen, das in der CAR des MSCA-VU-EGF-Zertifikats angegeben ist.

— Das in der Abbildung erwähnte Card.Link-Zertifikat ist als das Linkzertifikat der EGF zu verstehen, sofern vorhanden. Wie in Abschnitt 9.1.2 angegeben, handelt es sich hierbei um ein Linkzertifikat für ein neues europäisches Wurzel-Schlüsselpaar, das durch die ERCA erstellt und mithilfe des zuvor erwähnten europäischen privaten Schlüssels signiert wird.

— Bei dem Card.Link.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des Card.Link-Zertifikats angegeben ist.

— Anstelle der `cardExtendedSerialNumber` liest die VU die `sensorGNSSserialNumber` aus der EF-ICC.

— Die VU wählt nicht die Fahrtenschreiber-AID, sondern die EGF-AID.

— „Karte ignorieren“ ist als „EGF ignorieren“ zu verstehen.

CSM_207 Wenn die Fahrzeugeinheit das EGF_MA-Zertifikat verifiziert hat, speichert sie es zur Verwendung im Normalbetrieb; siehe Abschnitt 11.3.3.

CSM_208 Während der Koppelung an eine VU verwendet die externe GNSS-Ausrüstung das in Abbildung 5 (Abschnitt 10.2.2) dargestellte Protokoll, um die Zertifikatkette der VU zu verifizieren.

Hinweise zu Abbildung 5 in diesem Kontext:

— Die VU generiert mithilfe der Domänenparameter im EGF-Zertifikat ein neues flüchtiges Schlüsselpaar.

— Bei den in der Abbildung erwähnten VU-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur gegenseitigen Authentisierung. In Abschnitt 9.1.4 werden sie als VU_MA bezeichnet.

— Bei den in der Abbildung erwähnten VU.CA-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur Signierung der Zertifikate von VU und externer GNSS-Ausrüstung. In Abschnitt 9.1.3 werden sie als MSCA_VU-EGF bezeichnet.

— Bei dem in der Abbildung erwähnten VU.CA.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des VU.CA-Zertifikats angegeben ist.

— Das in der Abbildung erwähnte VU.Link-Zertifikat ist das Linkzertifikat der VU, sofern vorhanden. Wie in Abschnitt 9.1.2 angegeben, handelt es sich hierbei um ein Linkzertifikat für ein neues europäisches Wurzel-Schlüsselpaar, das durch die ERCA erstellt und mithilfe des zuvor erwähnten europäischen privaten Schlüssels signiert wird.

— Bei dem VU.Link.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des VU.Link-Zertifikats angegeben ist.

CSM_209 In Abweichung von Anforderung CSM_167 verwendet eine EGF die GNSS-Zeit, um die temporäre Gültigkeit präsentierter Zertifikate zu überprüfen.

CSM_210 Wenn die externe GNSS-Ausrüstung das VU_MA-Zertifikat verifiziert hat, speichert sie es zur Verwendung im Normalbetrieb; siehe Abschnitt 11.3.3.

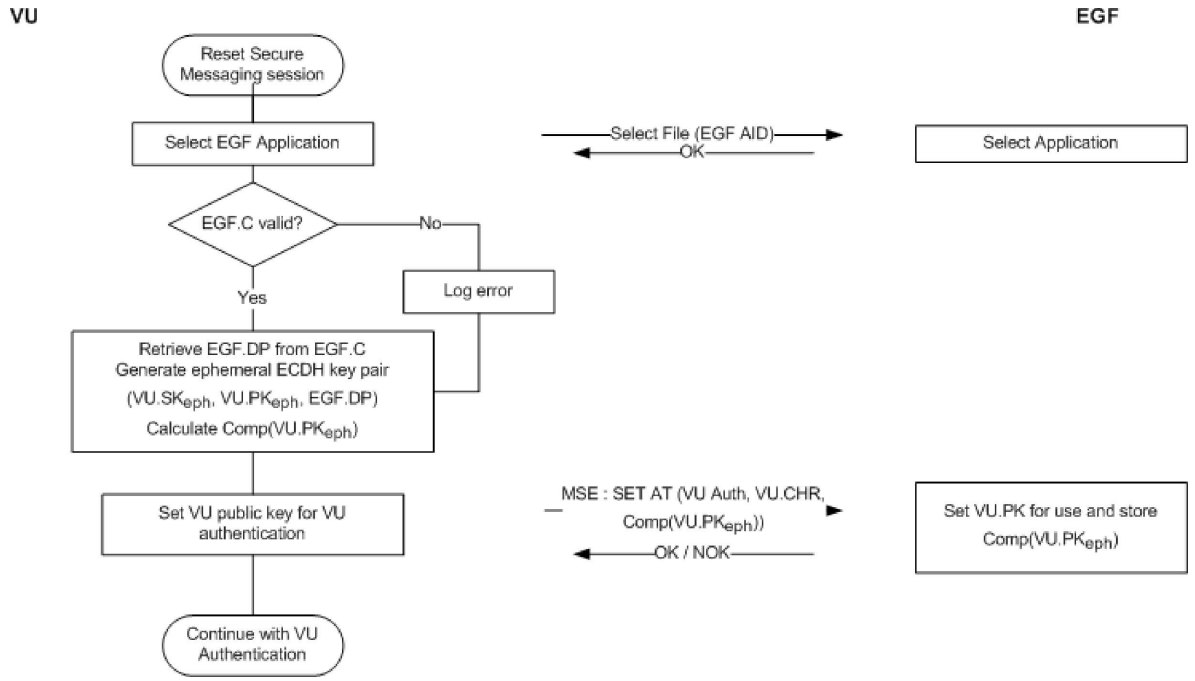
11.3.3 *Im Normalbetrieb*

CSM_211 Im Normalbetrieb verwenden Fahrzeugeinheit und EGF das in Abbildung 11 dargestellte Protokoll, um die temporäre Gültigkeit der gespeicherten EGF_MA- und VU_MA-Zertifikate zu überprüfen und um den öffentlichen VU_MA-Schlüssel zur anschließenden VU-Authentisierung festzulegen. Im Normalbetrieb findet keine weitere gegenseitige Verifizierung der Zertifikatketten statt.

Hinweis: Abbildung 11 besteht im Wesentlichen aus den ersten in Abbildung 4 und Abbildung 5 dargestellten Schritten. Wie bereits erwähnt, handelt es sich bei einer EGF nicht um eine Chipkarte, weshalb die VU vermutlich kein Reset zum Einleiten der Kommunikation senden und kein ATR erhalten wird. Dies ist nicht Gegenstand dieser Anlage.

Abbildung 11

Gegenseitige Verifizierung der temporären Gültigkeit von Zertifikaten im normalen VU-EGF-Betrieb



CSM_212 Wie in Abbildung 11 dargestellt, meldet die Fahrzeugeinheit einen Fehler, wenn das EGF_MA-Zertifikat nicht mehr gültig ist. Allerdings erfolgen gegenseitige Authentisierung, Schlüsselvereinbarung und anschließende Kommunikation per Secure Messaging normal.

11.4. VU-Authentisierung, Chip-Authentisierung und Vereinbarung des Sitzungsschlüssels

CSM_213 VU-Authentisierung, Chip-Authentisierung und Sitzungsschlüsselvereinbarung zwischen VU und EGF erfolgen im Rahmen der Koppelung und jedes Mal, wenn im Normalbetrieb eine Secure-Messaging-Sitzung wiederhergestellt wird. VU und EGF gehen wie in den Abschnitten 10.3 und 10.4 erläutert vor. Es gelten sämtliche Anforderungen dieser Abschnitte.

11.5. Secure Messaging

CSM_214 Alle zwischen Fahrzeugeinheit und externer GNSS-Ausrüstung im Anschluss an eine erfolgreiche Chip-Authentisierung bis zum Sitzungsende ausgetauschten Befehle und Antworten sind durch Secure Messaging im reinen Authentisierungsmodus zu schützen. Es gelten sämtliche Anforderungen von Abschnitt 10.5.

CSM_215 Wenn eine Secure-Messaging-Sitzung zwischen VU und EGF abgebrochen wird, leitet die VU sofort eine neue Secure-Messaging-Sitzung ein (siehe Abschnitte 11.3.3 und 11.4).

12. KOPPELUNG UND KOMMUNIKATION VU-BEWEGUNGSSENSOR

12.1. **Allgemein**

CSM_216 Die Kommunikation zwischen Fahrzeugeinheit und Bewegungssensor während der Koppelung und im Normalbetrieb hat mithilfe des in ISO 16844-3 spezifizierten Schnittstellenprotokolls zu erfolgen, unter Vornahme der in diesem Kapitel und in Abschnitt 9.2.1 beschriebenen Änderungen.

Hinweis: Es wird vorausgesetzt, dass die Leserinnen und Leser dieses Kapitels mit den Inhalten von ISO 16844-3 vertraut sind.

12.2. **Koppelung VU-Bewegungssensor unter Verwendung verschiedener Schlüsselgenerationen**

Wie in Abschnitt 9.2.1 erläutert, werden der Hauptschüssel des Bewegungssensors und alle damit verbundenen Schlüssel regelmäßig ersetzt. Dies führt dazu, dass in Werkstattkarten bis zu drei AES-Schlüssel $K_{M\text{-}WC}$ (fortlaufender Schlüsselgenerationen) für den Bewegungssensor vorhanden sind. Ebenso können in Bewegungssensoren bis zu drei verschiedene AES-basierte Datenverschlüsselungen (basierend auf fortlaufenden Generationen des K_M-Bewegungssensor-Hauptschlüssels) vorhanden sein. Eine Fahrzeugeinheit enthält nur einen $K_{M\text{-}VU}$-Schlüssel für den Bewegungssensor.

CSM_217 Eine VU der 2. Generation und ein Bewegungssensor der 2. Generation sind wie folgt zu koppeln (vergleiche Tabelle 6 in ISO 16844-3):

1. Eine Werkstattkarte der zweiten Generation wird in die VU eingesteckt und diese mit dem Bewegungssensor verbunden.

2. Die VU liest alle auf der Werkstattkarte verfügbaren $K_{M\text{-}WC}$-Schlüssel, geht deren Versionsnummern durch und wählt denjenigen aus, der mit der Versionsnummer des $K_{M\text{-}VU}$-Schlüssels der VU übereinstimmt. Befindet sich der passende $K_{M\text{-}WC}$-Schlüssel nicht auf der Werkstattkarte, bricht die VU den Koppelungsprozess ab und zeigt dem Inhaber der Werkstattkarte eine entsprechende Fehlermeldung an.

3. Die VU berechnet den Bewegungssensor-Hauptschlüssel K_M aus dem $K_{M\text{-}VU}$ und dem $K_{M\text{-}WC}$ sowie den Identifikationsschlüssel K_{ID} aus dem K_M, wie in Abschnitt 9.2.1 spezifiziert.

4. Die VU sendet den Befehl zum Einleiten des Koppelungsprozesses an den Bewegungssensor, wie in ISO 16844-3 beschrieben, und verschlüsselt die Seriennummer, die sie vom Bewegungssensor erhält, mit dem Identifikationsschlüssel $K_{ID.}$ Die VU sendet die verschlüsselte Seriennummer zurück an den Bewegungssensor.

5. Der Bewegungssensor gleicht die verschlüsselte Seriennummer nacheinander mit jeder intern vorhandenen Verschlüsselung der Seriennummer ab. Wenn er das passende Gegenstück findet, wird die VU authentisiert. Der Bewegungssensor erkennt die von der VU verwendete K_{ID}-Generation und sendet die kodierte Version des Koppelungsschlüssels, d. h. die Verschlüsselung, die mithilfe derselben K_M-Generation erstellt wurde, zurück.

6. Die VU entschlüsselt den Koppelungsschlüssel mithilfe des K_M, generiert einen Sitzungsschlüssel $K_{S,}$ verschlüsselt ihn mit dem Koppelungsschlüssel und sendet das Ergebnis an den Bewegungssensor. Der Bewegungssensor entschlüsselt den K_S.

7. Die VU setzt die Koppelungsinformation gemäß ISO 16844-3 zusammen, verschlüsselt die Information mit dem Koppelungsschlüssel und sendet das Ergebnis an den Bewegungssensor. Der Bewegungssensor entschlüsselt die Koppelungsinformation.

8. Der Bewegungssensor verschlüsselt die empfangene Koppelungsinformation mit dem empfangenen K_S und sendet sie an die VU zurück. Die VU prüft, ob die Koppelungsinformation mit derjenigen übereinstimmt, die die VU im vorherigen Schritt an den Bewegungssensor gesendet hat. Falls ja, ist damit belegt, dass der Bewegungssensor denselben K_S verwendet hat wie die VU und somit in Schritt 5 seinen mit der korrekten K_M-Generation verschlüsselten Koppelungsschlüssel gesendet hat. Der Bewegungssensor ist somit authentisiert.

Es ist zu beachten, dass die Schritte 2 und 5 vom Standardprozess gemäß ISO 16844-3 abweichen; die übrigen Schritte entsprechen dem Standardprozess.

Beispiel: Angenommen, im ersten Jahr der Gültigkeit des ERCA (3)-Zertifikats findet eine Koppelung statt; siehe Abbildung 2 in Abschnitt 9.2.1.2, und

— angenommen, der Bewegungssensor wurde im letzten Jahr der Gültigkeit des ERCA (1)-Zertifikats ausgestellt. Unter diesen Umständen enthält er die folgenden Schlüssel und Daten:

  — $N_s[1]$: seine Seriennummer, verschlüsselt mit K_{ID}-Generation 1

  — $N_s[2]$: seine Seriennummer, verschlüsselt mit K_{ID}-Generation 2

  — $N_s[3]$: seine Seriennummer, verschlüsselt mit K_{ID}-Generation 3

  — $K_P[1]$: seinen Koppelungsschlüssel der 1. Generation ([1]), verschlüsselt mit K_M-Generation 1

  — $K_P[2]$: seinen Koppelungsschlüssel der 2. Generation, verschlüsselt mit K_M-Generation 2

  — $K_P[3]$: seinen Koppelungsschlüssel der 3. Generation, verschlüsselt mit K_M-Generation 3

— Angenommen, die Werkstattkarte wurde im ersten Jahr der Gültigkeit des ERCA (3)-Zertifikats ausgestellt. Unter diesen Umständen enthält sie den Schlüssel $K_{M\text{-}WC}$ der 2. und 3. Generation.

— Angenommen, bei der VU handelt es sich um eine VU der 2. Generation, die die 2. Generation des $K_{M\text{-}VU}$ enthält.

Unter diesen Umständen geschieht in den Schritten 2–5 Folgendes:

— Schritt 2: Die VU liest den $K_{M\text{-}WC}$ der 2. und 3. Generation von der Werkstattkarte und prüft deren Versionsnummern.

— Schritt 3: Die VU kombiniert den $K_{M\text{-}WC}$ der 2. Generation mit $K_{M\text{-}VU}$, um $K_{M\ und}$ K_{ID} zu berechnen.

— Schritt 4: Die VU verschlüsselt die Seriennummer, die sie vom Bewegungssensor erhält, mit dem $K_{ID.}$

— Schritt 5: Der Bewegungssensor vergleicht die empfangenen Daten mit $N_s[1]$ und findet kein Gegenstück. Dann vergleicht er die Daten mit $N_s[2]$ und findet ein Gegenstück. Er folgert, dass es sich bei der VU um eine VU der 2. Generation handelt, und sendet daher $K_p[2]$ zurück.

12.3. **Koppelung und Kommunikation VU-Bewegungssensor mit AES**

CSM_218 Wie in Tabelle 3 in Abschnitt 9.2.1 spezifiziert, handelt es sich bei allen Schlüsseln, die an der Koppelung einer Fahrzeugeinheit (der 2. Generation) und eines Bewegungssensors sowie an der nachfolgenden Kommunikation beteiligt sind, nicht um T-DES-Schlüssel doppelter Länge, sondern um AES-Schlüssel (siehe ISO 16844-3). Diese AES-Schlüssel können eine Länge von 128, 192 oder 256 Bits aufweisen. Da die AES-Blockgröße bei 16 Bytes liegt, muss die Länge einer verschlüsselten Nachricht ein Mehrfaches von 16 Bytes betragen (T-DES: 8 Bytes). Darüber hinaus werden einige dieser Nachrichten für die Übertragung von AES-Schlüsseln verwendet, deren Länge bei 128, 192 oder 256 Bits liegen kann. Daher ist die Anzahl an Datenbyte pro Anweisung in Tabelle 5 von ISO 16844-3 gemäß folgender Tabelle 6 zu verändern:

Tabelle 6

Anzahl der Klartext- und verschlüsselten Datenbyte pro Befehl gemäß ISO 16844-3

Anweisung	Anforderung/ Antwort	Beschreibung der Daten:	Anz. der Klartext-Datenbytes gemäß ISO 16844-3	Anz. der Klartext-Datenbytes bei Verwendung von AES-Schlüsseln	Anz. der verschlüsselten Datenbytes bei Verwendung von AES-Schlüsseln mit Bitlänge		
					128	192	256
10	Anforderung	Authentisierungsdaten + Nummer der Datei	8	8	16	16	16

([1]) Es ist zu beachten, dass es sich bei den Koppelungsschlüsseln der 1., 2. und 3. Generation um denselben Schlüssel oder aber um drei verschiedene, unterschiedlich lange Schlüssel handeln kann, wie in CSM_117 erläutert.

Anweisung	Anforderung/ Antwort	Beschreibung der Daten:	Anz. der Klartext-Datenbytes gemäß ISO 16844-3	Anz. der Klartext-Datenbytes bei Verwendung von AES-Schlüsseln	Anz. der verschlüsselten Datenbytes bei Verwendung von AES-Schlüsseln mit Bitlänge		
					128	192	256
11	Antwort	Authentisierungsdaten + Inhalte der Datei	16 oder 32, je nach Datei	16 oder 32, je nach Datei	16/32	16/32	16/32
41	Anforderung	Seriennummer des Sensors	8	8	16	16	16
41	Antwort	Koppelungsschlüssel	16	16/24/32	16	32	32
42	Anforderung	Sitzungsschlüssel	16	16/24/32	16	32	32
43	Anforderung	Koppelungsinformation	24	24	32	32	32
50	Antwort	Koppelungsinformation	24	24	32	32	32
70	Anforderung	Authentisierungsdaten	8	8	16	16	16
80	Antwort	Zählerwert Bewegungssensor + Authentisierungsdaten	8	8	16	16	16

CSM_219 Die Koppelungsinformation, die in den Anweisungen 43 (VU-Anforderung) und 50 (Antwort des Bewegungssensors) gesendet wird, ist gemäß der Beschreibung in Abschnitt 7.6.10 von ISO 16844-3 zusammenzusetzen, allerdings wird anstelle des T-DES-Algorithmus im Verschlüsselungssystem für die Koppelungsdaten der AES-Algorithmus verwendet, sodass zwei AES-Verschlüsselungen erfolgen und die in CSM_220 beschriebene Auffüllmethode passend zur AES-Blockgröße angewandt wird. Der für diese Verschlüsselung verwendete Schlüssel K'_P wird wie folgt generiert:

— Wenn der Koppelungsschlüssel K_P 16 Bytes lang ist: $K'_P = K_P \text{ XOR } (N_s||N_s)$

— Wenn der Koppelungsschlüssel K_P 24 Bytes lang ist: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$

— Wenn der Koppelungsschlüssel K_P 32 Bytes lang ist: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

wobei N_s die 8-Byte-Seriennummer des Bewegungssensors ist.

CSM_220 Falls die Länge der Klartextdaten (bei Verwendung von AES-Schlüsseln) kein Vielfaches von 16 Bytes ist, hat die in ISO 9797-1 beschriebene Auffüllmethode 2 zur Anwendung zu kommen.

Hinweis: In ISO 16844-3 ist die Anzahl der Klartext-Datenbytes stets ein Vielfaches von 8, sodass bei Verwendung von T-DES kein Auffüllen erforderlich ist. Die Definition der Daten und Nachrichten in ISO 16844-3 wird durch diesen Teil der Anlage nicht verändert, was die Anwendung der Auffüllmethode erforderlich macht.

CSM_221 Für Anweisung 11 und falls mehr als ein Datenblock verschlüsselt werden muss, ist der Betriebsmodus Cipher Block Chaining gemäß ISO 10116 zu verwenden, mit einem Verschachtelungsparameter von $m = 1$. Der zu verwendende IV ist:

— für Anweisung 11: der in Abschnitt 7.6.3.3 von ISO 16844-3 spezifizierte 8-Byte-Authentisierungsblock, aufgefüllt mithilfe der in ISO 9797-1 beschriebenen Auffüllmethode 2; siehe auch Abschnitte 7.6.5 und 7.6.6 von ISO 16844-3.

— für alle anderen Befehle, in denen mehr als 16 Bytes übertragen werden, wie in Tabelle 6 spezifiziert: '00' {16}, d. h. sechzehn Bytes mit Binärwert 0.

Hinweis: Wie in den Abschnitten 7.6.5 und 7.6.6 von ISO 16844-3 beschrieben, wird — wenn der Bewegungssensor Dateien für die Einbeziehung in Anweisung 11 verschlüsselt — der Authentisierungsblock sowohl

— als Initialisierungsvektor für die Verschlüsselung der Dateien mithilfe des CBC-Modus verwendet als auch

— verschlüsselt und als erster Block in die Daten einbezogen, die an die VU gesendet werden.

12.4. **Koppelung VU-Bewegungssensor bei verschiedenen Gerätegenerationen**

CSM_222 Wie in Abschnitt 9.2.1 erläutert, kann ein Bewegungssensor der zweiten Generation die T-DES-basierte Verschlüsselung der Koppelungsdaten (wie in Teil A dieser Anlage definiert) enthalten, wodurch sich der Bewegungssensor mit einer VU der 1. Generation koppeln lässt. In diesem Fall sind eine VU der 1. Generation und ein Bewegungssensor der 2. Generation so zu koppeln, wie in Teil A dieser Anlage und in ISO 16844-3 beschrieben. Für den Koppelungsprozess kann eine Werkstattkarte der 1. oder 2. Generation verwendet werden.

Hinweise:

— Eine VU der 2. Generation kann nicht mit einem Bewegungssensor der 1. Generation gekoppelt werden.

— Eine Werkstattkarte der 1. Generation kann nicht zur Koppelung einer VU der 2. Generation an einen Bewegungssensor verwendet werden.

13. SICHERHEIT FÜR FERNKOMMUNIKATION PER DSRC

13.1. **Allgemein**

Wie in Anlage 14 spezifiziert, generiert eine VU regelmäßig Daten zur Fernüberwachung des Fahrtenschreibers (Remote Tachograph Monitoring, RTM) und sendet diese an die (interne oder externe) Fernkommunikationsvorrichtung (Remote Communication Facility, RCF). Die RCF sendet diese Daten über die in Anlage 14 beschriebene DSRC-Schnittstelle an die Fernabfrageeinrichtung (Remote Interrogator, RI). Gemäß Anlage 1 sind die RTM-Daten eine Verkettung von:

Fahrtenschreibernutzdaten die Verschlüsselung der Klartextnutzdaten des Fahrtenschreibers

DSRC-Sicherheitsdaten weiter unten beschrieben

Das Format der Klartextnutzdaten des Fahrtenschreibers ist in Anlage 1 spezifiziert und in Anlage 14 genauer erläutert. Dieser Abschnitt beschreibt die Struktur der DSRC-Sicherheitsdaten; die formale Spezifikation findet sich in Anlage 1.

CSM_223 Die `tachographPayload`-Klartextdaten, die von einer VU an eine RCF (wenn die RCF sich außerhalb der VU befindet) oder von der VU per DSRC-Schnittstelle an den RI (wenn die RCF sich innerhalb der VU befindet) gesendet werden, sind im Modus Verschlüsseln-dann-Authentisieren zu schützen, d. h., die Fahrtenschreibernutzdaten werden zunächst verschlüsselt, um die Vertraulichkeit der Nachricht sicherzustellen, und anschließend wird ein MAC berechnet, um die Authentizität und Integrität der Daten zu gewährleisten.

CSM_224 Die DSRC-Sicherheitsdaten müssen aus einer Verkettung folgender Datenelemente in folgender Reihenfolge bestehen; siehe auch Abbildung 12:

Current date time	aktuelles Datum und aktuelle Uhrzeit der Fahrzeugeinheit (Datentyp `TimeReal`)
Counter	ein 3-Byte-Zähler, siehe CSM_225

VU serial number	die Seriennummer der VU (Datentyp `VuSerialNumber`)
DSRC master key version number	die 1-Byte-Versionsnummer des DSRC-Hauptschlüssels, von dem die VU-spezifischen DSRC-Schlüssel abgeleitet wurden, siehe Abschnitt 9.2.2.
MAC	der mithilfe aller vorausgehenden Bytes in den RTM-Daten berechnete MAC

CSM_225 Der 3-Byte-Zähler in den DSRC-Sicherheitsdaten muss im Format MSB-first vorliegen. Bei der ersten Berechnung eines RTM-Datensatzes nach ihrer Inproduktionsnahme setzt die VU den Wert des Zählers auf 0. Die VU erhöht den Wert der Zählerdaten vor jeder Berechnung eines weiteren RTM-Datensatzes um 1.

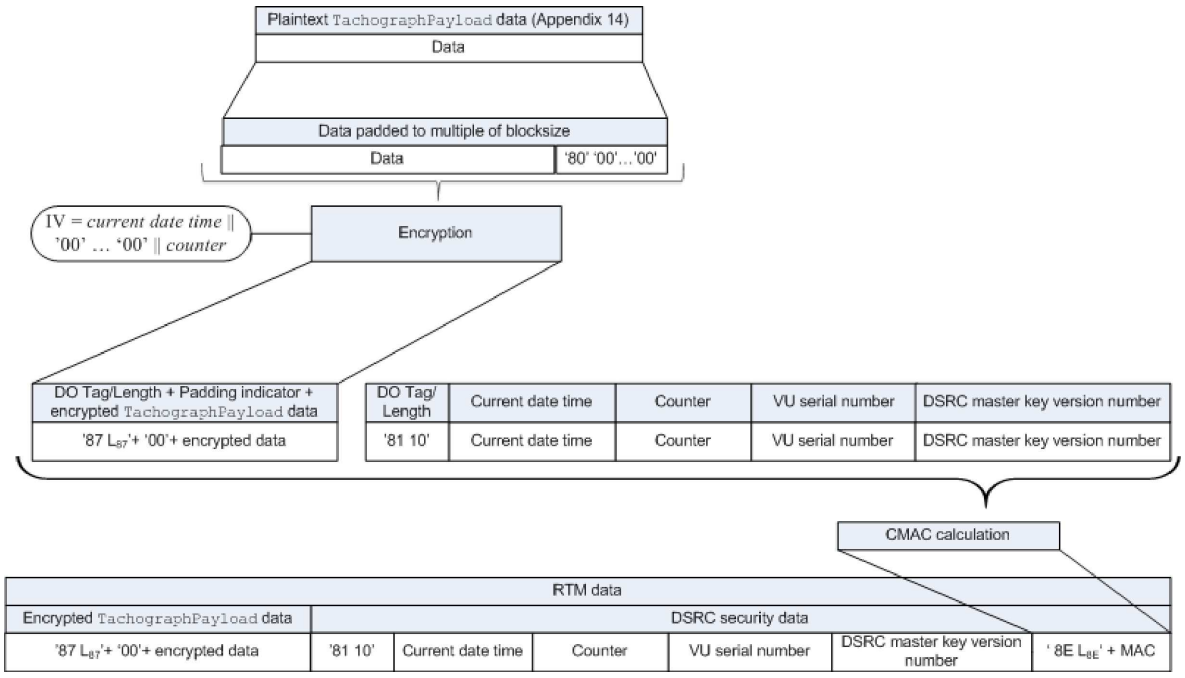
13.2. Verschlüsselung der Fahrtenschreibernutzdaten und MAC-Generierung

CSM_226 Bei Vorliegen eines Klartext-Datenelements vom Datentyp `TachographPayload` im Sinne von Anlage 14 verschlüsselt eine VU diese Daten gemäß Abbildung 12: Der DSRC-Schlüssel der VU für die Verschlüsselung $K\_VU_{DSRC}\_ENC$ (siehe Abschnitt 9.2.2) ist mit AES im Betriebsmodus Cipher Block Chaining (CBC) gemäß ISO 10116 zu verwenden, mit einem Verschachtelungsparameter von *m* = 1. Der Initialisierungsvektor muss *IV = current date time* ||*'00 00 00 00 00 00 00 00'* || *counter* entsprechen, wobei *current date time* und *counter* in CSM_224 spezifiziert sind. Die zu verschlüsselnden Daten sind mit der in ISO 9797-1 definierten Auffüllmethode 2 aufzufüllen.

CSM_227 Die VU berechnet MAC in den DSRC-Sicherheitsdaten gemäß Abbildung 12: Der MAC ist mithilfe aller vorausgehenden Bytes in den RTM-Daten zu berechnen, bis einschließlich der DSRC-Hauptschlüsselversionsnummer und einschließlich der Tags und Längen der Datenobjekte. Die VU muss ihren DSRC-Schlüssel zur Authentizität $K\_VU_{DSRC}\_MAC$ verwenden (siehe Abschnitt 9.2.2), mit dem AES-Algorithmus im CMAC-Modus (siehe SP 800-38B). Die Länge des MAC ist an die Länge des VU-spezifischen DSRC-Schlüssels gebunden (siehe CSM_50).

Abbildung 12

Verschlüsselung der Fahrtenschreibernutzdaten und MAC-Generierung



13.3. **Verifizierung und Entschlüsselung der Fahrtenschreibernutzdaten**

CSM_228 Wenn ein RI von einer VU RTM-Daten erhält, muss er die gesamten RTM-Daten an eine Kontrollkarte im Datenfeld eines Befehls PROCESS DSRC MESSAGE senden (siehe Anlage 2). Anschließend gilt:

1. Die Kontrollkarte überprüft die DSRC-Hauptschlüsselversionsnummer in den DSRC-Sicherheitsdaten. Wenn die Kontrollkarte den angegebenen DSRC-Hauptschlüssel nicht kennt, muss sie eine Fehlermeldung gemäß Anlage 2 zurücksenden und den Prozess abbrechen.

2. Die Kontrollkarte verwendet den angegebenen DSRC-Hauptschlüssel in Kombination mit der VU-Seriennummer in den DSRC-Sicherheitsdaten, um daraus die VU-spezifischen DSRC-Schlüssel K_VU_{DSRC}_ENC und K_VU_{DSRC}_MAC abzuleiten (siehe CSM_124).

3. Die Kontrollkarte verwendet K_VU_{DSRC}_MAC, um den MAC in den DSRC-Sicherheitsdaten zu überprüfen (siehe CSM_227). Wenn der MAC inkorrekt ist, muss die Kontrollkarte eine Fehlermeldung gemäß Anlage 2 zurücksenden und den Prozess abbrechen.

4. Die Kontrollkarte verwendet K_VU_{DSRC}_ENC, um die verschlüsselten Fahrtenschreibernutzdaten zu entschlüsseln, wie in CSM_226 spezifiziert. Die Kontrollkarte entfernt die Auffüllung und sendet die verschlüsselten Fahrtenschreibernutzdaten an den RI zurück.

CSM_229 Um Replay-Angriffe zu verhindert, muss der RI die Frische der RTM-Daten überprüfen, indem er sicherstellt, dass *current date time* in den DSRC-Sicherheitsdaten nicht zu sehr von der aktuellen Zeit des RI abweicht.

Hinweise:

— Hierfür muss der RI über eine präzise und verlässliche Zeitquelle verfügen.

— Da eine VU gemäß Anlage 14 alle 60 Sekunden einen neuen RTM-Datensatz berechnen muss und die Uhr der VU 1 Minute von der Echtzeit abweichen darf, beträgt die untere Grenze für die Frische der RTM-Daten 2 Minuten. Die jeweiligen Frischeanforderungen hängen auch von der Genauigkeit der RI-Uhr ab.

CSM_230 Wenn eine Werkstatt das einwandfreie Funktionieren der DSRC-Funktion der VU überprüft, sendet sie alle von der VU erhaltenen RTM-Daten an eine Werkstattkarte im Datenfeld eines Befehls PROCESS DSRC MESSAGE (siehe Anlage 2). Die Werkstattkarte muss alle in CSM_228 angegebenen Prüfungen und Aktionen durchführen.

14. SIGNIEREN VON DATENDOWNLOADS UND VERIFIZIEREN DER SIGNATUREN

14.1. **Allgemein**

CSM_231 Das Intelligent Dedicated Equipment (IDE) speichert die von einer VU oder Karte während eines Übertragungsvorgangs empfangenen Daten in einer Datei ab. Daten können auf einem externen Speichermedium (ESM) gespeichert werden. Die Datei enthält digitale Signaturen von Datenblöcken gemäß Anlage 7. Die betreffende Datei muss außerdem folgende Zertifikate enthalten (siehe Abschnitt 9.1):

— im Falle eines VU-Downloads:

  — das VU_Sign-Zertifikat

  — das MSCA_VU-EGF-Zertifikat mit dem öffentlichen Schlüssel zur Verifizierung des VU_Sign-Zertifikats

— im Falle eines Kartendownloads:

— das Card_Sign-Zertifikat

— das MSCA_Card-Zertifikat mit dem öffentlichen Schlüssel zur Verifizierung des Card_Sign-Zertifikats

CSM_232 Das IDE muss außerdem über Folgendes verfügen:

— falls es eine Kontrollkarte zur Verifizierung der Signatur verwendet, wie in Abbildung 13 gezeigt: das Linkzertifikat, das das neueste EUR-Zertifikat gegebenenfalls mit dem direkt davor gültigen EUR-Zertifikat verknüpft.

— falls es die Signatur selbst verifiziert: alle gültigen europäischen Wurzelzertifikate.

Hinweis: Die Methode, mit der das IDE diese Zertifikate abruft, ist in dieser Anlage nicht spezifiziert.

14.2. **Erzeugung der Signatur**

CSM_233 Als Signaturalgorithmus zur Erzeugung digitaler Signaturen anhand heruntergeladener Daten wird ECDSA gemäß DSS verwendet; dabei ist der an die Schlüsselgröße der VU oder Karte gebundene Hash-Algorithmus zu verwenden (siehe CSM_50). Das Signaturformat ist Klartext, wie in TR-03111 angegeben.

14.3. **Verifizierung der Signatur**

CSM_234 Ein IDE kann die Verifizierung einer Signatur anhand heruntergeladener Daten selbst durchführen oder zu diesem Zweck eine Kontrollkarte verwenden. Falls es eine Kontrollkarte verwendet, ist die Verifizierung der Signatur gemäß Abbildung 13 durchzuführen. Falls es die Verifizierung der Signatur selbst durchführt, muss das IDE die Authentizität und Gültigkeit aller Zertifikate in der Zertifikatkette der Datei sowie die Signatur anhand Daten gemäß dem in DSS definierten Signatursystem überprüfen.

Hinweise zu Abbildung 13:

— Das Gerät, das die zu analysierenden Daten signiert hat, ist mit EQT bezeichnet.

— Bei den in der Abbildung erwähnten EQT-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur Signierung von Kartenzertifikaten, d. h. VU_Sign oder Card_Sign.

— Bei den in der Abbildung erwähnten EQT.CA-Zertifikaten und öffentlichen Schlüsseln handelt es sich um diejenigen zur Signierung der Zertifikate von VU bzw. Karte.

— Bei dem in der Abbildung erwähnten EQT.CA.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des EQT.CA-Zertifikats angegeben ist.

— Das in der Abbildung erwähnte EQT.Link-Zertifikat ist das Linkzertifikat des Geräts, sofern vorhanden. Wie in Abschnitt 9.1.2 angegeben, handelt es sich hierbei um ein Linkzertifikat für ein neues europäisches Wurzel-Schlüsselpaar, das durch die ERCA erstellt und mithilfe des zuvor erwähnten europäischen privaten Schlüssels signiert wird.

— Bei dem EQT.Link.EUR-Zertifikat handelt es sich um das europäische Wurzelzertifikat, das in der CAR des EQT.Link-Zertifikats angegeben ist.

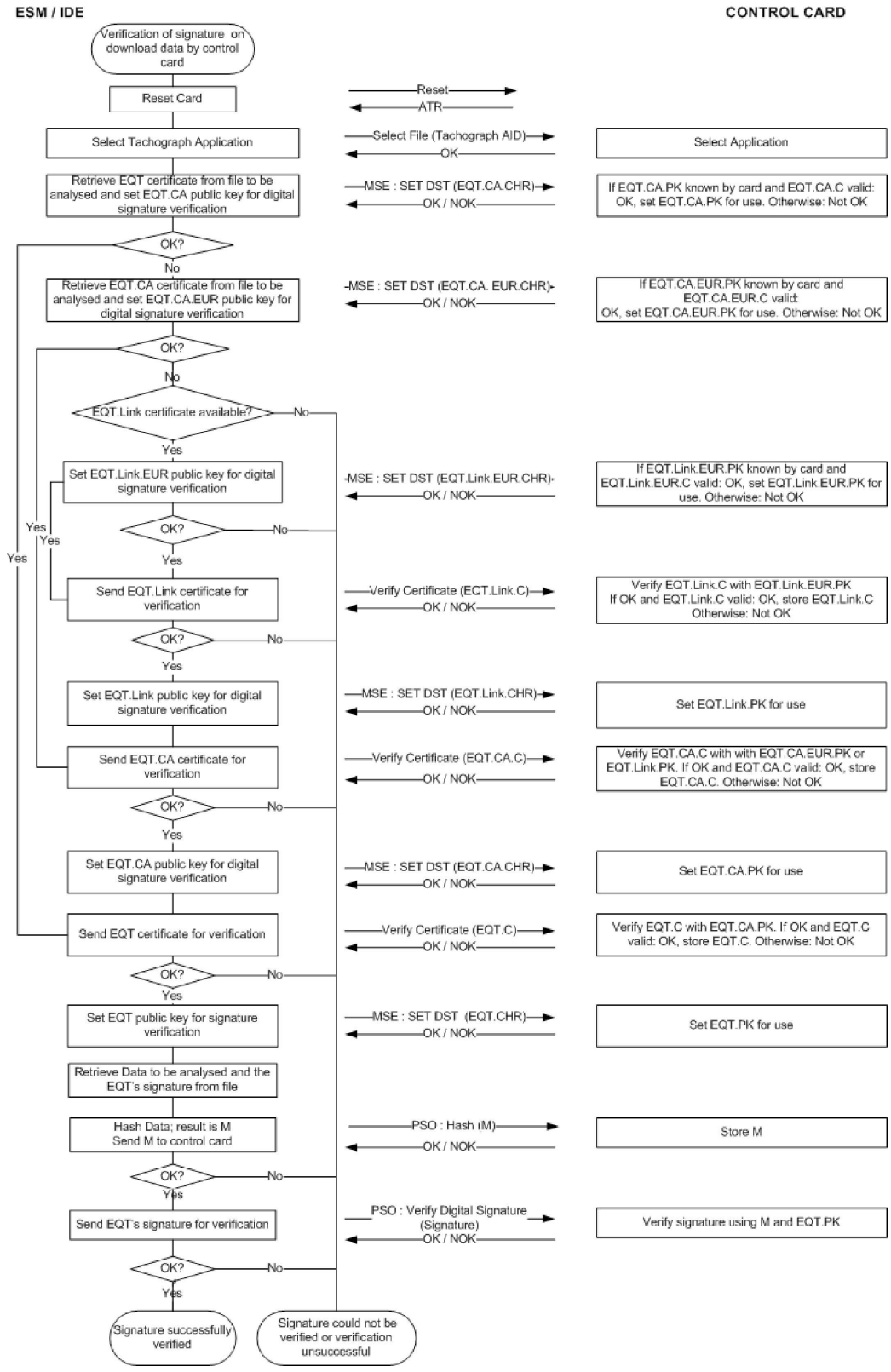
CSM_235 Zur Berechnung des Hashwerts M, der im Befehl PSO:Hash an die Kontrollkarte gesendet wird, verwendet das IDE den Hash-Algorithmus, der mit der Schlüsselgröße der VU oder der Karte, von der die Daten heruntergeladen werden, verlinkt ist (siehe CSM_50).

CSM_236 Bei der Verifizierung der Signatur des Geräts folgt die Kontrollkarte dem in DSS definierten Signatursystem.

Das vorliegende Dokument spezifiziert keinerlei Maßnahmen für den Fall, dass die Signatur über eine heruntergeladene Datei nicht verifiziert werden kann oder die Verifizierung erfolglos ist.

Abbildung 13

Protokoll für die Verifizierung der Signatur mithilfe einer heruntergeladenen Datei



Anlage 12

POSITIONSBESTIMMUNG MITHILFE EINES GLOBALEN SATELLITENNAVIGATIONSSYSTEMS (GNSS)

INHALTSVERZEICHNIS

1. EINLEITUNG 405

1.1. Anwendungsbereich 405

1.2. Akronyme und Notationen 405

2. SPEZIFIKATION DES GNSS-EMPFÄNGERS 406

3. NMEA-DATENSÄTZE 406

4. FAHRZEUGEINHEIT MIT EXTERNER GNSS-AUSRÜSTUNG 408

4.1. Konfiguration 408

4.1.1 Hauptkomponenten und Schnittstellen 408

4.1.2 Zustand der externen GNSS-Ausrüstung am Ende der Produktion 408

4.2. Kommunikation zwischen der externen GNSS-Ausrüstung und der Fahrzeugeinheit 409

4.2.1 Kommunikationsprotokoll 409

4.2.2 Sichere Übertragung von GNSS-Daten 411

4.2.3 Struktur des Befehls Read Record 412

4.3. Kopplung, gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung der externen GNSS-Ausrüstung mit der Fahrzeugeinheit 413

4.4. Fehlerbehandlung 413

4.4.1 Kommunikationsfehler mit der externen GNSS-Ausrüstung 413

4.4.2 Verletzung der physischen Integrität der externen GNSS-Ausrüstung. 413

4.4.3 Fehlende Positionsdaten des GNSS-Empfängers 413

4.4.4 Abgelaufenes Zertifikat der externen GNSS-Ausrüstung 414

5. FAHRZEUGEINHEIT OHNE EXTERNE GNSS-AUSRÜSTUNG 414

5.1. Konfiguration 414

5.2. Fehlerbehandlung 414

5.2.1 Fehlende Positionsdaten des GNSS-Empfängers 414

6. GNSS-ZEITKONFLIKT 414

7. DATENKONFLIKT FAHRZEUGBEWEGUNG 415

1. EINLEITUNG

Diese Anlage enthält die technischen Anforderungen für die von der Fahrzeugeinheit verwendeten GNSS-Daten, einschließlich der Protokolle, die implementiert werden müssen, um die sichere und korrekte Übertragung der Positionsbestimmungsinformationen zu gewährleisten.

Die wichtigsten Artikel dieser Verordnung (EU) Nr. 165/2014, die diese Anforderungen regeln, sind: „Artikel 8 Aufzeichnung des Fahrzeugstandorts an bestimmten Punkten bzw. Zeitpunkten während der täglichen Arbeitszeit", „Artikel 10 Schnittstelle zu intelligenten Verkehrssystemen" und „Artikel 11 Einzelvorschriften für intelligente Fahrtenschreiber".

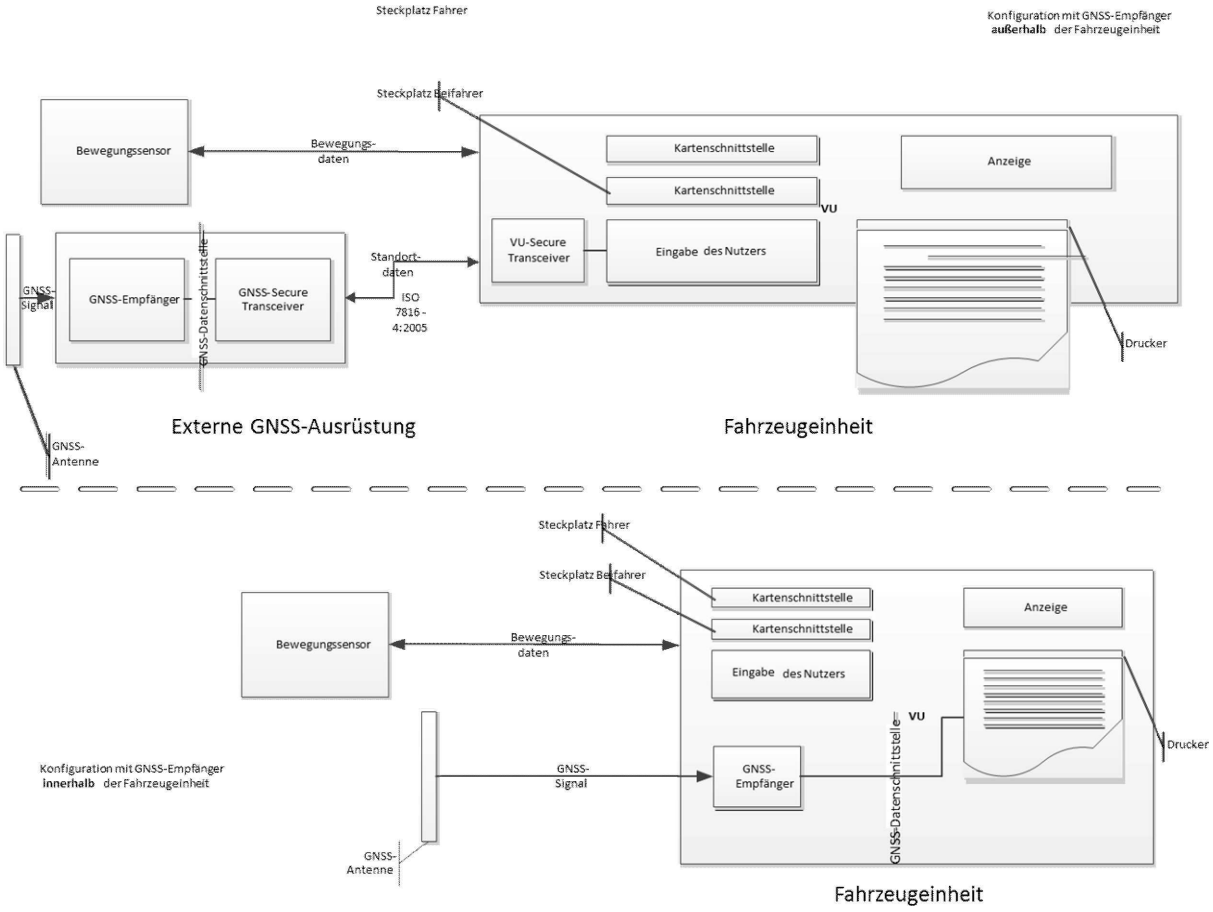
1.1. **Anwendungsbereich**

GNS_1 Die Fahrzeugeinheit muss Standortdaten von mindestens einem globalen GNSS erfassen, im Sinne der Durchführung von Artikel 8.

Die Fahrzeugeinheit kann gegebenenfalls über eine externe GNSS-Ausrüstung verfügen (siehe Abbildung 1):

Abbildung 1

Verschiedene Konfigurationen für den GNSS-Empfänger.



1.2. **Akronyme und Notationen**

In dieser Anlage werden folgende Akronyme verwendet:

DOP Dilution of Precision (Verschlechterung der Genauigkeit)

EGF Elementary file GNSS Facility (Elementardatei GNSS-Ausrüstung)

EGNOS European Geostationary Navigation Overlay Service (Europäische Erweiterung des geostationären Navigationssystems)

GNSS Global Navigation Satellite System (Globales Satellitennavigationssystem)

GSA GPS DOP und aktive Satelliten

HDOP Horizontal Dilution of Precision (Horizontalgenauigkeit)

ICD Interface Control Document (Schnittstellendokument)

NMEA National Marine Electronics Association (US-amerikanische Vereinigung für Marineelektronik)

PDOP Position Dilution of Precision (Positionsgenauigkeit)

RMC Recommended Minimum Specific (Empfohlener minimaler spezifischer Datensatz)

SIS Signal in Space (Signal im Raum)

VDOP Vertical Dilution of Precision (Vertikalgenauigkeit)

VU Fahrzeugeinheit

2. SPEZIFIKATION DES GNSS-EMPFÄNGERS

Unabhängig von der Konfiguration des intelligenten Fahrtenschreibers — mit oder ohne externer GNSS-Ausrüstung — ist die Bereitstellung präziser und verlässlicher Positionsbestimmungsinformationen eine wesentliche Voraussetzung für den effektiven Betrieb des intelligenten Fahrtenschreibers. Daher sollte seine Kompatibilität mit den Diensten, die gemäß der Verordnung (EU) Nr. 1285/2013 des Europäischen Parlaments und des Rates durch das Galileo-Programm und das Programm zur Europäischen Erweiterung des geostationären Navigationssystems (EGNOS) bereitgestellt werden, verlangt werden ([1]). Bei dem im Rahmen des Galileo-Programms eingerichteten System handelt es sich um ein unabhängiges globales Satellitennavigationssystem, bei dem im Rahmen von EGNOS eingerichteten System hingegen um ein regionales Satellitennavigationssystem zur Verbesserung der Qualität des GPS-Signals.

GNS_2 Die Hersteller müssen gewährleisten, dass die GNSS-Empfänger in den intelligenten Fahrtenschreibern mit den durch die Galileo- und EGNOS-Systeme bereitgestellten Positionsbestimmungsdiensten kompatibel sind. Die Hersteller können außerdem die Kompatibilität mit anderen Satellitennavigationssystemen gewährleisten.

GNS_3 Der GNSS-Empfänger muss fähig sein, die Authentisierung im Offenen Dienst von Galileo zu unterstützen, sofern dieser Dienst vom Galileo-System erbracht und von den Herstellern der GNSS-Empfänger unterstützt wird. Für intelligente Fahrtenschreiber, die auf den Markt gebracht wurden, bevor die vorstehenden Bedingungen erfüllt sind und die nicht fähig sind, die Authentisierung im Offenen Dienst von Galileo zu unterstützen, ist jedoch keine Nachrüstung vorgeschrieben.

3. NMEA-DATENSÄTZE

In diesem Abschnitt werden die NMEA-Datensätze beschrieben, die für das Funktionieren des intelligenten Fahrtenschreibers verwendet werden. Dieser Abschnitt gilt für die Konfiguration des intelligenten Fahrtenschreibers sowohl mit als auch ohne externe GNSS-Ausrüstung.

GNS_4 Die Standortdaten basieren auf dem von der NMEA empfohlenen minimalen spezifischen Datensatz (Recommended Minimum Specific, RMC) für das GNSS, der die Positionsinformation (Breite, Länge), die Zeit im UTC-Format (hhmmss.ss), die Geschwindigkeit in Knoten über Grund sowie zusätzliche Werte umfasst.

Der RMC-Datensatz weist folgendes Format auf (gemäß Norm NMEA V4.1):

([1]) Verordnung (EU) Nr. 1285/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 betreffend den Aufbau und den Betrieb der europäischen Satellitennavigationssysteme und zur Aufhebung der Verordnung (EG) Nr. 876/2002 und Verordnung (EG) Nr. 683/2008 des Rates und des Europäischen Parlaments und des Rates (ABl. L 347 vom 20.12.2013, S. 1).

Abbildung 2

Struktur des RMC-Datensatzes

1) Zeit (UTC)
2) Status, A = Gültige Position, V = Warnung
3) Breite
4) N oder S
5) Länge
6) O oder W
7) Geschwindigkeit in Knoten über Grund
8) Wahrer Kurs, Grad
9) Datum, TTMMJJ
10) Magnetische Deklination, Grad
11) O oder W
12) Prüfsumme

Der Status zeigt an, ob das GNSS-Signal verfügbar ist. Solange der Statuswert nicht auf A gesetzt ist, können die empfangenen Daten (z. B. Uhrzeit oder Breite/Länge) nicht verwendet werden, um die Position des Fahrzeugs in der VU aufzuzeichnen.

Die Auflösung der Position basiert auf dem oben beschriebenen RMC-Datensatzformat. Der erste Teil der Felder 3) und 5) (die ersten zwei Zahlen) wird verwendet, um die Gradwerte darzustellen. Der Rest dient dazu, die Minuten mit drei Dezimalzahlen darzustellen. Die Auflösung ist also 1/1000 Minute oder 1/60000 Grad (da eine Minute 1/60 Grad ist).

GNS_5 Die Fahrzeugeinheit muss die Positionsinformation zur Breite und Länge mit einer Auflösung von 1/10 Minute oder 1/600 Grad in der VU-Datenbank speichern, wie in Anlage 1 für GeoCoordinates beschrieben.

Der Befehl GPS DOP und aktive Satelliten (GSA) kann von der VU verwendet werden, um die Signalverfügbarkeit und -genauigkeit zu bestimmen und aufzuzeichnen. Die HDOP dient insbesondere dazu, die Genauigkeit der aufgezeichneten Standortdaten anzugeben (siehe 4.2.2). Die VU speichert den Wert der Horizontalgenauigkeit (HDOP), der als niedrigster der in den verfügbaren GNSS-Systemen erfassten HDOP-Werte berechnet wird.

Die ID des GNSS-Systems gibt an, ob es sich um GPS, Glonass, Galileo, Beidou oder das Satellite-Based Augmentation System (SBAS) handelt.

Abbildung 3

Struktur des GSA-Datensatzes

1) Auswahlmodus
2) Modus
3) ID des 1. für die Ortung verwendeten Satelliten
4) ID des 2. für die Ortung verwendeten Satelliten
...
14) ID des 12. für die Ortung verwendeten Satelliten
15) PDOP in Metern
16) HDOP in Metern
17) VDOP in Metern
18) ID des GNSS-Systems
19) Prüfsumme

Der Modus 2) gibt an, ob eine Ortung (Fix) nicht verfügbar (Modus=1), für 2D verfügbar (Modus=2) oder für 3D verfügbar (Modus=3) ist.

GNS_6 Der *GSA*-Datensatz muss unter der Datensatznummer '06' gespeichert werden.

GNS_7 Die maximale Größe der NMEA-Datensätze (z. B. RMC, GSA oder sonstige) für den Befehl Read Record beträgt 85 Bytes (siehe Tabelle 1).

4. FAHRZEUGEINHEIT MIT EXTERNER GNSS-AUSRÜSTUNG

4.1. **Konfiguration**

4.1.1 *Hauptkomponenten und Schnittstellen*

In dieser Konfiguration ist der GNSS-Empfänger Teil der externen GNSS-Ausrüstung.

GNS_8 Die externe GNSS-Ausrüstung muss über eine spezielle Fahrzeugschnittstelle eingeschaltet werden.

GNS_9 Die externe GNSS-Ausrüstung muss folgende Komponenten umfassen (siehe Abbildung 4):

a) Einen handelsüblichen GNSS-Empfänger, um die Positionsdaten über die GNSS-Datenschnittstelle bereitzustellen. Die GNSS-Datenschnittstelle kann beispielsweise der Norm NMEA V4.10 entsprechen; der GNSS-Empfänger dient dann als Sender und überträgt NMEA-Datensätze an den GNSS Secure Transceiver mit einer Frequenz von 1Hz für die zuvor festgelegten NMEA-Datensätze, die mindestens die RMC- und GSA-Datensätze umfassen müssen. Die Implementierung der GNSS-Datenschnittstelle wählt der Hersteller der externen GNSS-Ausrüstung.

b) Eine Sende- und Empfangseinheit (GNSS Secure Transceiver) mit der Fähigkeit zur Unterstützung der Norm ISO/IEC 7816-4:2013 (siehe 4.2.1) zur Kommunikation mit der Fahrzeugeinheit und zur Unterstützung der GNSS-Datenschnittstelle zum GNSS-Empfänger. Die Einheit muss über einen Speicher für die Kenndaten des GNSS-Empfängers und der externen GNSS-Ausrüstung verfügen.

c) Ein Gehäusesystem mit Funktion zur Manipulationserkennung, in dem der GNSS-Empfänger und der GNSS Secure Transceiver untergebracht sind. Die Funktion zur Manipulationserkennung muss den Sicherheitsmaßnahmen gemäß dem Schutzprofil des intelligenten Fahrtenschreibers entsprechen.

d) Eine auf dem Fahrzeug angebrachte und durch das Gehäusesystem mit dem GNSS-Empfänger verbundene GNSS-Antenne.

GNS_10 Die externe GNSS-Ausrüstung besitzt mindestens die folgenden externen Schnittstellen:

a) die Schnittstelle zu der auf dem Fahrzeug angebrachten GNSS-Antenne, falls eine externe Antenne verwendet wird.

b) die Schnittstelle zur Fahrzeugeinheit.

GNS_11 In der VU bildet der VU Secure Transceiver das andere Ende der sicheren Kommunikation mit dem GNSS Secure Transceiver und muss ISO/IEC 7816-4:2013 für die Verbindung zur externen GNSS-Ausrüstung unterstützen.

GNS_12 Hinsichtlich der physischen Aspekte der Kommunikation mit der externen GNSS-Ausrüstung muss die Fahrzeugeinheit ISO/IEC 7816-12:2005 oder einen anderen Standard unterstützen, der ISO/IEC 7816-4:2013 unterstützt (siehe 4.2.1).

4.1.2 *Zustand der externen GNSS-Ausrüstung am Ende der Produktion*

GNS_13 Die externe GNSS-Ausrüstung muss ab Werk folgende Werte im nichtflüchtigen Speicher des GNSS Secure Transceivers gespeichert haben:

— das EGF_MA-Schlüsselpaar mit zugehörigem Zertifikat,

— das MSCA_VU-EGF-Zertifikat mit dem öffentlichen MSCA_VU-EGF.PK-Schlüssel zur Verifizierung des EGF_MA-Zertifikats,

— das EUR-Zertifikat mit dem öffentlichen EUR.PK-Schlüssel zur Verifizierung des MSCA_VU-EGF-Zertifikats,

— das EUR-Zertifikat, dessen Gültigkeitsdauer direkt der Gültigkeitsdauer des zur Verifizierung des MSCA_VU-EGF-Zertifikats zu verwendenden EUR-Zertifikats vorausgeht, falls vorhanden,

— das Linkzertifikat, das diese beiden EUR-Zertifikate verbindet, sofern vorhanden,

— die erweiterte Seriennummer der externen GNSS-Ausrüstung,

— die Kennung des Betriebssystems der GNSS-Ausrüstung,

— die Typgenehmigungsnummer der externen GNSS-Ausrüstung,

— den Bezeichner der Sicherheitskomponente des externen GNSS-Moduls.

4.2. **Kommunikation zwischen der externen GNSS-Ausrüstung und der Fahrzeugeinheit**

4.2.1 *Kommunikationsprotokoll*

GNS_14 Das Protokoll der Kommunikation zwischen der externen GNSS-Ausrüstung und der Fahrzeugeinheit muss drei Funktionen unterstützen:

1. das Erfassen und Verteilen von GNSS-Daten (z. B. Standort, Zeit, Geschwindigkeit),
2. das Erfassen der Konfigurationsdaten der externen GNSS-Ausrüstung,
3. das Verwaltungsprotokoll zur Unterstützung der Kopplung, gegenseitigen Authentisierung und Sitzungsschlüsselvereinbarung zwischen der externen GNSS-Ausrüstung und der VU.

GNS_15 Das Kommunikationsprotokoll muss auf der Norm ISO/IEC 7816-4:2013 beruhen, wobei der VU Secure Transceiver den Master und der GNSS Secure Transceiver den Slave bildet. Die physische Verbindung zwischen der externen GNSS-Ausrüstung und der Fahrzeugeinheit basiert auf ISO/IEC 7816-12:2005 oder einem anderen Standard, der ISO/IEC 7816-4:2013 unterstützt.

GNS_16 Im Kommunikationsprotokoll müssen erweiterte Längenfelder nicht unterstützt werden.

GNS_17 Das Kommunikationsprotokoll nach ISO 7816 (sowohl *-4:2013 als auch *-12:2005) zwischen der externen GNSS-Ausrüstung und der VU muss auf T=1 eingestellt sein.

GNS_18 Im Hinblick auf die Funktionen 1) Erfassen und Verteilen von GNSS-Daten, 2) Erfassen der Konfigurationsdaten der externen GNSS-Ausrüstung und 3) Verwaltungsprotokoll muss der GNSS Secure Transceiver eine Chipkarte mit einer Dateisystemarchitektur simulieren, die sich aus einem Wurzelverzeichnis (Master File, MF), einer Verzeichnisdatei (Directory File, DF) mit Anwendungskennung gemäß Spezifikation in Anlage 1 Kapitel 6.2 ('FF 44 54 45 47 4D') und mit 3 EF, die Zertifikate enthalten, sowie aus einer Elementardatei (EF.EGF) mit Dateikennung '2F2F' gemäß Beschreibung in Tabelle 1 zusammensetzt.

GNS_19 Der GNSS Secure Transceiver muss die vom GNSS-Empfänger kommenden Daten und die Konfiguration in der Elementardatei EF.EGF speichern. Es handelt sich hierbei um einen linearen Datensatz von variabler Länge mit der Kennung '2F2F' im Hexadezimalformat.

GNS_20 Der GNSS Secure Transceiver muss für die Speicherung der Daten einen Speicher verwenden, der mindestens 20 Millionen Schreib/Lese-Zyklen durchführen kann. Von diesem Aspekt abgesehen bleiben das Innendesign und die Implementierung des GNSS Secure Transceivers dem Hersteller überlassen.

Das Mapping der Datensatznummern und Daten geht aus Tabelle 1 hervor. Es ist zu beachten, dass es vier GSA-Datensätze für die vier Satellitensysteme und das satellitenbasierte Ergänzungssystem (Satellite-Based Augmentation System, SBAS) gibt.

GNS_21 Die Dateistruktur geht aus Tabelle 1 hervor. Für die Zugriffsbedingungen (ALW, NEV, SM-MAC) siehe Anlage 2 Kapitel 3.5.

Tabelle 1

Dateistruktur

		Zugriffsbedingungen		
Datei	Dateikennung	Lesen	Aktualisieren	Verschlüsselt
MF	3F00			
EF.ICC	0002	ALW	NEV (durch VU)	Nein
DF GNSS-Ausrüstung	0501	ALW	NEV	Nein
EF EGF_MACertificate	C100	ALW	NEV	Nein
EF CA_Certificate	C108	ALW	NEV	Nein
EF Link_Certificate	C109	ALW	NEV	Nein
EF.EGF	2F2F	SM-MAC	NEV (durch VU)	Nein

Datei/Datenelement	Datensatz Nr.	Größe (Bytes)		Standardwerte
		Min.	Max.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS-Ausrüstung		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
RMC NMEA-Datensatz	'01'	85	85	
1. GSA NMEA-Datensatz	'02'	85	85	
2. GSA NMEA-Datensatz	'03'	85	85	

Datei/Datenelement	Datensatz Nr.	Größe (Bytes)		Standardwerte
		Min.	Max.	
3. GSA NMEA-Datensatz	'04'	85	85	
4. GSA NMEA-Datensatz	'05'	85	85	
5. GSA NMEA-Datensatz	'06'	85	85	
Erweiterte Seriennummer der externen GNSS-Ausrüstung gemäß Anlage 1 als SensorGNSSSerialNumber.	'07'	8	8	
Kennung des Betriebssystems des GNSS Secure Transceiver gemäß Anlage 1 als SensorOSIdentifier.	'08'	2	2	
Typgenehmigungsnummer der externen GNSS-Ausrüstung gemäß Anlage 1 als SensorExternalGNSSApprovalNumber.	'09'	16	16	
Kennung der Sicherheitskomponente der externen GNSS-Ausrüstung gemäß Anlage 1 als SensorExternalGNSSSCIdentifier.	'10'	8	8	
RFU Für künftige Anwendungen reserviert	von '11' bis 'FD'			

4.2.2 *Sichere Übertragung von GNSS-Daten*

GNS_22 Die sichere Übertragung von GNSS-Positionsdaten ist nur unter den folgenden Bedingungen zulässig:

1. Der Koppelungsprozess ist gemäß der Beschreibung in Anlage 11, Gemeinsame Sicherheitsmechanismen, abgeschlossen.

2. Die regelmäßige gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung zwischen VU und externer GNSS-Ausrüstung gemäß Anlage 11 ist erfolgt. Die gemeinsamen Sicherheitsmechanismen wurden mit der angegebenen Häufigkeit angewandt.

GNS_23 Alle T Sekunden (wobei T kleiner/gleich 10 ist), sofern nicht eine Koppelung oder gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung erfolgen, fordert die VU von der externen GNSS-Ausrüstung die Positionsdaten auf Grundlage des folgenden Datenflusses an:

1. Die VU fordert von der externen GNSS-Ausrüstung die Standortdaten samt DOP-Daten an (aus dem GSA NMEA-Datensatz). Der VU Secure Transceiver verwendet die Befehle SELECT und READ RECORD(S) gemäß ISO/IEC 7816-4:2013 im Secure Messaging (reiner Authentisierungsmodus), wie in Anlage 11 Abschnitt 11.5 beschrieben, mit der Dateikennung '2F2F' und der Datensatznummer '01' für den RMC NMEA-Datensatz und den Datensatznummern '02', '03', '04', '05' und '06' für den GSA NMEA-Datensatz.

2. Die zuletzt empfangenen Standortdaten werden in der EF mit der Kennung '2F2F' gespeichert und die in Tabelle 1 beschriebenen Datensätze im GNSS Secure Transceiver, wenn der GNSS Secure Transceiver vom GNSS-Empfänger NMEA-Daten mit einer Frequenz von mindestens 1 Hz über die GNSS-Datenschnittstelle erhält.

3. Der GNSS Secure Transceiver sendet die Antwort an den VU Secure Transceiver, indem er die APDU-Antwortnachricht im Secure Messaging (reiner Authentisierungsmodus) verwendet, wie in Anlage 11 Abschnitt 11.5 beschrieben.

4. Der VU Secure Transceiver prüft die Authentizität und Integrität der erhaltenen Antwort. Im Falle eines positiven Ergebnisses werden die Standortdaten über die GNSS-Datenschnittstelle an den VU-Prozessor übertragen.

5. Der VU-Prozessor prüft die empfangenen Daten, indem er die Informationen (z. B. Breite, Länge, Zeit) aus dem RMC NMEA-Datensatz extrahiert. Der RMC NMEA-Datensatz gibt Auskunft darüber, ob die Position gültig ist. Wenn die Position nicht gültig ist, sind die Standortdaten noch nicht verfügbar und können nicht zur Aufzeichnung der Fahrzeugposition verwendet werden. Wenn die Position gültig ist, extrahiert der VU-Prozessor auch die HDOP-Werte aus den GSA NMEA-Datensätzen und berechnet den Mittelwert für das verfügbare Satellitensystem (z. B. wenn die Ortung verfügbar ist).

6. Der VU-Prozessor speichert die empfangenen und verarbeiteten Informationen wie Breite, Länge, Zeit und Geschwindigkeit in der VU, in dem in Anlage 1 (Datenglossar) definierten Format als GeoCoordinates, zusammen mit dem HDOP-Wert, der als kleinster der in den verfügbaren GNSS-Systemen erfassten HDOP-Werte berechnet wurde.

4.2.3 *Struktur des Befehls Read Record*

Dieser Abschnitt beschreibt die Struktur des Befehls Read Record im Einzelnen. Secure Messaging (reiner Authentisierungsmodus) wird gemäß der Beschreibung in Anlage 11 (Gemeinsame Sicherheitsmechanismen) hinzugefügt.

GNS_24 Der Befehl muss das Secure Messaging (reiner Authentisierungsmodus) unterstützen, siehe Anlage 11.

GNS_25 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	'0Ch'	Secure Messaging angefordert.
INS	1	'B2h'	Read Record
P1	1	'XXh'	Datensatznummer ('00' verweist auf den aktuellen Datensatz)
P2	1	'04h'	Lesen des Datensatzes mit der in P1 angegebenen Datensatznummer
Le	1	'XXh'	Erwartete Datenlänge. Anzahl der zu lesenden Bytes.

GNS_26 Der in P1 angegebene Datensatz wird zum aktuellen Datensatz.

Byte	Länge	Wert	Beschreibung
#1-#X	X	'XX..XXh'	Gelesene Daten
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Ist der Befehl erfolgreich, sendet der GNSS Secure Transceiver '**9000**' zurück.

— Wenn die aktuelle Datei nicht datensatzorientiert ist, sendet der GNSS Secure Transceiver '**6981**' zurück.

— Wenn der Befehl mit P1 = '00' verwendet wird, aber keine aktuelle EF vorliegt, sendet der GNSS Secure Transceiver '**6986**' (Befehl nicht zulässig) zurück.

— Wird der Datensatz nicht gefunden, sendet der GNSS Secure Transceiver '**6A 83**' zurück.

— Wenn die externe GNSS-Ausrüstung eine Manipulation erkannt hat, muss sie die Statusbytes '**66 90**' zurücksenden.

GNS_27 Der GNSS Secure Transceiver muss die folgenden, in Anlage 2 spezifizierten Befehle für Fahrtenschreiber der 2. Generation unterstützen:

Befehl	Referenzdokument
Select	Anlage 2 Kapitel 3.5.1
Read Binary	Anlage 2 Kapitel 3.5.2
Get Challenge	Anlage 2 Kapitel 3.5.4
PSO: Verify Certificate	Anlage 2 Kapitel 3.5.7
External Authenticate	Anlage 2 Kapitel 3.5.9
General Authenticate	Anlage 2 Kapitel 3.5.10
MSE:SET	Anlage 2 Kapitel 3.5.11

4.3. **Kopplung, gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung der externen GNSS-Ausrüstung mit der Fahrzeugeinheit**

Kopplung, gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung zwischen externer GNSS-Ausrüstung und Fahrzeugeinheit werden in Anlage 11, Gemeinsame Sicherheitsmechanismen, Kapitel 11, beschrieben.

4.4. **Fehlerbehandlung**

In diesem Abschnitt wird erläutert, wie mögliche Fehlerzustände der externen GNSS-Ausrüstung behandelt und in der VU aufgezeichnet werden.

4.4.1 *Kommunikationsfehler mit der externen GNSS-Ausrüstung*

GNS_28 Kann die VU länger als 20 Minuten durchgehend nicht mit der gekoppelten externen GNSS-Ausrüstung kommunizieren, muss die VU ein Ereignis des Typs EventFaultType mit dem Enum-Wert '53'H *External GNSS communication fault* und mit dem Zeitstempel der aktuellen Zeit aufzeichnen. Das Ereignis wird nur generiert, wenn die folgenden beiden Bedingungen erfüllt sind: a) der intelligente Fahrtenschreiber befindet sich nicht im Kalibrierungsmodus und b) das Fahrzeug bewegt sich. In diesem Kontext wird ein Kommunikationsfehler ausgelöst, wenn der VU Secure Transceiver im Anschluss an eine Anforderungsnachricht gemäß 4.2 keine Antwortnachricht erhält.

4.4.2 *Verletzung der physischen Integrität der externen GNSS-Ausrüstung*.

GNS_29 Wenn bei der externen GNSS-Ausrüstung eine Sicherheitsverletzung stattgefunden hat, muss der GNSS Secure Transceiver seinen gesamten Speicher löschen, einschließlich des kryptografischen Materials. Gemäß GNS_25 und GNS_26 muss die VU einen Eingriff erkennen, wenn die Antwort den Status '6690' aufweist. Die VU generiert dann ein Ereignis des Typs EventFaultType Enum *'55'H Tamper detection of GNSS*.

4.4.3 *Fehlende Positionsdaten des GNSS-Empfängers*

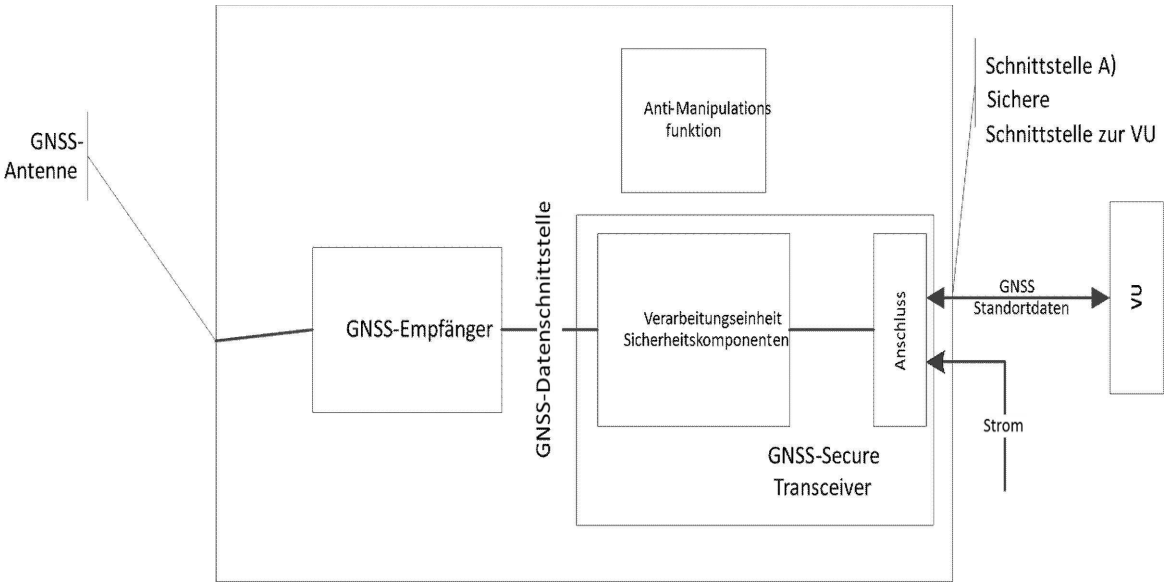
GNS_30 Wenn der GNSS Secure Transceiver länger als 3 Stunden durchgehend keine Daten vom GNSS-Empfänger erhält, generiert der GNSS Secure Transceiver auf den Befehl READ RECORD eine Antwortnachricht mit der RECORD-Nummer '01' und einem Datenfeld von 12 Bytes, die alle auf 0xFF gesetzt sind. Bei Erhalt der Antwortnachricht mit diesem Wert im Datenfeld muss die VU ein Ereignis des Typs EventFaultType Enum '52'H *external GNSS receiver fault* mit einem Zeitstempel des aktuellen Zeitwerts generieren und aufzeichnen, wenn die folgenden beiden Bedingungen erfüllt sind: a) der intelligente Fahrtenschreiber befindet sich nicht im Kalibrierungsmodus und b) das Fahrzeug bewegt sich.

4.4.4 *Abgelaufenes Zertifikat der externen GNSS-Ausrüstung*

GNS_31 Wenn die VU erkennt, dass das EGF-Zertifikat zur gegenseitigen Authentisierung nicht mehr gültig ist, muss die VU einen Kontrollgerätfehler des Typs EventFaultType Enum *'56'H external GNSS facility certificate expired* mit einem Zeitstempel des aktuellen Zeitwerts generieren und aufzeichnen. Die VU verwendet weiterhin die erhaltenen GNSS-Positionsdaten.

Abbildung 4

Schema der externen GNSS-Ausrüstung.



5. FAHRZEUGEINHEIT OHNE EXTERNE GNSS-AUSRÜSTUNG

5.1. Konfiguration

In dieser Konfiguration befindet sich der GNSS-Empfänger innerhalb der Fahrzeugeinheit, wie in Abbildung 1 beschrieben:

GNS_32 Der GNSS-Empfänger dient als Sender und überträgt NMEA-Datensätze an den als Empfänger dienenden VU-Prozessor mit einer Frequenz von mindestens 1/10 Hz für die zuvor festgelegten NMEA-Datensätze, die mindestens die RMC- und GSA-Datensätze umfassen müssen.

GNS_33 Eine auf dem Fahrzeug angebrachte externe GNSS-Antenne oder eine interne GNSS-Antenne muss mit der VU verbunden sein.

5.2. Fehlerbehandlung

5.2.1 *Fehlende Positionsdaten des GNSS-Empfängers*

GNS_34 Erhält die VU mehr als 3 Stunden durchgehend keine Daten vom GNSS-Empfänger muss die VU ein Ereignis des Typs EventFaultType mit einem Enum-Wert '51' H *Internal GNSS receiver fault* und einem Zeitstempel des aktuellen Zeitwerts nur generieren und aufzeichnen, wenn die folgenden beiden Bedingungen erfüllt sind: a) der intelligente Fahrtenschreiber befindet sich nicht im Kalibrierungsmodus und b) das Fahrzeug bewegt sich.

6. GNSS-ZEITKONFLIKT

Stellt die VU eine Abweichung von mehr als 1 Minute zwischen der Zeit der VU-Zeitmessfunktion und der vom GNSS-Empfänger stammenden Zeit fest, muss die VU ein Ereignis des Typs EventFaultType enum *'0B'H Time conflict (GNSS versus VU internal clock)* aufzeichnen. Dieses Ereignis wird zusammen mit dem Wert der Systemuhr der Fahrzeugeinheit aufgezeichnet und geht mit einer automatischen Einstellung der aktuellen Zeit einher. Wenn ein Zeitkonflikt-Ereignis ausgelöst wurde, prüft die VU die Zeitabweichung in den nächsten 12 Stunden nicht. Dieses Ereignis darf nicht ausgelöst werden, wenn der GNSS-Empfänger innerhalb der letzten 30 Tage kein gültiges GNSS-Signal empfangen konnte. Sobald jedoch die Positionsinformation vom GNSS-Empfänger wieder verfügbar ist, muss die automatische Einstellung der aktuellen Zeit erfolgen.

7. DATENKONFLIKT FAHRZEUGBEWEGUNG

GNS_35 Die VU muss einen Datenkonflikt Fahrzeugbewegung (siehe Randnummer 84 in diesem Anhang) mit einem Zeitstempel der aktuellen Zeit auslösen und aufzeichnen, falls die vom Bewegungssensor errechneten Bewegungsdaten von den vom internen GNSS-Empfänger oder der externen GNSS-Ausrüstung errechneten Bewegungsdaten abweicht. Zur Erfassung derartiger Abweichungen wird der Medianwert der Geschwindigkeitsdifferenzen zwischen den verschiedenen Quellen gemäß folgender Erläuterung verwendet:

— Höchstens alle 10 Sekunden wird der Absolutwert der Differenz zwischen der vom GNSS und der vom Bewegungssensor kalkulierten Fahrzeuggeschwindigkeit berechnet.

— Alle in einem die letzten fünf Minuten, in denen Bewegung stattgefunden hat, umfassenden Zeitfenster berechneten Werte werden herangezogen, um den Medianwert zu errechnen.

— Der Medianwert wird als Durchschnitt von 80 % der übrigen Werte berechnet, nachdem die höchsten Absolutwerte ausgeschlossen wurden.

Der Datenkonflikt Fahrzeugbewegung wird ausgelöst, wenn der Medianwert ununterbrochen für fünf Minuten, in denen Bewegung stattfindet, über 10 km/h liegt. Fakultativ können andere unabhängige Quellen für die Ermittlung von Fahrzeugbewegungsdaten herangezogen werden, um eine noch verlässlichere Erkennung der Manipulation des Fahrtenschreibers zu gewährleisten. (Hinweis: Der Medianwert der letzten 5 Minuten wird verwendet, um dem Risiko von Messausreißern und transienter Messwerte mindern.) Dieses Ereignis darf nicht ausgelöst werden, wenn folgende Bedingungen erfüllt sind: a) während einer Fährüberfahrt/Zugfahrt, b) wenn die Positionsinformation vom GNSS-Empfänger nicht verfügbar ist und c) der Kalibrierungsmodus aktiv ist.

Anlage 13

ITS-SCHNITTSTELLE

INHALTSVERZEICHNIS

1. EINLEITUNG 416

2. ANWENDUNGSBEREICH 416

2.1. Akronyme, Definitionen und Notationen 417

3. REFERENZIERTE VERORDNUNGEN UND NORMEN 418

4. FUNKTIONSPRINZIPIEN DER SCHNITTSTELLE 418

4.1. Voraussetzungen für den Datentransfer über die ITS-Schnittstelle 418

4.1.1 Die Daten, die über die ITS-Schnittstelle zur Verfügung gestellt werden 418

4.1.2 Inhalt der Daten 418

4.1.3 ITS-Anwendungen 418

4.2. Kommunikationseinrichtung 419

4.3. PIN-Autorisierung 419

4.4. Nachrichtenformat 421

4.5. Zustimmung des Fahrers 425

4.6. Abrufen allgemeiner Daten 426

4.7. Abrufen persönlicher Daten 426

4.8. Abrufen von Ereignis- und Störungsdaten 426

1. EINLEITUNG

In dieser Anlage werden das Design und die Verfahren spezifiziert, die bei der Umsetzung der Schnittstelle zu intelligenten Verkehrssystemen (ITS), wie in Artikel 10 der Verordnung (EU) Nr. 165/2014 (*die Verordnung*) vorgeschrieben, eingehalten werden müssen.

In der *Verordnung* wird festgelegt, dass Fahrtenschreiber von Fahrzeugen mit genormten Schnittstellen ausgerüstet werden können, die im Betriebsmodus die Nutzung der vom Fahrtenschreiber aufgezeichneten oder erzeugten Daten durch externe Geräte ermöglichen, sofern die folgenden Voraussetzungen erfüllt sind:

(a) Die Schnittstelle beeinträchtigt die Authentizität und Integrität der Daten des Fahrtenschreibers nicht.

(b) Die Schnittstelle entspricht den Einzelvorschriften nach Artikel 11 der Verordnung.

(c) Das an die Schnittstelle angeschlossene externe Gerät kann auf personenbezogene Daten, einschließlich Ortsbestimmungsdaten, nur zugreifen, wenn der Fahrer, auf den sich die Daten beziehen, nachweisbar seine Zustimmung erteilt hat.

2. ANWENDUNGSBEREICH

In dieser Anlage soll festgelegt werden, wie Anwendungen, die auf externen Geräten gehostet werden, mittels Bluetooth®-Verbindung Daten (*die Daten*) von einem Fahrtenschreiber abrufen können.

Die Daten, die über diese Schnittstelle zur Verfügung stehen, sind in Anhang 1 des vorliegenden Dokuments beschrieben. Diese Schnittstelle verbietet es nicht, sonstige Schnittstellen (z. B. per CAN-Bus) zu implementieren, mit denen die Daten der VU auf andere Fahrzeugverarbeitungseinheiten übertragen werden.

In dieser Anlage wird Folgendes festgelegt:

— *Die Daten*, die über die ITS-Schnittstelle zur Verfügung gestellt werden

— Das Bluetooth®-Profil, das für die Datenübertragung genutzt wird

— Die Abfrage- und Downloadverfahren sowie die Sequenz der Operationen

— Den Koppelungsmechanismus zwischen Fahrtenschreiber und externem Gerät

— Den Zustimmungsmechanismus, der dem Fahrer zur Verfügung steht

Folgendes wird in diesem Anhang nicht spezifiziert:

— Erfassung und Verwaltung der *Daten* innerhalb der VU (dies ist an anderer Stelle in *der Verordnung* festgelegt oder ergibt sich aus dem Produktdesign).

— Die Darstellungsform der erfassten Daten gegenüber der auf dem externen Gerät gehosteten Anwendung.

— Datensicherheitsbestimmungen, die über Bluetooth® hinausgehen (wie beispielsweise Verschlüsselung) und den Inhalt *der Daten* betreffen (diese werden an anderer Stelle *der Verordnung* spezifiziert [Anlage 10 Gemeinsame Sicherheitsmechanismen]).

— Die Bluetooth®-Protokolle, die durch die ITS-Schnittstelle genutzt werden

2.1. **Akronyme, Definitionen und Notationen**

Folgende für diese Anlage spezifische Akronyme und Definitionen werden in dieser Anlage verwendet:

Kommunikation	Austausch von Informationen/Daten zwischen einer Haupteinheit (d. h. den Fahrtenschreibern) und einer externen Einheit per Bluetooth® über die ITS-Schnittstelle.
Daten	Datensätze gemäß Anhang 1.
Verordnung	Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr, zur Aufhebung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr und zur Änderung der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr
BR	Basic Rate (Basissatz)
EDR	Enhanced Data Rate (Erhöhte Datenquote)
GNSS	Global Navigation Satellite System (Globales Satellitennavigationssystem)
IRK	Identity Resolution Key (Schlüssel zur Identitätsbestimmung)
ITS	Intelligentes Verkehrssystem (Intelligent Transport System)
LE	Low Energy (Niedrigenergie)
PIN	Personal Identification Number (Persönliche Geheimzahl)
PUC	Personal Unblocking Code (Persönlicher Code zum Entsperren)
SID	Service Identifier (Dienstkennung)
SPP	Serial Port Profile (Profil des seriellen Anschlusses)
SSP	Secure Simple Pairing (Sichere einfache Koppelung)
TRTP	Transfer Request Parameter (Anfrageübertragungsparameter)
TREP	Transfer Response Parameter (Antwortübertragungsparameter)
VU	Fahrzeugeinheit (Vehicle Unit, VU)

3. REFERENZIERTE VERORDNUNGEN UND NORMEN

Die in dieser Anlage definierte Spezifikation verweist auf die folgenden Verordnungen und Normen im Ganzen oder in Teilen und hängt von diesen ab. In den Klauseln dieser Anlage sind die relevanten Normen oder die relevanten Klauseln der Normen angegeben. Bei Widersprüchen haben die Klauseln dieser Anlage Vorrang.

Auf folgende Verordnungen und Normen wird in dieser Anlage Bezug genommen:

— Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr, zur Aufhebung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr und zur Änderung der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr

— Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates vom 15. März 2006 zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr und zur Änderung der Verordnungen (EWG) Nr. 3821/85 und (EG) Nr. 2135/98 des Rates sowie zur Aufhebung der Verordnung (EWG) Nr. 3820/85 des Rates.

— ISO 16844-4: Road vehicles — Tachograph systems — Part 4: Can interface (Straßenfahrzeuge — Fahrtschreiber (Kontrollgeräte) — Teil 4: CAN-Schnittstelle)

— ISO 16844-7: Road vehicles — Tachograph systems — Part 7: Parameters (Straßenfahrzeuge — Fahrtschreiber (Kontrollgeräte) — Teil 7: Parameter).

— Bluetooth® — Serial Port Profile — V1.2

— Bluetooth® — Core Version 4.2

— NMEA 0183 Protokoll V4.1

4. FUNKTIONSPRINZIPIEN DER SCHNITTSTELLE

4.1. **Voraussetzungen für den Datentransfer über die ITS-Schnittstelle**

Die VU ist dafür verantwortlich, die in ihr zu speichernden Daten ohne Einbeziehung der ITS-Schnittstelle zu aktualisieren und auf dem neusten Stand zu halten. Die Mittel, durch die dies erreicht wird, sind VU-intern und werden anderweitig in der Verordnung spezifiziert; diese Anlage enthält keine entsprechende Spezifikation.

4.1.1 *Die Daten, die über die ITS-Schnittstelle zur Verfügung gestellt werden*

Die VU ist dafür verantwortlich, die Daten in regelmäßigen Abständen, die in den VU-Verfahren festgelegt sind, ohne Einbeziehung der ITS-Schnittstelle zu aktualisieren. Die VU-Daten dienen als Grundlage zur Einspeisung und Aktualisierung *der Daten*; die Mittel, durch die dies erreicht wird, werden anderweitig in *der Verordnung* spezifiziert oder, wenn keine entsprechende Spezifikation vorliegt, sind abhängig vom Produktdesign; sie werden nicht in dieser Anlage spezifiziert.

4.1.2 *Inhalt der Daten*

Der Inhalt *der Daten* entspricht den Festlegungen aus Anhang 1 dieser Anlage.

4.1.3 *ITS-Anwendungen*

ITS-Anwendungen nutzen die über die ITS-Schnittstelle bereitgestellten Daten beispielsweise zur Optimierung der Verwaltung der Fahrertätigkeiten unter Einhaltung der Verordnung, zur Feststellung möglicher Störungen des Fahrtenschreibers oder zur Verwendung der GNSS-Daten. Die Spezifikation der Anwendungen fällt nicht in den Aufgabenbereich dieser Anlage.

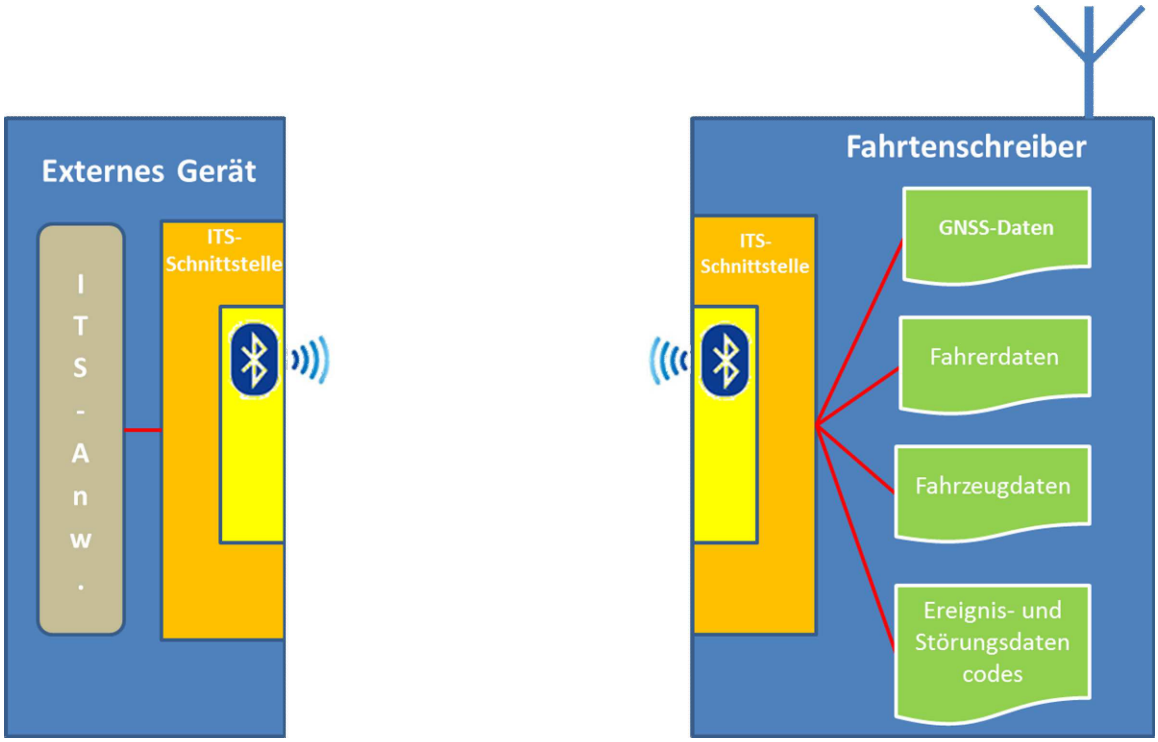
4.2. **Kommunikationseinrichtung**

Der Austausch *der Daten* mittels der ITS-Schnittstelle erfolgt über eine Bluetooth®-Schnittstelle, die mit Version 4.2 oder höher kompatibel ist. Bluetooth® wird im lizenzfreien ISM-Band (Industrial, Scientific and Medical Band) zwischen 2,4 und 2,485 GHz betrieben. Bluetooth® 4.2 bietet verbesserte Datenschutz- und Sicherheitsmechanismen und steigert sowohl Geschwindigkeit als auch Zuverlässigkeit von Datenübertragungen. Für die Zwecke dieser Spezifikation wird ein Bluetooth®-Gerät der Klasse 2 mit einer Reichweite bis zu 10 Metern genutzt. Weitere Informationen zu Bluetooth® 4.2 finden sich unter www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Die *Kommunikation* mit der Kommunikationseinrichtung wird nach Abschluss eines Koppelungsprozesses durch ein autorisiertes Gerät aufgebaut. Da bei Bluetooth® über ein Master/Slave-Modell gesteuert wird, wann und wo Geräte Daten senden können, übernimmt der Fahrtenschreiber die Master-Rolle, während dem externen Gerät die Slave-Rolle zugewiesen wird.

Kommt ein externes Gerät erstmalig in den Sendebereich der VU, kann der Bluetooth®-Koppelungsprozess begonnen werden (siehe auch Anhang 2). Die Geräte tauschen ihre Adressen, Namen, Profile sowie einen gemeinsamen geheimen Schlüssel aus, was es ihnen ermöglicht, sich zukünftig miteinander zu verbinden, wenn sie sich in Reichweite befinden. Nach Abschluss dieses Schritts wird dem externen Gerät vertraut und es kann Datendownloads vom Fahrtenschreiber veranlassen. Es ist nicht vorgesehen, Verschlüsselungsmechanismen zu ergänzen, die über die Funktionen von Bluetooth® hinausreichen. Sollten allerdings zusätzliche Sicherheitsmaßnahmen erforderlich sein, so müssen diese Anlage 10 Gemeinsame Sicherheitsmechanismen entsprechen.

Das typische Kommunikationsprinzip ist in der folgenden Abbildung dargestellt:



Für die Datenübertragung von der VU auf das externe Gerät wird das SPP (Serial Port Profile) von Bluetooth® genutzt.

4.3. **PIN-Autorisierung**

Aus Sicherheitsgründen verlangt die VU ein Autorisierungssystem mittels PIN-Code, das von der Bluetooth-Koppelung getrennt ist. Jede VU muss PIN-Codes mit einer Länge von mindestens 4 Ziffern zur Authentisierung erzeugen können. Jedes Mal, wenn ein externes Gerät eine Koppelung mit der VU vornimmt, muss es den korrekten PIN-Code angeben, bevor es Daten empfängt.

Bei erfolgreicher Eingabe der PIN wird das Gerät auf die Whitelist gesetzt. Die Whitelist muss mindestens 64 mit der gegebenen VU gekoppelte Geräte speichern können.

Wird der PIN-Code dreimal hintereinander falsch eingegeben, wird das Gerät vorübergehend auf die Blacklist gesetzt. Solange es sich auf der Blacklist befindet, wird jeder neue Versuch des Geräts zurückgewiesen. Bei wiederholter dreifacher Fehleingabe des PIN-Codes verlängert sich die Sperrzeit zunehmend (siehe Tabelle 1). Durch die Eingabe des korrekten PIN-Codes werden die Sperrzeit und die Anzahl an Versuchen zurückgesetzt. Abbildung 1 in Anhang 2 zeigt das Ablaufdiagramm eines PIN-Validierungsversuchs.

Tabelle 1

Sperrzeit in Abhängigkeit der Menge der Fehleingaben des PIN-Codes in Folge

Anzahl Fehleingaben in Folge	Sperrzeit
3	30 Sekunden
6	5 Minuten
9	1 Stunde
12	24 Stunden
15	Dauerhaft

Wird der PIN-Code fünfzehnmal hintereinander (5 × 3) falsch eingegeben, wird die ITS-Einheit dauerhaft auf die Blacklist gesetzt. Eine dauerhafte Sperrung kann nur durch Eingabe des korrekten PUC-Codes aufgehoben werden.

Der PUC-Code besteht aus 8 Ziffern und wird zusammen mit der VU durch den Hersteller bereitgestellt. Bei zehnmaliger Fehleingabe des PUC-Codes in Folge wird die ITS-Einheit unwiderruflich auf die Blacklist gesetzt.

Der Hersteller kann es optional ermöglichen, den PIN-Code direkt über die VU zu ändern, der PUC-Code jedoch muss unabänderlich sein. Für die Änderung des PIN-Codes sollte es möglichst erforderlich sein, den aktuellen PIN-Code direkt in der VU einzugeben.

Darüber hinaus müssen alle Geräte in der Whitelist gespeichert bleiben, bis der Benutzer sie manuell entfernt (beispielsweise über die Mensch-Maschine-Schnittstelle der VU oder mit anderen Mitteln). Verlorene oder gestohlene ITS-Einheiten können dabei von der Whitelist entfernt werden. Ebenso müssen alle ITS-Einheiten, die den Bluetooth-Verbindungsbereich für mehr als 24 Stunden verlassen, automatisch aus der Whitelist der VU gelöscht werden und beim nächsten Verbindungsaufbau erneut den korrekten PIN-Code angeben.

Das Format der Nachrichten zwischen der VU-Schnittstelle und der VU ist nicht vorgegeben, sondern kann vom Hersteller festgelegt werden. Letzterer muss allerdings sicherstellen, dass das Nachrichtenformat zwischen der ITS-Einheit und der VU-Schnittstelle eingehalten wird (siehe ASN.1-Spezifikationen).

Bei allen Datenanforderungen müssen die Sicherheitsangaben des Senders vor jeglicher Verarbeitung ordnungsgemäß verifiziert werden. Abbildung 2 von Anhang 2 zeigt das Ablaufdiagramm für dieses Verfahren. Alle Geräte auf der Blacklist müssen automatisch abgelehnt werden; Geräte, die weder auf der Blacklist noch auf der Whitelist verzeichnet sind, müssen eine PIN-Aufforderung erhalten, der das betreffende Gerät entsprechen muss, bevor es die Datenanforderung erneut senden kann.

4.4. **Nachrichtenformat**

Alle zwischen ITS-Gerät und der VU-Schnittstelle ausgetauschten Nachrichten sind mit einer dreiteiligen Struktur formatiert, die sich zusammensetzt aus dem Kopf, bestehend aus einem Zielbyte (TGT), einem Quellbyte (SRC) und einem Längenbyte (LEN),

dem Datenfeld, bestehend aus einem Service-Identifier-Byte (SID) und einer variablen Anzahl von Datenbytes (maximal 255).

Das Prüfsummenbyte ist die 1-Byte-Summenreihe modulo 256 aller Bytes der Nachricht außer CS selbst.

Die Nachricht muss dem Big-Endian-Format entsprechen.

Tabelle 2

Allgemeines Nachrichtenformat

Kopf			Datenfeld					Prüfsumme
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 Bytes			Max. 255 Bytes					1 Byte

Kopf

TGT und SRC: die Kennung der Ziel- (TGT) und Quellgeräte (SRC) der Nachricht. Die Standardkennung der VU-Schnittstelle lautet "EE" und kann nicht geändert werden. Für ihre erste Nachricht des Kommunikationsvorgangs nutzt die ITS-Einheit die Standardkennung "A0". Anschließend weist die VU-Schnittstelle der ITS-Einheit eine eindeutige Kennung zu und setzt die ITS-Einheit für zukünftige Nachrichten im Verlauf des Vorgangs über diese Kennung in Kenntnis.

Das LEN-Byte berücksichtigt nur den „DATA"-Teil des Datenfelds (siehe Tabelle 2), die ersten 4 Bytes sind impliziert.

Die VU-Schnittstelle bestätigt die Authentizität des Senders der Nachricht durch Gegenkontrolle der eigenen IDList anhand der Bluetooth-Daten, indem sie überprüft, ob sich die ITS-Einheit, die unter der angegebenen Kennung eingetragen ist, aktuell innerhalb der Reichweite der Bluetooth-Verbindung befindet.

Datenfeld

Neben der SID enthält das Datenfeld weitere Parameter: einen Anfrageübertragungsparameter (Transfer Request Parameter, TRTP) sowie Zählbytes.

Falls die aufzunehmenden Daten länger sind als der in einer Einzelnachricht zur Verfügung stehende Raum, werden sie in mehrere Teilnachrichten aufgespalten. Jede Teilnachricht weist den gleichen Kopf und die gleiche SID auf, enthält aber einen 2-Byte-Zähler, d. h. Counter Current (CC) und Counter Max (CM), zur Angabe der Teilnachrichtnummer. Damit Fehlerprüfung und Abbruch möglich sind, bestätigt das Empfangsgerät jede Teilnachricht. Das Empfangsgerät kann die Teilnachricht annehmen, ihre erneute Übertragung anfordern sowie das Sendegerät zum Neubeginn oder zum Abbruch der Übertragung auffordern.

Bei Nichtverwendung wird CC und CM der Wert 0xFF zugewiesen.

Beispielsweise wird die nachstehende Nachricht

HEADER	SID	TRTP	CC	CM	DATA	CS
3 Bytes	Länger als 255 Bytes					1 Byte

wie folgt übertragen:

HEADER	SID	TRTP	01	n	DATA	CS
3 Bytes	255 Bytes					1 Byte

HEADER	SID	TRTP	02	n	DATA	CS
3 Bytes	255 Bytes					1 Byte

…

HEADER	SID	TRTP	N	N	DATA	CS
3 Bytes	Max. 255 Bytes					1 Byte

Tabelle 3 enthält die Nachrichten, die die VU und die ITS-Einheit austauschen können sollen. Der Inhalt jedes Parameters ist als Hexadezimalwert angegeben. Zur besseren Übersichtlichkeit sind CC und CM in dieser Tabelle nicht angegeben. Für das vollständige Format siehe oben.

Tabelle 3

Detaillierter Inhalt der Nachricht

Nachricht	Kopf			DATA			Prüf-summe
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Time	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Nachricht	Kopf			DATA			Prüfsumme
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestAccepted	*ITSID*	EE	Len	09	TREP	Daten	
DataUnavailable							
No data available	*ITSID*	EE	02	0A	TREP	10	
Personal data not shared	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
General reject	*ITSID*	EE	02	0B	SID Req	10	
Service not supported	*ITSID*	EE	02	0B	SID Req	11	
Sub function not supported	*ITSID*	EE	02	0B	SID Req	12	
Incorrect message length	*ITSID*	EE	02	0B	SID Req	13	
Conditions not correct or request sequence error	*ITSID*	EE	02	0B	SID Req	22	
Request out of range	*ITSID*	EE	02	0B	SID Req	31	
Response pending	*ITSID*	EE	02	0B	SID Req	78	
ITSID Mismatch	*ITSID*	EE	02	0B	SID Req	FC	
ITSID Not Found	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Diese Nachricht wird durch die VU-Schnittstelle ausgegeben, wenn eine ITS-Einheit, die weder auf der Whitelist noch auf der Blacklist eingetragen ist, eine Datenanforderung sendet.

SendITSID (SID 02)

Diese Nachricht wird durch die VU-Schnittstelle immer dann ausgegeben, wenn ein neues Gerät eine Anforderung sendet. Dieses Gerät verwendet die Standardkennung "A0", bevor ihm für den Kommunikationsvorgang eine eindeutige Kennung zugewiesen wird.

SendPIN (SID 03)

Diese Nachricht wird durch die ITS-Einheit ausgegeben, um durch die VU-Schnittstelle auf die Whitelist gesetzt zu werden. Beim Inhalt dieser Nachricht handelt es sich um einen aus 4 Ganzzahlen zwischen 0 und 9 bestehenden Code.

PairingResult (SID 04)

Diese Nachricht wird durch die VU-Schnittstelle ausgegeben, um die ITS-Einheit darüber in Kenntnis zu setzen, ob der übermittelte PIN-Code korrekt war. Beim Inhalt der Nachricht handelt es sich um eine boolesche Variable mit dem Wert „True", wenn der PIN-Code korrekt war, und andernfalls mit dem Wert „False".

SendPUC (SID 05)

Diese Nachricht wird durch die ITS-Einheit ausgegeben, um von der der Blacklist der VU-Schnittstelle gelöscht zu werden. Beim Inhalt dieser Nachricht handelt es sich um einen aus 8 Ganzzahlen zwischen 0 und 9 bestehenden Code.

BanLiftingResult (SID 06)

Diese Nachricht wird durch die VU-Schnittstelle ausgegeben, um die ITS-Einheit darüber in Kenntnis zu setzen, ob der übermittelte PUC-Code korrekt war. Beim Inhalt der Nachricht handelt es sich um eine boolesche Variable mit dem Wert „True", wenn der PUC-Code korrekt war, und andernfalls mit dem Wert „False".

RequestRejected (SID 07)

Diese Nachricht wird durch die VU-Schnittstelle als Antwort auf alle Nachrichten einer auf der Blacklist befindlichen ITS-Einheit mit Ausnahme von „SendPUC" ausgegeben. In der Nachricht wird angegeben, wie lange die ITS-Einheit noch auf der Blacklist verbleibt; dies geschieht im Sequenzformat „Zeit" gemäß Anhang 3.

RequestData (SID 08)

Diese Nachricht für den Zugriff auf Daten wird durch die ITS-Einheit ausgegeben. Mit dem Byte Transfer Request Parameter (TRTP) wird der benötigte Datentyp angegeben. Es gibt verschiedene Datentypen:

— standardTachData (TRTP 01): als nicht persönlich eingestufte, vom Fahrtenschreiber verfügbare Daten.

— personalTachData (TRTP 02): als persönlich eingestufte, vom Fahrtenschreiber verfügbare Daten.

— gnssData (TRTP 03): GNSS-Daten (immer persönlich).

— standardEventData (TRTP 04): als nicht persönlich eingestufte Daten zu aufgezeichneten Ereignissen.

— personalEventData (TRTP 05): als persönlich eingestufte Daten zu aufgezeichneten Ereignissen.

— standardFaultData (TRTP 06): als nicht persönlich eingestufte Daten zu aufgezeichneten Störungen.

— manufacturerData (TRTP 07): durch den Hersteller zur Verfügung gestellte Daten.

Für weitere Informationen zu den Inhalten jedes Datentyps siehe Anhang 3 dieser Anlage.

Nähere Informationen zum Format und Inhalt der GNSS-Daten entnehmen Sie Anlage 12.

Siehe Anhang IB und IC für weitere Informationen zu Ereignisdatencodes und Störungen.

RequestAccepted (SID 09)

Diese Nachricht wird durch die VU-Schnittstelle ausgegeben, wenn die „RequestData"-Nachricht einer ITS-Einheit akzeptiert wurde. Diese Nachricht beinhaltet einen 1-Byte-TREP, nämlich das TRTP-Byte der zugehörigen RequestData-Nachricht, sowie alle Daten des angeforderten Typs.

DataUnavailable (SID 0A)

Diese Nachricht wird durch die VU-Schnittstelle ausgegeben, wenn aus bestimmten Gründen die angeforderten Daten nicht zur Übermittlung an eine auf der Whitelist befindliche ITS-Einheit verfügbar sind. Diese Nachricht beinhaltet einen 1-Byte-TREP (den TRTP der angeforderten Daten) sowie einen der in Tabelle 3 aufgeführten 1-Byte-Fehlercodes. Folgende Codes stehen zur Verfügung:

— No data available (10): Die VU-Schnittstelle kann aus nicht näher angegebenen Gründen nicht auf die VU-Daten zugreifen.

— Personal data not shared (11): Die ITS-Einheit versucht, persönliche Daten abzurufen, die nicht freigegeben sind.

NegativeAnswer (SID 0B)

Diese Nachrichten werden durch die VU-Schnittstelle ausgegeben, wenn eine Anfrage aus einem anderen Grund als der Nichtverfügbarkeit der Daten nicht erfüllt werden kann. Ursache für diese Art von Nachrichten sind im Allgemeinen — aber nicht immer — fehlerhafte Anfrageformate (Länge, SID, ITSID …). Der TRTP im Datenfeld beinhaltet die SID der Anfrage. Das Datenfeld enthält einen Code zur Identifizierung des Grunds für eine negative Antwort. Folgende Codes stehen zur Verfügung:

— General Reject (Code: 10)

— Die Aktion ist aus einem Grund nicht möglich, der weder unten noch in Abschnitt (Nummer des Abschnitts *DataUnavailable* eintragen) angegeben ist.

— Service not supported (Code: 11)

— Die SID der Anfrage wird nicht verstanden.

— Sub function not supported (Code: 12)

— Der TRTP der Anfrage wird nicht verstanden. Möglicherweise fehlt er oder liegt außerhalb der akzeptierten Werte.

— Incorrect message length (Code: 13)

— Die Länge der erhaltenen Nachricht ist nicht korrekt (Abweichung zwischen dem LEN-Byte und der tatsächlichen Nachrichtenlänge).

— Conditions not correct or request sequence error (Code: 22)

— Der angeforderte Dienst ist nicht aktiv, oder die Reihenfolge der Anforderungsnachrichten ist nicht korrekt.

— Request out of range (Code: 33)

— Der Parameterdatensatz der Anforderung (Datenfeld) ist ungültig.

— Response pending (Code: 78)

— Die angeforderte Aktion kann nicht rechtzeitig abgeschlossen werden, und die VU ist nicht bereit, eine weitere Anforderung anzunehmen.

— *ITSID* Mismatch (Code: FB)

— Die SRC *ITSID* stimmt nach Abgleich mit den Bluetooth-Informationen nicht mit dem zugehörigen Gerät überein.

— *ITSID* Not Found (Code: FC)

— Die SRC *ITSID* ist keinem Gerät zugewiesen.

In den Zeilen 1 bis 72 (**FormatMessageModule**) des ASN.1-Codes in Anhang 3 wird das Nachrichtenformat wie in Tabelle 3 beschrieben spezifiziert. Nähere Angaben zum Nachrichteninhalt werden weiter unten gemacht.

4.5. **Zustimmung des Fahrers**

Alle verfügbaren Daten werden als allgemein oder persönlich klassifiziert. Auf persönliche Daten darf nur zugegriffen werden, wenn das Einverständnis des Fahrers vorliegt, dass die persönlichen Daten des Fahrtenschreibers das Fahrzeugnetzwerk zugunsten von Drittanbieteranwendungen verlassen dürfen.

Die Zustimmung des Fahrers wird beim ersten Einstecken einer bestimmten Fahrer- oder Werkstattkarte gegeben, die der Fahrzeugeinheit zu diesem Zeitpunkt unbekannt ist; hierzu wird der Karteninhaber aufgefordert, der Ausgabe persönlicher Fahrtenschreiberdaten über die optionale ITS-Schnittstelle zuzustimmen (siehe auch Anhang I C Abschnitt 3.6.2).

Der Zustimmungsstatus (aktiviert/deaktiviert) wird im Speicher des Fahrtenschreibers aufgezeichnet.

Bei mehreren Fahrern werden nur die persönlichen Daten derjenigen Fahrer mit der ITS-Schnittstelle ausgetauscht, die hierzu ihre Zustimmung gegeben haben. Gibt es beispielsweise zwei Fahrer für ein Fahrzeug und hat nur einer von ihnen zugestimmt, dass seine persönlichen Daten weitergegeben werden, so werden die persönlichen Daten des anderen Fahrers nicht weitergegeben.

4.6. **Abrufen allgemeiner Daten**

Abbildung 3 von Anhang 2 zeigt die Ablaufdiagramme einer gültigen Anforderung seitens der ITS-Einheit für den Zugriff auf allgemeine Daten. Die ITS-Einheit ist ordnungsgemäß auf der Whitelist eingetragen und fordert keine persönlichen Daten an, weshalb keine weitere Verifizierung erforderlich ist. Die Diagramme setzen voraus, dass das in Abbildung 2 von Anhang 2 dargestellte korrekte Verfahren bereits befolgt wurde. Sie entsprechen dem grauen Kasten *REQUEST TREATMENT* (Verarbeitung anfordern) in Abbildung 2.

Unter den verfügbaren Daten gelten folgende Daten als allgemein:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Abrufen persönlicher Daten**

Abbildung 4 von Anhang 2 zeigt das Ablaufdiagramm die Verarbeitung von Anfragen zu persönlichen Daten. Wie bereits angegeben, übermittelt die VU-Schnittstelle nur dann persönliche Daten, wenn der Fahrer hierzu seine ausdrückliche Zustimmung gegeben hat (siehe auch 4.5). Andernfalls muss die Anforderung automatisch zurückgewiesen werden.

Unter den verfügbaren Daten gelten folgende Daten als persönlich:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Abrufen von Ereignis- und Störungsdaten**

ITS-Einheiten müssen Ereignisdaten anfordern können, die die Liste aller unerwarteten Ereignisse beinhalten. Diese Daten gelten als allgemein oder persönlich, siehe Anhang 3. Der Inhalt jedes Ereignisses entspricht der in Anhang 1 dieser Anlage bereitgestellten Dokumentation.

ANHANG 1

LISTE DER ÜBER DIE ITS-SCHNITTSTELLE VERFÜGBAREN DATEN

Daten	Quelle	Empfohlene Klassifizierung
VehicleIdentificationNumber	Fahrzeugeinheit	**nicht persönlich**
CalibrationDate	Fahrzeugeinheit	**nicht persönlich**
TachographVehicleSpeed speed instant t	Fahrzeugeinheit	persönlich
Driver1WorkingState Selector driver	Fahrzeugeinheit	persönlich
Driver2WorkingState	Fahrzeugeinheit	persönlich
DriveRecognize Speed Threshold detected	Fahrzeugeinheit	**nicht persönlich**
Driver1TimeRelatedStates Weekly day time	Fahrerkarte	persönlich
Driver2TimeRelatedStates	Fahrerkarte	persönlich
DriverCardDriver1	Fahrzeugeinheit	**nicht persönlich**
DriverCardDriver2	Fahrzeugeinheit	**nicht persönlich**
OverSpeed	Fahrzeugeinheit	persönlich
TimeDate	Fahrzeugeinheit	**nicht persönlich**
HighResolutionTotalVehicleDistance	Fahrzeugeinheit	**nicht persönlich**
ServiceComponentIdentification	Fahrzeugeinheit	**nicht persönlich**
ServiceDelayCalendarTimeBased	Fahrzeugeinheit	**nicht persönlich**
Driver1Identification	Fahrerkarte	persönlich
Driver2Identification	Fahrerkarte	persönlich
NextCalibrationDate	Fahrzeugeinheit	**nicht persönlich**
Driver1ContinuousDrivingTime	Fahrerkarte	persönlich
Driver2ContinuousDrivingTime	Fahrerkarte	persönlich
Driver1CumulativeBreakTime	Fahrerkarte	persönlich
Driver2CumulativeBreakTime	Fahrerkarte	persönlich
Driver1CurrentDurationOfSelectedActivity	Fahrerkarte	persönlich
Driver2CurrentDurationOfSelectedActivity	Fahrerkarte	persönlich

Daten	Quelle	Empfohlene Klassifizierung
SpeedAuthorised	Fahrzeugeinheit	**nicht persönlich**
TachographCardSlot1	Fahrerkarte	**nicht persönlich**
TachographCardSlot2	Fahrerkarte	**nicht persönlich**
Driver1Name	Fahrerkarte	persönlich
Driver2Name	Fahrerkarte	persönlich
OutOfScopeCondition	Fahrzeugeinheit	**nicht persönlich**
ModeOfOperation	Fahrzeugeinheit	**nicht persönlich**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Fahrerkarte	persönlich
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Fahrerkarte	persönlich
EngineSpeed	Fahrzeugeinheit	persönlich
RegisteringMemberState	Fahrzeugeinheit	**nicht persönlich**
VehicleRegistrationNumber	Fahrzeugeinheit	**nicht persönlich**
Driver1EndOfLastDailyRestPeriod	Fahrerkarte	persönlich
Driver2EndOfLastDailyRestPeriod	Fahrerkarte	persönlich
Driver1EndOfLastWeeklyRestPeriod	Fahrerkarte	persönlich
Driver2EndOfLastWeeklyRestPeriod	Fahrerkarte	persönlich
Driver1EndOfSecondLastWeeklyRestPeriod	Fahrerkarte	persönlich
Driver2EndOfSecondLastWeeklyRestPeriod	Fahrerkarte	persönlich
Driver1CurrentDailyDrivingTime	Fahrerkarte	persönlich
Driver2CurrentDailyDrivingTime	Fahrerkarte	persönlich
Driver1CurrentWeeklyDrivingTime	Fahrerkarte	persönlich
Driver2CurrentWeeklyDrivingTime	Fahrerkarte	persönlich
Driver1TimeLeftUntilNewDailyRestPeriod	Fahrerkarte	persönlich
Driver2TimeLeftUntilNewDailyRestPeriod	Fahrerkarte	persönlich
Driver1CardExpiryDate	Fahrerkarte	persönlich

Daten	Quelle	Empfohlene Klassifizierung
Driver2CardExpiryDate	Fahrerkarte	persönlich
Driver1CardNextMandatoryDownloadDate	Fahrerkarte	persönlich
Driver2CardNextMandatoryDownloadDate	Fahrerkarte	persönlich
TachographNextMandatoryDownloadDate	Fahrzeugeinheit	**nicht persönlich**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Fahrerkarte	persönlich
Driver2TimeLeftUntilNewWeeklyRestPeriod	Fahrerkarte	persönlich
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Fahrerkarte	persönlich
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Fahrerkarte	persönlich
Driver1CumulativeUninterruptedRestTime	Fahrerkarte	persönlich
Driver2CumulativeUninterruptedRestTime	Fahrerkarte	persönlich
Driver1MinimumDailyRest	Fahrerkarte	persönlich
Driver2MinimumDailyRest	Fahrerkarte	persönlich
Driver1MinimumWeeklyRest	Fahrerkarte	persönlich
Driver2MinimumWeeklyRest	Fahrerkarte	persönlich
Driver1MaximumDailyPeriod	Fahrerkarte	persönlich
Driver2MaximumDailyPeriod	Fahrerkarte	persönlich
Driver1MaximumDailyDrivingTime	Fahrerkarte	persönlich
Driver2MaximumDailyDrivingTime	Fahrerkarte	persönlich
Driver1NumberOfUsedReducedDailyRestPeriods	Fahrerkarte	persönlich
Driver2NumberOfUsedReducedDailyRestPeriods	Fahrerkarte	persönlich
Driver1RemainingCurrentDrivingTime	Fahrerkarte	persönlich
Driver2RemainingCurrentDrivingTime	Fahrerkarte	persönlich
GNSS position	Fahrzeugeinheit	persönlich

2) NACH ZUSTIMMUNG DES FAHRERS VERFÜGBARE UNUNTERBROCHENE GNSS-DATEN

Siehe Anlage 12 — GNSS.

3) OHNE ZUSTIMMUNG DES FAHRERS VERFÜGBARE EREIGNISCODES

Ereignis	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Einstecken einer ungültigen Karte	— die 10 jüngsten Ereignisse.	— Datum und Uhrzeit des Ereignisses, — Kartentyp, Nummer, ausstellender Mitgliedstaat und Generation der Karte, die das Ereignis erstellt hat. — Anzahl ähnlicher Ereignisse an diesem Tag
Kartenkonflikt	— die 10 jüngsten Ereignisse.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Kartentyp, Nummer, ausstellender Mitgliedstaat und Generation der beiden Karten, die den Konflikt verursacht haben.
Letzte nicht korrekt abgeschlossene Kartensitzung	— die 10 jüngsten Ereignisse.	— Datum und Uhrzeit des Einsteckens der Karte — Kartentyp, Nummer, ausgebender Mitgliedstaat und Generation, — letzte von der Karte ausgelesene Vorgangsdaten: — Datum und Uhrzeit des Einsteckens der Karte — amtliches Kennzeichen, Zulassungsmitgliedstaat und VU-Generation.
Unterbrechung der Stromversorgung (2)	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.
Kommunikationsfehler mit der Ausrüstung zur Fernkommunikation	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.
Fehlende Positionsdaten des GNSS-Empfängers	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.
Bewegungsdatenfehler	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.

Ereignis	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Datenkonflikt Fahrzeugbewegung	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.
Versuch Sicherheitsverletzung	die 10 jüngsten Ereignisse je Ereignisart.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes (falls relevant), — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Art des Ereignisses.
Zeitkonflikt	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— aktuelles Datum und Uhrzeit des Aufzeichnungsgeräts, — GNSS-Datum und -Uhrzeit, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.

4) MIT ZUSTIMMUNG DES FAHRERS VERFÜGBARE EREIGNISCODES

Ereignis	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Lenken ohne geeignete Karte	— das längste Ereignis an jedem der letzten 10 Tage des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende des Ereignisses eingesteckten Karte, — Anzahl ähnlicher Ereignisse an diesem Tag.
Einstecken der Karte während des Lenkens	— das letzte Ereignis an jedem der letzten 10 Tage des Auftretens,	— Datum und Uhrzeit des Ereignisses, — Kartentyp, Nummer, ausgebender Mitgliedstaat und Generation, — Anzahl ähnlicher Ereignisse an diesem Tag
Geschwindigkeitsüberschreitung (1)	— das schwerwiegendste Ereignis an jedem der letzten 10 Tage des Auftretens (d. h. das Ereignis mit der höchsten Durchschnittsgeschwindigkeit), — die 5 schwerwiegendsten Ereignisse in den letzten 365 Tagen. — das erste Ereignis nach der letzten Kalibrierung	— Datum und Uhrzeit des Ereignisbeginns, — Datum und Uhrzeit des Ereignisendes, — die während des Ereignisses gemessene Höchstgeschwindigkeit, — die während des Ereignis gemessene arithmetische Durchschnittsgeschwindigkeit, — Kartentyp, Nummer, ausstellender Mitgliedstaat und Generation der Fahrerkarte (falls zutreffend) — Anzahl ähnlicher Ereignisse an diesem Tag.

5) OHNE ZUSTIMMUNG DES FAHRERS VERFÜGBARE STÖRUNGSDATENCODES

Störung	Speicherungsvorschriften	Pro Störung zu speichernde Daten
Kartenstörung	— die 10 jüngsten Fahrerkartenstörungen.	— Datum und Uhrzeit des Störungsbeginns, — Datum und Uhrzeit des Störungsendes, — Kartentyp, Nummer, ausgebender Mitgliedstaat und Generation.
Störungen Kontrollgerät	— die 10 jüngsten Ereignisse für jede Störungsart, — die erste Störung nach der letzten Kalibrierung.	— Datum und Uhrzeit des Störungsbeginns, — Datum und Uhrzeit des Störungsendes, — Art der Störung, — Typ, Nummer, ausstellender Mitgliedstaat und Generation jeder zu Beginn und/oder Ende der Störung eingesteckten Karte.

Diese Störung wird bei folgenden Fehlern ausgelöst, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet:

— Interne Störung VU

— Druckerstörung

— Anzeigestörung

— Störung beim Herunterladen

— Sensorstörung

— Störung des GNSS-Empfängers oder der externen GNSS-Ausrüstung

— Störung der Ausrüstung zur Fernkommunikation

6) HERSTELLERSPEZIFISCHE EREIGNISSE UND STÖRUNGEN OHNE ZUSTIMMUNG DES FAHRERS

Ereignis oder Störung	Speicherungsvorschriften	Pro Ereignis zu speichernde Daten
Durch den Hersteller festzulegen	Durch den Hersteller festzulegen	Durch den Hersteller festzulegen

ANHANG 2

ABLAUFDIAGRAMME FÜR DEN NACHRICHTENAUSTAUSCH MIT DER ITS-EINHEIT.

Abbildung 1

Ablaufdiagramm für PIN-Validierungsversuch

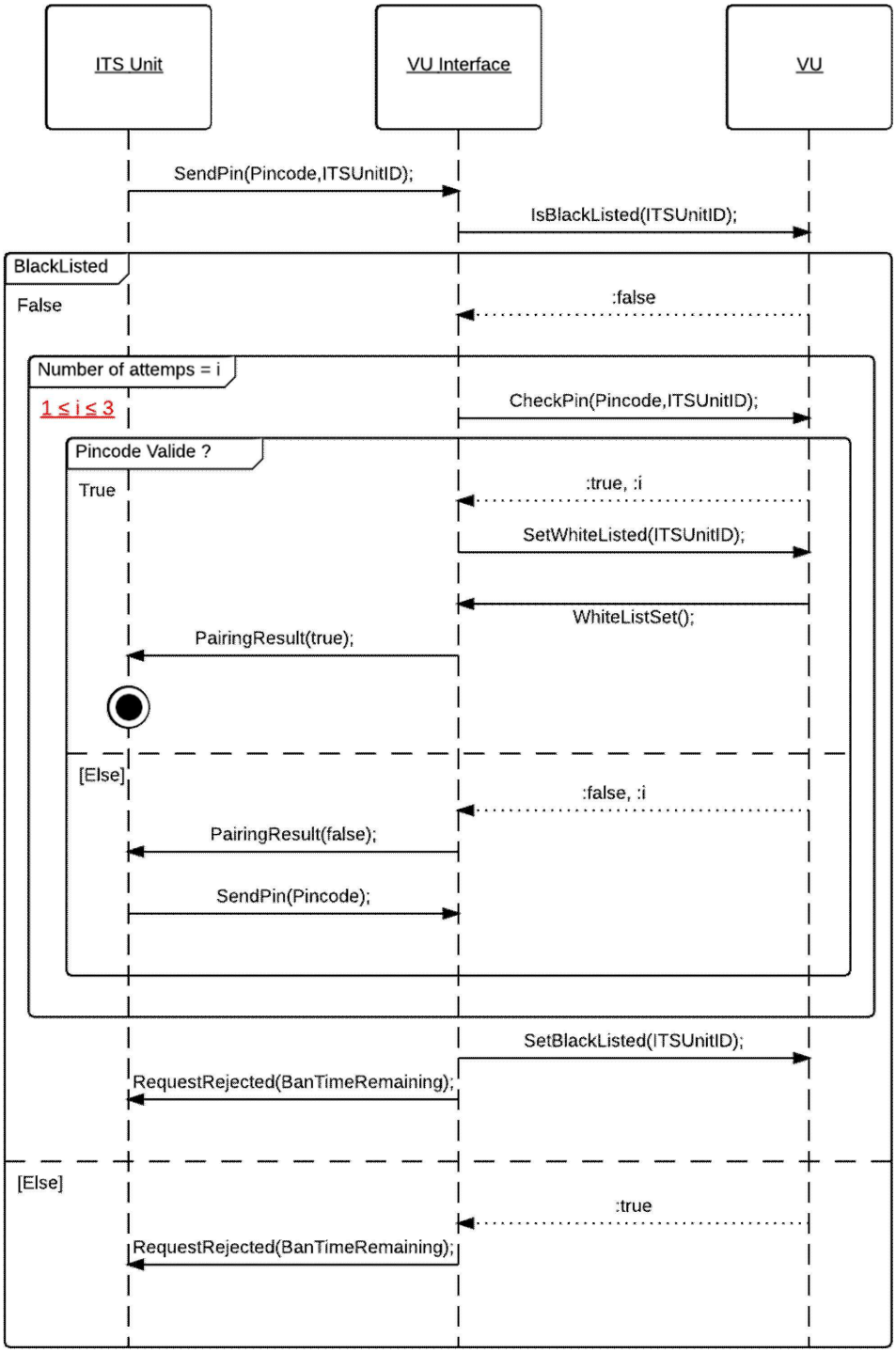


Abbildung 2

Ablaufdiagramm für die Autorisierungsverifizierung der ITS-Einheit

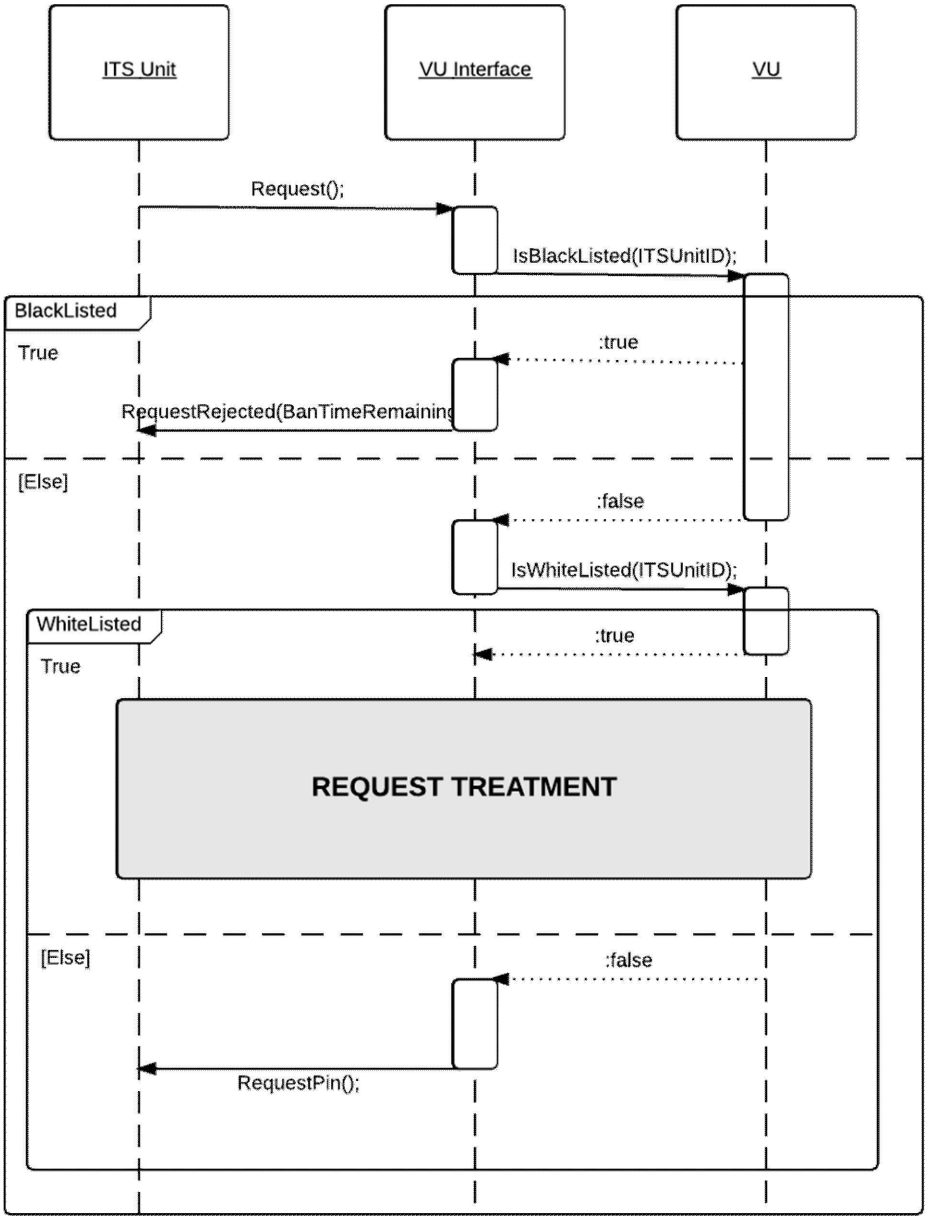


Abbildung 3

Ablaufdiagramm zur Verarbeitung der Anforderung als nicht persönlich klassifizierter Daten (nach korrektem PIN-Zugriff)

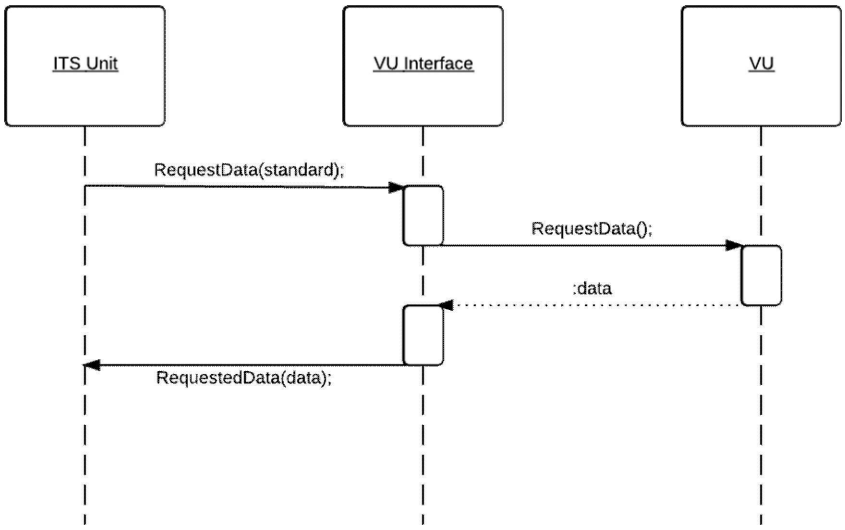


Abbildung 4

Ablaufdiagramm zur Verarbeitung der Anforderung als persönlich klassifizierter Daten (nach korrektem PIN-Zugriff)

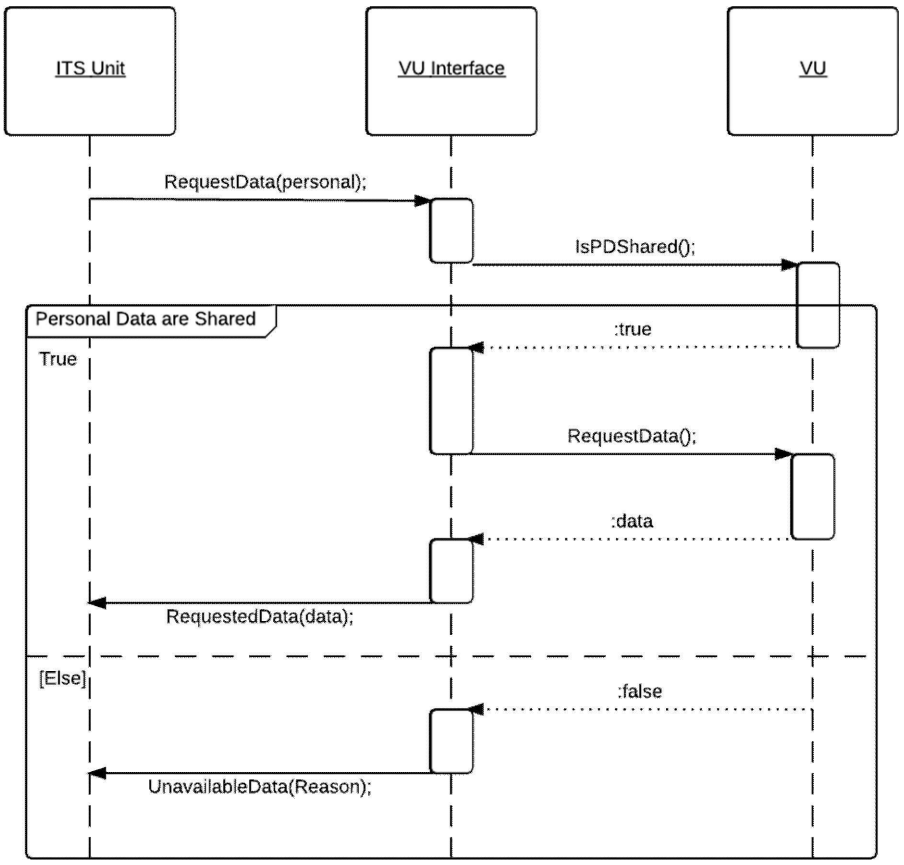
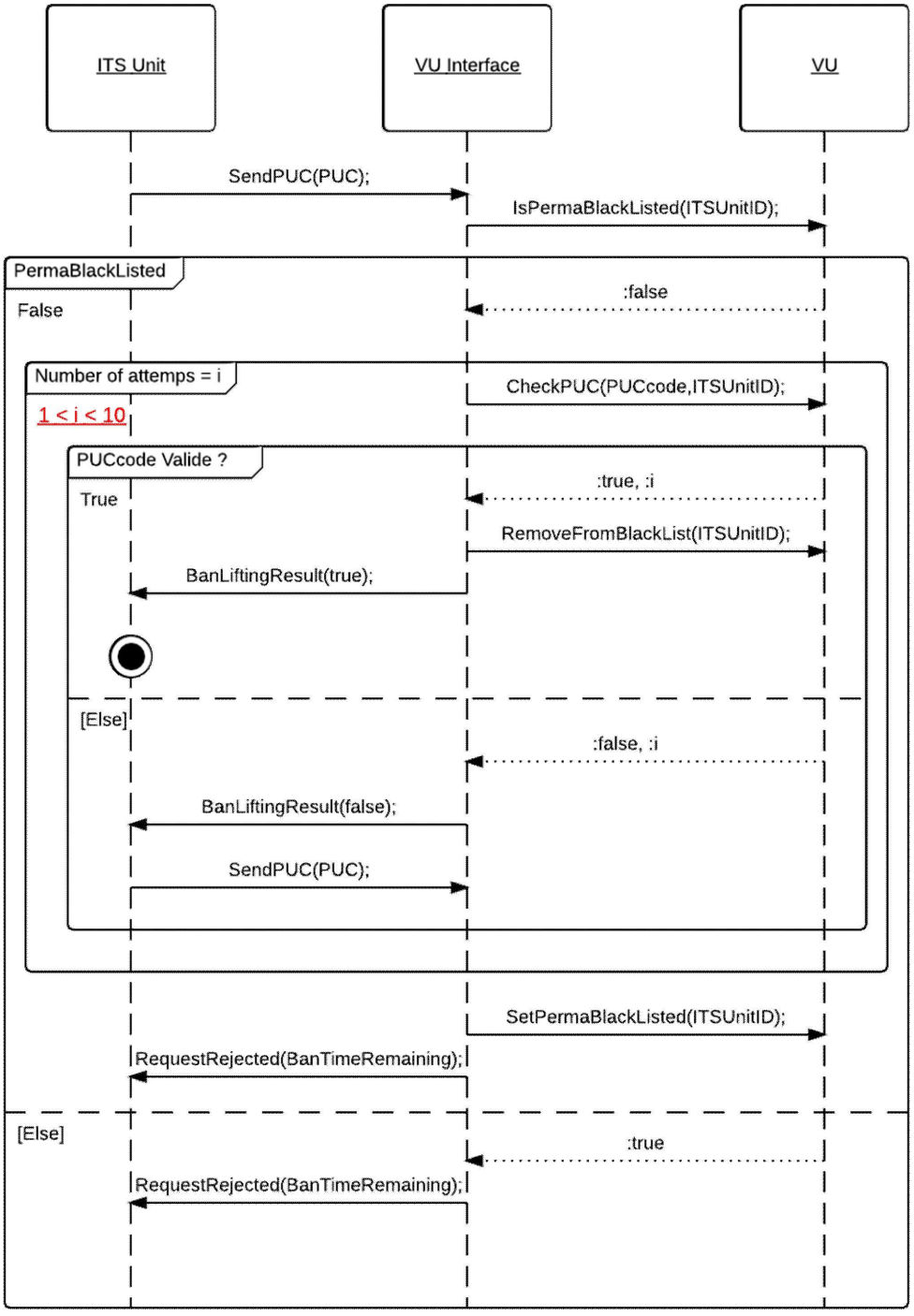


Abbildung 5

Ablaufdiagramm für PUC-Validierungsversuch



ANHANG 3

ASN.1-SPEZIFIKATIONEN

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246           }
247
248           ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252           }
253
254           ---------------
255           --DATA SHEETS--
256           ---------------
257
258           --Data sheet format follows ISO 16844-7.--
259           StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267     5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270     -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278           vehicleRegistrationNumber SEQUENCE {
279                       codePageVRN INTEGER (0..255),
280                       vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284           }
285
286           PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289     UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291     UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294     1002 UNION
295                                                   1012 UNION 1102 UNION 1112 UNION
296     10002 UNION 10012 UNION
297                                                   10102 UNION 10112 UNION 11002 UNION
298     11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300     1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Anlage 14.

FERNKOMMUNIKATIONSFUNKTION

INHALTSVERZEICHNIS

1 EINFÜHRUNG ... 450

2 GELTUNGSBEREICH ... 451

3 AKRONYME, DEFINITIONEN UND NOTATIONEN ... 452

4 BETRIEBSSZENARIOS ... 454

4.1 Überblick ... 454

4.1.1 Voraussetzungen für den Datentransfer über die 5,8-GHz-DSRC-Schnittstelle ... 454

4.1.2 Profil 1a: über eine von Hand ausgerichtete oder vorübergehend an der Straße aufgestellte und ausgerichtete Fernabfragekommunikation ... 455

4.1.3 Profil 1b: über ein in einem Fahrzeug eingerichtetes und ausgerichtetes Fernabfragegerät (REDCR) ... 456

4.2 Sicherheit/Integrität ... 456

5 DESIGN UND PROTOKOLLE DER FERNKOMMUNIKATION ... 456

5.1 Design ... 456

5.2 Ablauf ... 459

5.2.1 Betrieb ... 459

5.2.2 Interpretation der über die DSRC-Kommunikation empfangenen Daten ... 461

5.3 Parameter der physischen DSRC-Schnittstelle zur Fernkommunikation ... 461

5.3.1 Beschränkungen hinsichtlich des Ortes ... 461

5.3.2 Downlink- und Uplinkparameter ... 461

5.3.3 Antennendesign ... 466

5.4 DSRC-Protokollanforderungen für RTM ... 466

5.4.1 Überblick ... 466

5.4.2 Befehle ... 469

5.4.3 Abfragebefehlssequenz ... 469

5.4.4 Datenstrukturen ... 470

5.4.5 Elemente von RtmData, durchgeführte Aktionen und Definitionen ... 472

5.4.6 Mechanismus der Datenübertragung ... 476

5.4.7 Detaillierte Beschreibung der DSRC-Transaktion ... 476

5.4.8 Beschreibung der DSRC-Prüftransaktion ... 486

5.5 Unterstützung für Richtlinie 2015/71/EG des Rates ... 490

5.5.1 Überblick ... 490

5.5.2 Befehle 490
5.5.3 Abfragebefehlssequenz 490
5.5.4 Datenstrukturen 490
5.5.5 ASN.1-Modul für die OWS-DSRC-Transaktion 491
5.5.6 Elemente von OswData, durchgeführte Aktionen und Definitionen 492
5.5.7 Mechanismen der Datenübertragung 492
5.6 Datenübermittelung zwischen DSRC-VU und VU 492
5.6.1 Physische Verbindung und Schnittstellen 492
5.6.2 Anwendungsprotokoll 493
5.7 Fehlerbehandlung 494
5.7.1 Aufzeichnung und Kommunikation der Daten in der DSRC-VU 494
5.7.2 Fehler in der Drahtloskommunikation 494
6 INBETRIEBNAHME- UND REGELMÄSSIGE INSPEKTIONSPRÜFUNGEN DER FERNKOMMUNIKATIONSFUNKTION 496
6.1 Allgemein 496
6.2 ECHO 496
6.3 Prüfungen zur Validierung sicherer Dateninhalte 496

1 EINFÜHRUNG

In dieser Anlage werden das Design und die Verfahren spezifiziert, die bei der Umsetzung der Fernkommunikationsfunktion („Kommunikation") gemäß Artikel 9 der Verordnung (EU) Nr. 165/2014 (die Verordnung) befolgt werden müssen.

DSC_1 In der Verordnung (EU) Nr. 165/2014 ist festgelegt, dass der Fahrtenschreiber mit einer Fernkommunikationsfunktion ausgestattet sein muss, durch die Mitarbeiter der zuständigen Kontrollbehörden Fahrtenschreiberinformationen vorbeifahrender Fahrzeuge mithilfe eines Fernabfragegeräts (Remote Early Detection Communication Reader [REDCR]; Abfragegeräte, die über DSRC-Schnittstellen [Dedicated Short Range Communication] mit CEN 5,8 GHz eine Drahtlosverbindung herstellen) auslesen können.

Hierbei muss betont werden, dass diese Funktion lediglich als Vorfilter dienen soll, um Fahrzeuge zur näheren Prüfung auszuwählen, und nicht das formelle Prüfverfahren gemäß der Verordnung (EU) Nr. 165/2014 ersetzt. Siehe Erwägungsgrund 9 in der Präambel dieser Verordnung, wo dargelegt wird, dass die Fernkommunikation zwischen Fahrtenschreiber und Kontrollbehörden zu Straßenkontrollzwecken die Durchführung gezielter Straßenkontrollen erleichtert.

DSC_2 *Die Daten* sind unter Verwendung *der Kommunikation* auszutauschen; bei dieser handelt es sich um Drahtlosverkehr über eine 5,8-GHz-DSRC-Drahtlosverbindung gemäß der Anlage und geprüft gegen die geeigneten Parameter von EN 300 674-1 (Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s/250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU), Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) — Straßentransport- und Verkehrstelematik (RTTT) — DSRC-Übertragungseinrichtungen (500 kbit/s/250 kbit/s), die im 5,8-GHz-ISM-Band arbeiten — Teil 1: Allgemeine Kennwerte und Prüfverfahren für Road Side Units (RSU) und On-Board Units (OBU)).

DSC_3 *Die Kommunikation* ist ausschließlich dann mit dem Kommunikationsgerät herzustellen, wenn dies von dem Gerät der zuständigen Kontrollbehörde mithilfe zulässiger Funkverbindungsmittel (*Remote Early Detection Communication Reader (REDCR)* angefordert wird.

DSC_4 Die Integrität *der Daten* ist zu schützen.

DSC_5 Der Zugang zu den übertragenen *Daten* ist auf die Kontrollbehörden beschränkt, die ermächtigt sind, Verstöße gegen die Verordnungen (EG) Nr. 561/2006 und (EU) Nr. 165/2014 zu überprüfen, und auf Werkstätten, soweit ein Zugang für die Überprüfung des ordnungsgemäßen Funktionierens des Fahrtenschreibers erforderlich ist.

DSC_6 Bei *der Kommunikation* dürfen nur *Daten* übertragen werden, die für die Zwecke der gezielten Straßenkontrolle von Fahrzeugen notwendig sind, deren Fahrtenschreiber mutmaßlich manipuliert oder missbraucht wurde.

DSC_7 Die Integrität und Sicherheit der Daten ist zu gewährleisten, indem *die Daten* innerhalb der Fahrzeugeinheit (VU) gesichert werden und indem ausschließlich die gesicherten Nutzlastdaten und sicherheitsbezogenen Daten (siehe 5.4.4) über das 5,8-GHz-DSRC-Fernkommunikationsmedium weitergegeben werden, sodass nur befugte Personen zuständiger Kontrollbehörden in der Lage sind, die über *die Kommunikation* weitergegebenen Daten zu verstehen und ihre Authentizität zu überprüfen. Siehe Anlage 11, Gemeinsame Sicherheitsmechanismen.

DSC_8 *Die Daten* müssen einen Zeitstempel mit dem Zeitpunkt der letzten Aktualisierung enthalten.

DSC_9 Der Inhalt der Sicherheitsdaten darf nur den zuständigen Kontrollbehörden und denjenigen Parteien, mit denen sie diese Informationen austauschen, bekannt sein und von diesen kontrolliert werden und liegt außerhalb der Bestimmungen der *Kommunikation*, die Gegenstand dieser Anlage ist, sofern *die Kommunikation* nicht vorsieht, mit jedem Paket an Nutzlastdaten ein Paket an Sicherheitsdaten zu übermitteln.

DSC_10 Die Architektur und Geräte müssen in der Lage sein, mithilfe der hierin angegebenen Architektur andere Datenkonzepte zu verwenden (etwa eingebaute Wiegesysteme).

DSC_11 Zur Klarstellung: Gemäß den Bestimmungen der Verordnung (EU) Nr. 165/2014 (Artikel 7) werden über *die Kommunikation* keine Daten bezüglich der Identität des Fahrers übertragen.

2 GELTUNGSBEREICH

In dieser Anlage wird festgelegt, wie die Mitarbeiter der zuständigen Kontrollbehörden eine angegebene 5,8-GHz-DSRC- Drahtloskommunikation verwenden, um aus der Entfernung Daten (*die Daten*) eines anvisierten Fahrzeugs zu erhalten, die belegen, dass das anvisierten Fahrzeug vermutlich gegen die Verordnung (EU) Nr. 165/2014 verstößt und unter Umständen angehalten werden muss, um weitere Überprüfungen vorzunehmen.

Die Verordnung (EU) Nr. 165/2014 schreibt vor, dass die erfassten Daten sich auf Daten beschränken oder mit solchen im Zusammenhang stehen müssen, die einen möglichen Verstoß eines der Datensubjekte gemäß Definition in Artikel 9 der Verordnung (EU) Nr. 165/2014 belegen.

In einem solchen Szenario ist die für die Kommunikation zur Verfügung stehende Zeit begrenzt, da *die Kommunikation* zielgerichtet ist und innerhalb einer Kurzstrecke erfolgt. Weiterhin können die zur Fahrtenschreiberfernüberwachung (Remote Tachograph Monitoring, RTM) genutzten Daten von den zuständigen Kontrollbehörden auch für andere Anwendungszwecke eingesetzt werden (etwa die höchstzulässigen Gewichte und Abmessungen von Nutzfahrzeugen gemäß der Richtlinie (EU) Nr. 2015/719); diese Maßnahmen können im Ermessen der zuständigen Kontrollbehörden getrennt oder aufeinander folgend durchgeführt werden.

In dieser Anlage wird Folgendes festgelegt:

— die zur *Kommunikation* genutzten Kommunikationsgeräte, -verfahren und -protokolle

— die Normen und Verordnungen, die die Funkgeräte erfüllen müssen

— die Art, wie *die Daten* dem *Kommunikationsgerät* präsentiert werden

— die Abfrage- und Downloadverfahren sowie die Sequenz der Operationen

— die zu übertragenden *Daten*

— die mögliche Auslegung der über *die Kommunikation* übertragenen *Daten*

— die Bestimmungen zu Sicherheitsdaten im Zusammenhang mit der *Kommunikation*

— die Verfügbarkeit der *Daten* für die zuständigen Kontrollbehörden

— die Art und Weise, wie das *Fernabfragegerät* unterschiedliche Datenkonzepte für Fracht und Flotten abfragen kann

Folgendes wird in dieser Anlage nicht festgelegt:

— die Erfassung und Verwaltung *der Daten* innerhalb der VU (diese ergibt sich aus dem Produktdesign, sofern sie nicht an anderer Stelle in der Verordnung (EU) Nr. 165/2014 festgelegt ist).

— die Art der Präsentation der erfassten Daten gegenüber dem Mitarbeiter der zuständigen Kontrollbehörden, ebenso wenig wie die Kriterien, anhand derer die zuständigen Kontrollbehörden entscheiden, welche Fahrzeuge angehalten werden (diese ergeben sich aus dem Produktdesign, sofern sie nicht an anderer Stelle der Verordnung (EU) Nr. 165/2014 oder in einer Grundsatzentscheidung der zuständigen Kontrollbehörden festgelegt werden). Zur Klarstellung: Durch *die Kommunikation* werden den zuständigen Kontrollbehörden lediglich *die Daten* zur Verfügung gestellt, auf deren Grundlage sie fundierte Entscheidungen treffen können.

— Datensicherheitsbestimmungen (wie beispielsweise Verschlüsselung), die den Inhalt *der Daten* betreffen (diese werden in Anlage 11 Gemeinsame Sicherheitsmechanismen spezifiziert).

— Einzelheiten von Datenkonzepten (ausgenommen RTM), die über die gleiche Architektur und Ausrüstung erhalten werden können

— Details über das Verhalten und Management zwischen VU und DSRC-VU, ebenso wenig wie das Verhalten innerhalb der DSRC-VU (außer zum Bereitstellen *der Daten* nach Aufforderung durch ein REDCR).

3 AKRONYME, DEFINITIONEN UND NOTATIONEN

Folgende für diese Anlage spezifische Akronyme und Definitionen werden in dieser Anlage verwendet:

Antenne	elektrisches Gerät, das Strom in Funkwellen und umgekehrt umwandelt und zusammen mit einem Funksender oder -empfänger verwendet wird. Im Betrieb versorgt der Funksender das Endgerät der Antenne mit einem elektrischen Strom, der in der Funkfrequenz oszilliert, und die Antenne strahlt die Energie des Stroms als elektromagnetische Wellen (Funkwellen) aus. Beim Empfang fängt eine Antenne einen Teil der Leistung der elektromagnetischen Welle ab, um eine kleine Spannung an ihren Anschlüssen zu erzeugen, die an einen Empfänger angelegt und verstärkt wird.
Kommunikation	Austausch von Informationen/Daten zwischen DSRC-REDCR und DSRC-VU gemäß Abschnitt 5 in Master-Slave-Beziehung, um die Daten zu erhalten.
Daten	gesicherte Daten eines definierten Formats (siehe 5.4.4), die vom *DSRC-REDCR* abgerufen und dem *DSRC-REDCR* per *DSRC-VU* über eine 5,8-GHz-DSRC-Verbindung nach Definition unter Ziffer 5 unten bereitgestellt werden.
Verordnung (EU) Nr. 165/2014	Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr, zur Aufhebung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr und zur Änderung der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr
AID	Application Identifier (Anwendungskennung)
BLE	Bluetooth Low Energy
BST	Beacon Service Table

CIWD	Card insertion while driving (Einstecken der Karte während des Lenkens)
CRC	Cyclic Redundancy Check (zyklische Redundanzprüfung)
DSC (n)	Kennung einer Anforderung an einer bestimmten DSRC-Anlage
DSRC	Dedicated Short Range Communication (Dedizierte Nahbereichskommunikation)
DSRC-REDCR	DSRC — Remote Early Detection Communication Reader
DSRC-VU	DSRC — Vehicle Unit (Fahrzeugeinheit, damit ist die in Anhang 1C beschriebene „Fernabfrageausrüstung“ gemeint)
DWVC	Driving without valid card (Fahren ohne gültige Karte)
EID	Element Identifier (Elementkennung)
LLC	Logical Link Control
LPDU	LLC Protocol Data Unit
OWS	Onboard Weighing System (Eingebautes Wiegesystem)
PDU	Protocol Data Unit (Protokolldateneinheit)
REDCR	Remote Early Detection Communication Reader (Fernabfragegerät, damit ist das in Anhang 1C beschriebene „Fernabfragegerät“ gemeint)
RTM	Remote Tachograph Monitoring (Fahrtenschreiberfernüberwachung)
SM-REDCR	Security Module-Remote Early Detection Communication Reader (Sicherheitsmodul-Fernabfragegerät)
TARV	Telematics Applications for Regulated Vehicles [ISO 15638 series of Standards] (Telematikanwendungen für regulierte Fahrzeuge [ISO-Normenreihe 15638])
VU	Fahrzeugeinheit (Vehicle Unit, VU)
VUPM	Vehicle Unit Payload Memory (Nutzlastspeicher der Fahrzeugeinheit)
VUSM	Vehicle Unit Security Module (Fahrzeugeinheit-Sicherheitsmodul)
VST	Vehicle Service Table (Servicetabelle des Fahrzeugs)
WIM	Weigh in motion (Wiegen unterwegs)
WOB	Weigh on board (Wiegen an Bord)

Die in dieser Anlage definierte Spezifikation verweist auf die folgenden Verordnungen und Normen im Ganzen oder in Teilen und hängt von diesen ab. In den Klauseln dieser Anlage sind die relevanten Normen oder die relevanten Klauseln der Normen angegeben. Bei Widersprüchen haben die Klauseln dieser Anlage Vorrang. Im Falle eines Widerspruchs und sofern in dieser Anlage nicht klar eine Spezifikation angegeben ist, hat der Betrieb gemäß ERC 70-03 (und geprüft anhand der geeigneten Parameter von EN 300 674-1) Vorrang, gefolgt in absteigender Reihenfolge von EN 12795, EN 12253 EN 12834 und EN 13372, 6.2, 6.3, 6,4 und 7.1.

Auf folgende Verordnungen und Normen wird in dieser Anlage Bezug genommen:

[1] Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr, zur Aufhebung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr und zur Änderung der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr

[2] Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates vom 15. März 2006 zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr und zur Änderung der Verordnungen (EWG) Nr. 3821/85 und (EG) Nr. 2135/98 des Rates sowie zur Aufhebung der Verordnung (EWG) Nr. 3820/85 des Rates.

[3] ERC 70-03 CEPT: ECC-Empfehlung 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s/250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU) (Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) — Straßentransport- und Verkehrstelematik (RTTT) — DSRC-Übertragungseinrichtungen (500 kbit/s/250 kbit/s), die im 5,8-GHz-ISM-Band arbeiten — Teil 1: Allgemeine Kennwerte und Prüfverfahren für Road Side Units (RSU) und On-Board Units (OBU)).

[6] EN 12253 Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5.8 GHz (Straßentransport- und Verkehrstelematik — Nahbereichskommunikation — Datenverbindungsschicht — Bitübertragungsschicht für die Frequenz 5,8 GHz) (Straßentransport- und Verkehrstelematik (RTTT) — Nahbereichskommunikation Fahrzeug-Bake (DSRC) — Bitübertragungsschicht für die Frequenz 5,8 GHz).

[7] EN 12795 Road transport and traffic telematics — Dedicated short-range communication — Data link layer: medium access and logical link control (Straßentransport- und Verkehrstelematik — Nahbereichskommunikation — Datenverbindungsschicht — Zugriffsmedium und Verbindungssteuerung).

[8] EN 12834 Road transport and traffic telematics — Dedicated short-range communication — Application layer (Straßentransport- und Verkehrstelematik — Nahbereichskommunikation — Anwendungsschicht).

[9] EN 13372 Road transport and traffic telematics — Dedicated short-range communication — Profiles for RTTT applications (Straßentransport- und Verkehrstelematik — Nahbereichskommunikation — DSRC-Profile für RTTT-Anwendungen).

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication (Elektronische Gebührenerhebung — Anwendungsschnittstelle zur dezidierten Nahbereich-Kommunikation)

4 BETRIEBSSZENARIOS

4.1 **Überblick**

In der Verordnung (EU) Nr. 165/2014 sind spezifische und kontrollierte Szenarios vorgesehen, innerhalb derer *die Kommunikation* zu verwenden ist.

Die unterstützen Szenarios lauten:

„Kommunikationsprofil 1: Straßenkontrolle mithilfe eines drahtlosen Nahbereich-Fernabfragegeräts, die eine physische Straßenkontrolle in Gang setzt (Master–Slave)

Leserprofil 1a: über eine von Hand ausgerichtete oder vorübergehend an der Straße aufgestellte und ausgerichtete Fernabfragekommunikation

Leserprofil 1b: über ein in einem Fahrzeug eingerichtetes und ausgerichtetes Fernabfragegerät".

4.1.1 *Voraussetzungen für den Datentransfer über die 5,8-GHz-DSRC-Schnittstelle*

HINWEIS: Für ein besseres Verständnis des Kontexts der Voraussetzungen siehe Abbildung 14.3 unten.

4.1.1.1 In der VU gespeicherte Daten

DSC_12 Die VU ist dafür verantwortlich, die in ihr zu speichernden Daten ohne Einbeziehung der DSRC-Kommunikationsfunktion alle 60 Sekunden zu aktualisieren und auf dem neuesten Stand zu halten. Die Mittel, mit denen dies erreicht wird, sind eine wesentliche Eigenschaft der VU und nicht in dieser Anlage, sondern in Anhang 1C Abschnitt 3.19 „*Fernkommunikation für gezielte Straßenkontrollen*" der Verordnung (EU) Nr. 165/2014 angegeben.

4.1.1.2 Der DSRC-VU-Ausrüstung bereitgestellte Daten

DSC_13 Die VU ist dafür verantwortlich, die Daten des DSRC-Fahrtenschreibers (*die Daten*) zu aktualisieren, sobald die in der VU gespeicherten Daten aktualisiert werden. Dies erfolgt in dem in 4.1.1.1 (DSC_12) angegebenen Intervall und ohne Beteiligung der DSRC-Kommunikationsfunktion.

DSC_14 Die VU-Daten dienen als Grundlage zur Einspeisung und Aktualisierung *der Daten;* die Mittel, durch die dies erreicht wird, sind in Anhang 1C Abschnitt 3.19 „*Fernkommunikation für gezielte Straßenkontrollen*" der festgelegt oder sind, wenn keine solche Festlegung vorliegt, abhängig vom Produktdesign und werden nicht in dieser Anlage spezifiziert. Zur Konzeption der Verbindung zwischen DSRC-VU-Ausrüstung und VU siehe Abschnitt 5.6.

4.1.1.3 Inhalt der Daten

DSC_15 Inhalt und Format der Daten sind so zu gestalten, dass sie nach Entschlüsselung in Form und Format wie in 5.4.4 dieser Anlage (Datenstrukturen) angegeben strukturiert sind und verfügbar gemacht werden.

4.1.1.4 Präsentation der Daten

DSC_16 *Die Daten*, die gemäß dem in 4.1.1.1 angegebenen Verfahren regelmäßig aktualisiert worden sind, werden vor der Präsentation gegenüber der *DSRC-VU* gesichert und als gesicherter Datenkonzeptwert präsentiert, um in der *DSRC-VU* als aktuelle Version *der Daten* temporär gespeichert zu werden. Diese Daten werden von der *VUSM* an die DSRC-Funktion *VUPM* weitergeleitet. *VUSM* und *VUPM* sind Funktionen und nicht zwangsläufig physische Einheiten. Die Form der physischen Instanziierung, um diese Funktionen zu erfüllen, ist eine Frage des Produktdesigns, sofern sie nicht an anderer Stelle in der Verordnung (EU) Nr. 165/2014 festgelegt ist.

4.1.1.5 Sicherheitsdaten

DSC_17 Sicherheitsdaten (*Sicherheitsdaten*), die die vom *REDCR* benötigten Daten zur Erfüllung seiner Aufgabe, *die Daten* zu entschlüsseln, enthalten, müssen gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen bereitgestellt und als ein Datenkonzeptwert zur vorübergehenden Speicherung in der *DSRC-VU* als aktuelle Version der *Sicherheitsdaten* in der in dieser Anlage Abschnitt 5.4.4 definierten Form präsentiert werden.

4.1.1.6 VUPM-Daten verfügbar zur Übermittlung per DSRC-Schnittstelle

DSC_18 Das Datenkonzept, das jederzeit in der DSRC-Funktion VUPM zur unmittelbaren Übertragung auf Anfrage durch das *REDCR* zur Verfügung stehen muss, ist in Abschnitt 5.4.4 für die vollständigen Spezifikationen des ASN.1-Moduls definiert.

Allgemeiner Überblick über das Kommunikationsprofil 1

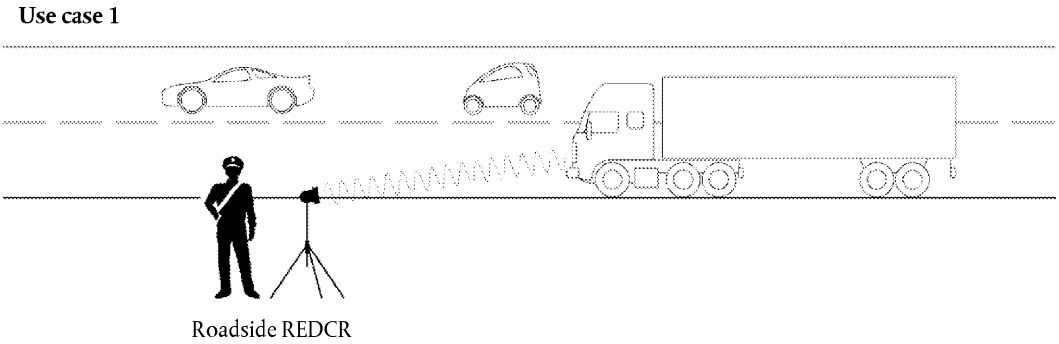
Dieses Profil betrifft den Anwendungsfall, in dem ein Mitarbeiter der zuständigen Kontrollbehörden ein Nahbereich-Fernabfragegerät (5,8-GHz-DSRC-Schnittstellen, betrieben innerhalb von ERC 70-03 und geprüft gegen die geeigneten Parameter von EN 300 674-1 gemäß Abschnitt 5) (*REDCR*), um per Fernkommunikation ein Fahrzeug zu identifizieren, das möglicherweise gegen Verordnung (EU) Nr. 165/2014 verstößt. Nach der Identifizierung entscheidet der Mitarbeiter der zuständigen Kontrollbehörden, der die Abfrage kontrolliert, ob das Fahrzeug angehalten werden soll.

4.1.2 *Profil 1a: über eine von Hand ausgerichtete oder vorübergehend an der Straße aufgestellte und ausgerichtete Fernabfragekommunikation*

In diesem Fall befindet sich der Mitarbeiter der zuständigen Kontrollbehörden am Straßenrand und richtet ein auf einem Stativ befestigtes oder tragbares Handgerät, *REDCR*, vom Straßenrand aus auf die Mitte der Windschutzscheibe des anvisierten Fahrzeugs. Die Abfrage erfolgt mithilfe von 5,8-GHz-DSRC-Schnittstellen, betrieben innerhalb von ERC 70-03 und geprüft gegen die geeigneten Parameter von EN 300 674-1 gemäß Abschnitt 5. Siehe Abbildung 14.1 (Anwendungsfall 1).

Abbildung 14.1

Abfrage am Straßenrand mithilfe von 5,8-GHz-DSRC

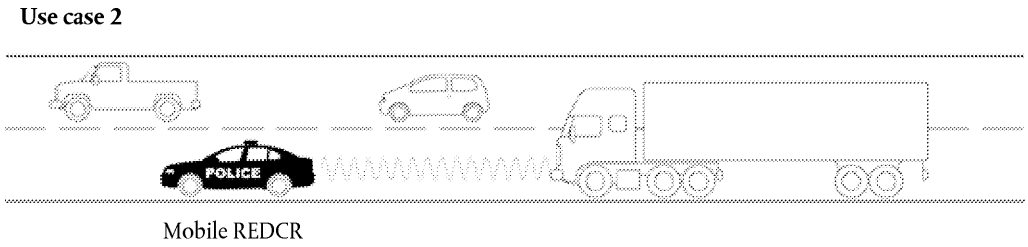


4.1.3 *Profil 1b: über ein in einem Fahrzeug eingerichtetes und ausgerichtetes Fernabfragegerät (REDCR)*

In diesem Fall befindet sich der Mitarbeiter der zuständigen Kontrollbehörden in einem sich bewegenden Fahrzeug und richtet entweder ein *REDCR*-Handgerät aus dem Fahrzeug auf die Mitte der Windschutzscheibe des anvisierten Fahrzeugs, oder *das REDCR* ist in oder auf dem Fahrzeug montiert und zeigt auf die Mitte der Windschutzscheibe des anvisierten Fahrzeugs, wenn sich das Fahrzeug mit dem Fernabfragegerät in einer bestimmten Position zum anvisierten Fahrzeug befindet (zum Beispiel unmittelbar voraus im Verkehrsfluss). Die Abfrage erfolgt mithilfe von 5,8-GHz-DSRC-Schnittstellen, betrieben innerhalb von ERC 70-03 und geprüft gegen die geeigneten Parameter von EN 300 674-1 gemäß Abschnitt 5. Siehe Abbildung 14.2 (Anwendungsfall 2).

Abbildung 14.2

Abfrage aus dem Fahrzeug mithilfe von 5,8-GHz-DSRC (s. o.)



4.2 **Sicherheit/Integrität**

Um die die Authentizität und Integrität der heruntergeladenen Daten per Fernkommunikation überprüfen zu können, werden die gesicherten *Daten* gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen verifiziert und entschlüsselt.

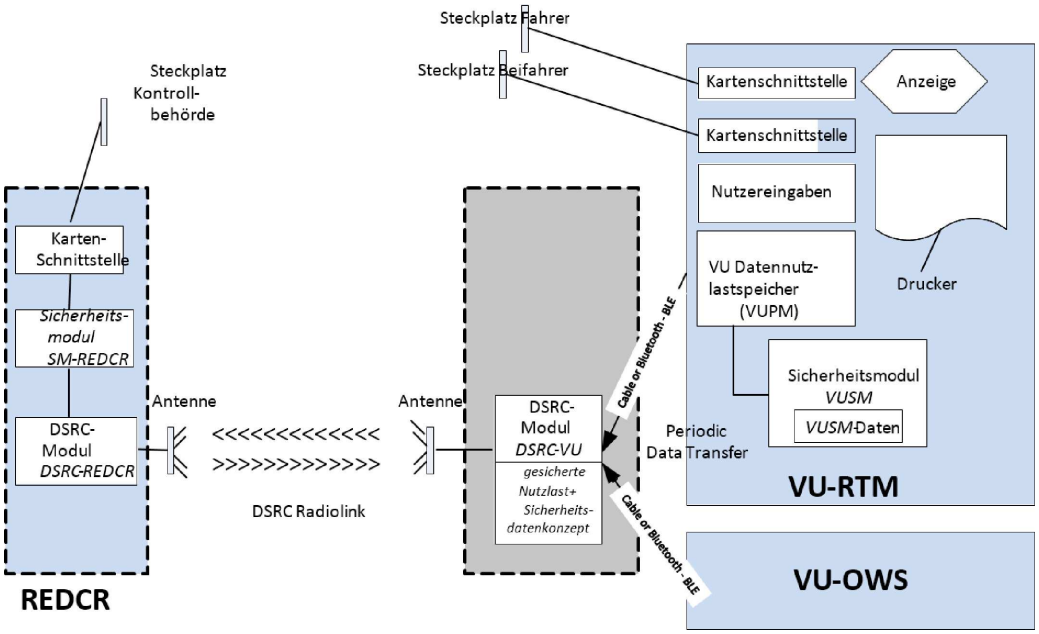
5 DESIGN UND PROTOKOLLE DER FERNKOMMUNIKATION

5.1 **Design**

Das Design der Fernkommunikationsfunktion im intelligenten Fahrtenschreiber ist in Abbildung 14.3 dargestellt.

Abbildung 14.3

Design der Fernkommunikationsfunktion



DSC_19 Die VU enthält die folgenden Funktionen:

— Sicherheitsmodul (*VUSM*). Diese in der VU vorhandene Funktion ist für die Sicherung *der Daten* zuständig, die per Fernkommunikation von der *DSRC-VU* an den Mitarbeiter der zuständigen Kontrollbehörden übermittelt werden sollen.

— Die gesicherten Daten werden im VUSM-Speicher abgelegt. In den in 4.1.1.1 (DSC_12) festgelegten Intervallen verschlüsselt und befüllt die VU das RTMdata-Konzept (welches die weiter unten in dieser Anlage festgelegten Nutzlast- und Sicherheitsdatenkonzeptwerte umfasst) im Speicher der DSRC-VU. Der Betrieb des Sicherheitsmoduls ist in Anlage 11 Gemeinsame Sicherheitsmechanismen definiert und fällt nicht in den Anwendungsbereich dieser Anlage, sofern es nicht dafür benötigt wird, das VU-Kommunikationsgerät jeweils bei einer Änderung der VUSM-Daten zu aktualisieren.

— Die Kommunikation zwischen VU und DSRC-VU kann per drahtgebundener Kommunikation oder per BLE-Kommunikation (Bluetooth Low Energy) erfolgen; die DSRC-VU kann in die Antenne auf der Windschutzscheibe des Fahrzeugs integriert sein, interner Bestandteil der VU sein oder sich irgendwo dazwischen befinden.

— Die DSRC-VU benötigt eine jederzeit verfügbare Stromquelle. Die Art der Stromversorgung kann im Rahmen des Produktdesigns entschieden werden.

— Der Speicher der DSRC-VU muss nichtflüchtig sein, damit die Daten stets in der DSRC-VU verbleiben, selbst wenn die Fahrzeugzündung ausgeschaltet ist.

— Wenn die Kommunikation zwischen VU und DSRC-VU per BLE erfolgt und es sich bei der Stromquelle um eine nicht wieder aufladbare Batterie handelt, muss die Stromquelle der DSRC-VU bei jeder regelmäßigen Nachprüfung ausgetauscht werden; der Hersteller der DSRC-VU-Ausrüstung muss sicherstellen, dass die Stromversorgung den Zeitraum zwischen zwei aufeinanderfolgenden regelmäßigen Nachprüfungen übersteht und in diesem Zeitraum ohne Ausfall oder Unterbrechung einen normalen Zugriff auf die Daten per REDCR gewährleistet

— VU-RTM-„Datennutzlastspeicher“ (*VUPM*). Diese Funktion in der VU ist für die Bereitstellung und Aktualisierung *der Daten* verantwortlich. Der Inhalt *der Daten* („Fahrtenschreibernutzlast“) wird in 5.4.4/5.4.5 unten definiert und in dem in 4.1.1.1 (DSC_12) festgelegten Intervall aktualisiert.

— DSRC-VU. Diese Funktion innerhalb der VU oder mit dieser per Antenne in drahtgebundener oder drahtloser (BLE) Kommunikation stehend speichert die aktuellen Daten (*VUPM-Daten)* und steuert die Antwort auf eine Abfrage über das 5,8-GHz-DSRC-Medium. Eine Trennung der DSRC-Einrichtung oder Störung der Funktion des DSRC-Geräts während des normalen Fahrzeugbetriebs gilt als Verstoß gegen die Verordnung (EU) Nr. 165/2014.

— Das Sicherheitsmodul (REDCR) (*SM-REDCR*) ist die Funktion zur Entschlüsselung und Integritätsprüfung der aus der VU stammenden Daten. Die Mittel, mit denen dies erreicht wird, sind in Anlage 11 Gemeinsame Sicherheitsmechanismen festgelegt und nicht in dieser Anlage definiert.

— Das DSRC-Gerät (REDCR) (*DSRC-REDCR*) beinhaltet einen 5,8-GHz-Sender und dazugehörige Firm- und Software, welche *die Kommunikation* mit der *DSRC-VU* in Überstimmung dieser Anlage gewährleisten.

— Das *DSRC-REDCR* fragt die *DSRC-VU* des anvisierten Fahrzeugs ab, erhält *die Daten* (die aktuellen *VUPM-Daten* des anvisierten Fahrzeugs) per DSRC-Verbindung und speichert diese in seinem *SM-REDCR* ab.

— Die *DSRC-VU*-Antenne muss an einer Stelle angebracht werden, an der sie die DSRC-Kommunikation zwischen dem Fahrzeug und der Antenne am Straßenrand optimiert (im allgemeinen in oder nahe der Mitte der Windschutzscheibe des Fahrzeugs). Bei leichten Fahrzeugen ist eine Anbringung im oberen Teil der Windschutzscheibe geeignet.

— Vor oder in der Nähe der Antenne dürfen sich keine Metallgegenstände (z. B. Namensschilder, Aufkleber, Antireflektionsfolien (Tönungen), Sonnenblenden, Scheibenwischer in Ruheposition) befinden, welche die Kommunikation beeinträchtigen könnten.

— Die Antenne muss so angebracht sein, dass ihre Mittelachse ungefähr parallel zur Straßenoberfläche steht.

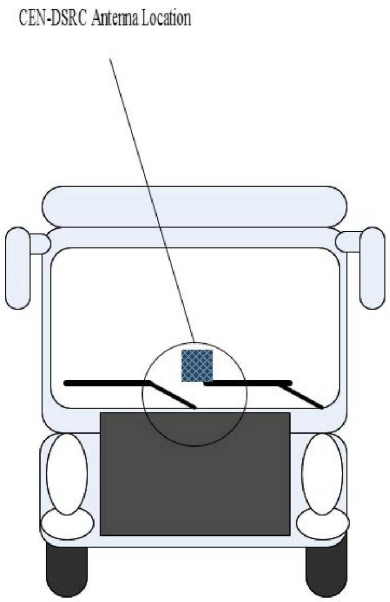
DSC_20 Betrieb der Antenne und der Kommunikation erfolgt innerhalb von ERC 70-03 und geprüft gegen die geeigneten Parameter von EN 300 674-1 gemäß Abschnitt 5. Antenne und Kommunikation können über Verfahren zur Minderung der Risiken von Funkstörungen gemäß ECC-Bericht 228 verfügen, also z. B. mit Filtern in der CEN-DSRC 5,8 GHz-Kommunikation ausgestattet sein,

DSC_21 Die DSRC-Antenne muss mit der DSRC-VU-Ausrüstung entweder direkt in dem an oder in der Nähe der Windschutzscheibe angebrachten Modul oder über ein spezielles Kabel, das durch seine Bauart eine rechtswidrige Trennung erschwert, verbunden sein. Eine Trennung oder Störung der Funktion der Antenne während des normalen Fahrzeugbetriebs gilt als Verstoß gegen die Verordnung (EU) Nr. 165/2014. Ein absichtliches Verbergen oder eine sonstige Beeinträchtigung der Antennenfunktion ist als Verstoß gegen Verordnung (EU) Nr. 165/2014 auszulegen.

DSC_22 Der Formfaktor der Antenne ist nicht definiert und kann betriebswirtschaftlich entschieden werden, solange die angebrachte DSRC-VU die Konformitätsvorgaben in Abschnitt 5 unten erfüllt. Die Antenne soll gemäß den Festlegungen in DSC_19 und der Darstellung in Abbildung 14.4 (Oval) befestigt werden und muss den in 4.1.2 und 4.1.3 beschriebenen Anwendungsfällen effizient gerecht werden.

Abbildung 14.4

Anbringung der 5,8-GHz-DSRC-Antenne an der Windschutzscheibe regulierter Fahrzeuge (HINWEIS: Legende im Bild soll nicht übersetzt werden, Titel der Abbildung ist ausreichend)



Der Formfaktor von *REDCR* und Antenne kann je nach den vom Mitarbeiter der zuständigen Kontrollbehörden gewählten Lese- (Stativbefestigung, Handgerät, Fahrzeugbefestigung usw.) und Betriebsmodi variieren.

Die Ergebnisse der Fernkommunikationsfunktion werden dem Mitarbeiter der zuständigen Kontrollbehörden mittels einer Anzeige- und/oder Benachrichtigungsfunktion präsentiert. Eine Anzeige kann auf einem Bildschirm, als Ausdruck, als Audiosignal oder als Kombination solcher Benachrichtigungen erfolgen. Die Form einer solchen Anzeige und/oder Benachrichtigung hängt von den Anforderungen der Mitarbeiter der zuständigen Kontrollbehörden und dem Gerätedesign ab und ist in dieser Anlage nicht festgelegt.

DSC_23 Design und Formfaktor des *REDCR* ergeben sich aus dem kommerziellen Design innerhalb von ERC 70-03 und den Design- und Leistungsvorgaben in dieser Anlage (Abschnitt 5.3.2), wodurch der Markt über maximale Flexibilität verfügt, um die Ausrüstung nach den besonderen Anforderungen der zuständigen Kontrollbehörden für deren jeweilige Abfrageszenarios zu gestalten und bereitzustellen.

DSC_24 Design und Formfaktor der *DSRC-VU* und deren Positionierung innerhalb oder außerhalb der VU ergeben sich aus dem kommerziellen Design innerhalb der Vorgaben von ERC 70-03 und den in dieser Anlage (Abschnitt 5.3.2) und innerhalb dieses Abschnitts (5.1) angegebenen Design- und Leistungsvorgaben.

DSC_25 Allerdings muss die *DSRC-VU* auf angemessene Weise in der Lage sein, Datenkonzeptwerte anderer intelligenter Fahrzeugausrüstung über eine Verbindung und Protokolle eines offenen Branchenstandards zu akzeptieren (zum Beispiel von Geräten zum Wiegen an Bord), solange solche Datenkonzepte durch eindeutige und bekannte Anwendungskennungen/Dateinamen identifiziert sind und die Anweisungen zum Betrieb solcher Protokolle der Europäischen Kommission zur Verfügung gestellt werden und den Herstellern der relevanten Ausrüstung ohne Kosten verfügbar gemacht werden.

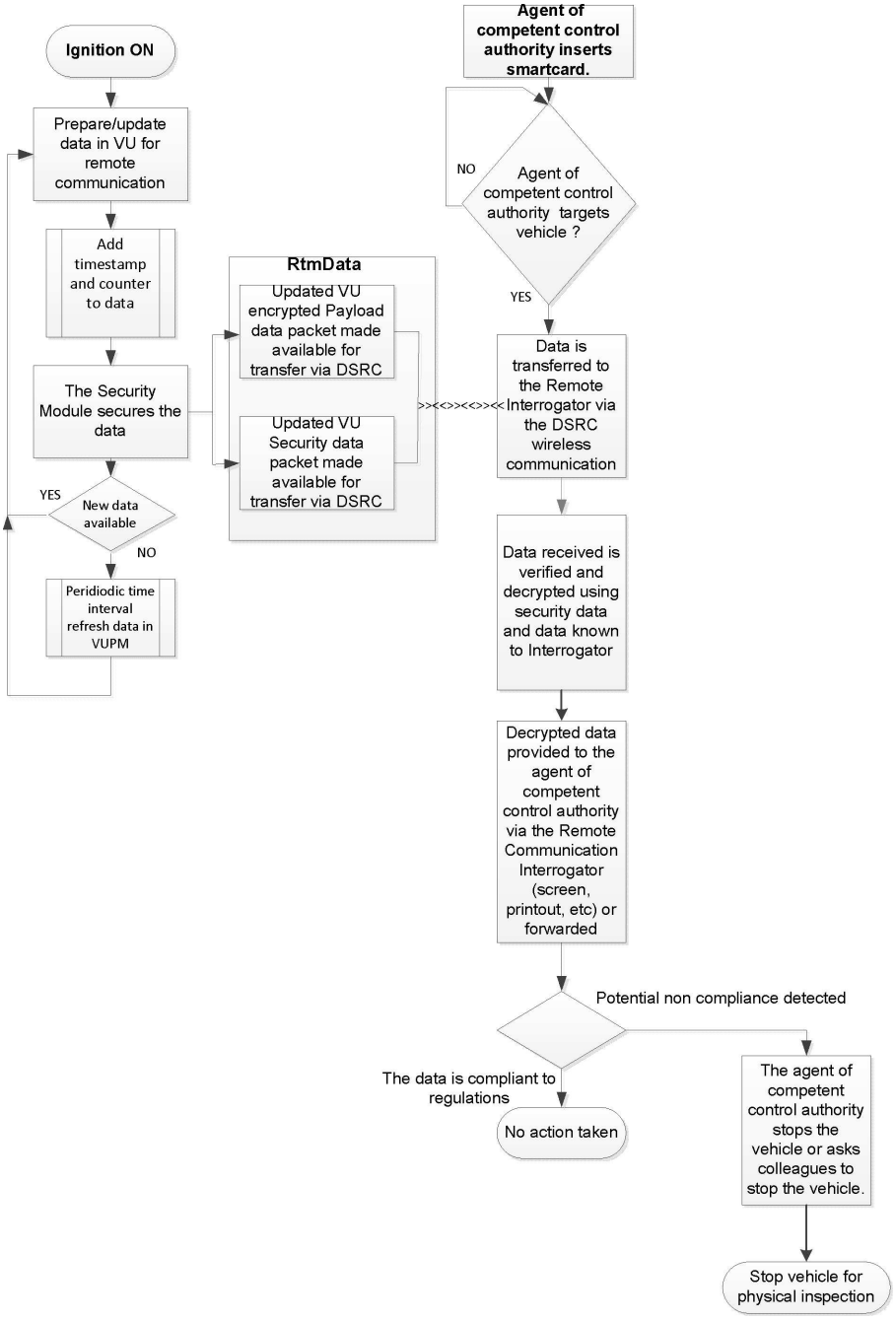
5.2 **Ablauf**

5.2.1 *Betrieb*

Der Betriebsablauf ist in Abbildung 14.5 dargestellt. (HINWEIS: Soll nicht übersetzt werden)

Abbildung 14.5

Ablauf der Fernkommunikationsfunktion



Die Schritte werden im Folgenden beschrieben:

a. Immer, wenn sich das Fahrzeug in Betrieb befindet (Zündung eingeschaltet), stellt der Fahrtenschreiber der VU-Funktion Daten bereit. Die VU-Funktion bereitet *die Daten* für die Fernkommunikationsfunktion (verschlüsselt) vor und aktualisiert die *VUPM* im Speicher der *DSRC-VU* (gemäß Definition in 4.1.1.1 — 4.1.1.2). Die erfassten *Daten* sind wie in 5.4.4 bis 5.4.5 unten dargelegt zu formatieren.

b. Jedes Mal, wenn *die Daten* aktualisiert werden, ist auch der im Sicherheitsdatenkonzept definierte Zeitstempel zu aktualisieren.

c. Die *VUSM*-Funktion sichert die Daten gemäß den in Anlage 11 angegebenen Verfahren.

d. Jedes Mal, wenn *die Daten* aktualisiert werden (siehe 4.1.1.1 bis 4.1.1.2), werden *die Daten* an die *DSRC-VU* übermittelt, wo sie alle vorherigen Daten ersetzen, damit die aktualisierten Daten (*die Daten)* immer zur Verfügung stehen, um bei einer Abfrage durch ein *REDCR* bereitgestellt zu werden. Wenn sie von der VU der DSRC-VU bereitgestellt werden, müssen *die Daten* anhand des Dateinamens *RTMData* oder Anwendungs-ID und Attributskennung zu identifizieren sein.

e. Wenn ein Mitarbeiter der zuständigen Kontrollbehörden ein Fahrzeug anvisieren und von diesem *die Daten* erfassen möchte, muss der Mitarbeiter der zuständigen Kontrollbehörden zuerst seine Chipkarte in *das REDCR* einsetzen, um die *Kommunikation* zu ermöglichen und dem *SM-REDCR* zu ermöglichen, die Authentizität zu überprüfen und die Daten zu entschlüsseln.

f. Anschließend visiert der Mitarbeiter der zuständigen Kontrollbehörde ein Fahrzeug an und fordert per Fernkommunikation die Daten an. *Das REDCR* eröffnet mit dem *DSRC-VU* des anvisierten Fahrzeugs eine 5,8-GHz-DSRC-Schnittstellensitzung und fordert *die Daten* an. *Die Daten* werden über das Drahtloskommunikationssystem als DSRC-Attribut mithilfe des Anwendungsdienstes GET gemäß 5.4 an *das REDCR* übermittelt. Das Attribut enthält die verschlüsselten Nutzdatenwerte und die DSRC-Sicherheitsdaten.

g. Die Daten werden durch das *REDCR*-Gerät analysiert und dem Mitarbeiter der zuständigen Kontrollbehörde bereitgestellt.

h. Der Mitarbeiter der zuständigen Kontrollbehörde nutzt die Daten zur Unterstützung bei der Entscheidung, ob er oder ein anderer Mitarbeiter der zuständigen Kontrollbehörde das Fahrzeug für eine umfangreiche Überprüfung anhalten soll.

5.2.2 *Interpretation der über die DSRC-Kommunikation empfangenen Daten*

DSC_26 Für die über die 5,8-GHz-Schnittstelle empfangenen Daten gelten Bedeutung und Tragweite entsprechend der Definition in 5.4.4 und 5.4.5 unten und auch nur diese Bedeutung und Tragweite sind im Rahmen der hierin definierten Ziele zu verstehen. Gemäß den Bestimmungen der Verordnung (EU) Nr. 165/2014 dürfen *die Daten* nur dazu verwendet werden, einer zuständigen Kontrollbehörde zweckdienliche Informationen zur Hand zu geben, um zu entscheiden, welches Fahrzeug zu einer physischen Überprüfung angehalten werden soll, und müssen anschließend gemäß Artikel 9 der Verordnung (EU) Nr. 165/2014 vernichtet werden.

5.3 Parameter der physischen DSRC-Schnittstelle zur Fernkommunikation

5.3.1 *Beschränkungen hinsichtlich des Ortes*

DSC_27 Die Fernabfrage von Fahrzeugen über eine 5,8-GHz-DSRC-Schnittstelle sollte nicht innerhalb von 200 Metern um eine in Betrieb befindliche 5,8-GHz-DSRC-Brücke erfolgen.

5.3.2 *Downlink- und Uplinkparameter*

DSC_28 Die zur Fahrtenschreiberfernüberwachung verwendete Ausrüstung muss ERC 70-03 und die in den Tabellen 14.1 und 14.2 unten definierten Parameter erfüllen und innerhalb dieser betrieben werden.

DSC_29 Zudem muss die zur Fahrtenschreiberfernüberwachung verwendete Ausrüstung, um Kompatibilität mit den Betriebsparametern anderer standardisierter 5,8-GHz-DSRC-Systeme zu gewährleisten, den Parametern aus EN 12253 und EN 13372 entsprechen.

Namentlich:

Tabelle 14.1

Downlink-Parameter

Punkt	Parameter	Wert(e)	Anmerkung
D1	Downlink-Trägerfrequenzen	Dem REDCR stehen vier Alternativen zur Verfügung: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Innerhalb von ERC 70-03. Die Trägerfrequenzen können vom Implementierer des Straßenrandkontrollsystems ausgewählt werden und brauchen in der DSRC-VU nicht bekannt zu sein. (Konsistent mit EN 12253, EN 13372)
D1a (*)	Toleranz der Träger-frequenzen	innerhalb von ± 5 ppm	(Konsistent mit EN 12253)
D2 (*)	RSU (REDCR)-Sendespektrumsmaske	Innerhalb von ERC 70-03. Das REDCR muss Klasse B,C gemäß EN 12253 entsprechen. Keine anderen spezifischen Anforderungen innerhalb dieses Anhangs	Parameter zur Kontrolle der Interferenz zwischen benachbarten Abfrageeinrichtungen (gemäß EN 12253 und EN 13372).
D3	OBU (DSRC-VU)-Mindestfrequenzbereich	5,795 — 5,815 GHz	(Konsistent mit EN 12253)
D4 (*)	Max. E.I.R.P.	Innerhalb von ERC 70-03 (unlizenziert) und innerhalb der nationalen Vorschriften Max. + 33 dBm	(Konsistent mit EN 12253)
D4a	E.I.R.P.-Winkelmaske	Gemäß der deklarierten und veröffentlichten Spezifikation des Konstrukteurs der Abfrageeinrichtung	(Konsistent mit EN 12253)
D5	Polarisation	Linkszirkular	(Konsistent mit EN 12253)
D5a	Kreuzpolarisation	XPD: In Achsensicht: (REDCR) RSU t ≥ 15 δB (DSRC-VU) OBU r ≥ 10 δB Im Bereich − 3 dB: (REDCR) RSU t ≥ 10 δB (DSRC-VU) OBU r ≥ 6 δB	(Konsistent mit EN 12253)
D6 (*)	Modulation	Zweistufige Amplitudenmodulation	(Konsistent mit EN 12253)
D6a (*)	Modulationsindex	0,5 … 0,9	(Konsistent mit EN 12253)

Punkt	Parameter	Wert(e)	Anmerkung
D6b	Augendiagramm	≥ 90 % (Zeit) / ≥ 85 % (Amplitude)	
D7 (*)	Datenverschlüsselung	FM0 Bit „1“ weist lediglich zu Beginn und Ende des Bit-Intervalls Übergänge auf. Bit „0“ weist gegenüber dem Bit „1“ in der Mitte des Bit-Intervalls einen zusätzlichen Übergang auf.	(Konsistent mit EN 12253)
D8 (*)	Bit-Rate	500 kBit/s	(Konsistent mit EN 12253)
D8a	Toleranz des Bit-Takts	besser als ± 100 ppm	(Konsistent mit EN 12253)
D9 (*)	Bit-Fehlerquote (B.E.R.) zur Kommunikation	≤ 10^{-6} wenn Vorlaufleistung bei OBU (DSRC-VU) in dem durch [D11a bis D11b] vorgegebenen Bereich liegt.	(Konsistent mit EN 12253)
D10	Weckimpuls für OBU (DSRC-VU)	OBU (DSRC-VU) muss beim Empfang von Frames mit 11 oder mehr Oktetten (einschl. Präambel) aufwachen.	Es ist kein spezielles Weckmuster erforderlich. DSRC-VU kam beim Empfang von Frames mit weniger als 11 Oktetten aufwachen. (Konsistent mit EN 12253)
D10a	Maximale Startzeit	≤ 5 ms	(Konsistent mit EN 12253)
D11	Kommunikationsbereich	Raum, in dem eine B.E.R. gemäß D9a erreicht wird	(Konsistent mit EN 12253)
D11a (*)	(Obere) Leistungsgrenze zur Kommunikation.	– 24 dBm	(Konsistent mit EN 12253)
D11b (*)	(Untere) Leistungsgrenze zur Kommunikation.	Vorlaufleistung: – 43 dBm (Mittelachse) – 41 dBm (im Bereich von – 45° bis + 45° entsprechend der Ebene parallel zur Straßenoberfläche, wenn die DSRC-VU später im Fahrzeug installiert wird (Azimuth))	(Konsistent mit EN 12253) Erweiterte Voraussetzungen für waagerechte Winkel bis ± 45° aufgrund der in diesem Anhang definierten Anwendungsfälle.
D12 (*)	IVS-Leistungsgrenzwert (DSRC-VU)	– 60 dBm	(Konsistent mit EN 12253)
D13	Präambel	Präambel vorgeschrieben.	(Konsistent mit EN 12253)
D13a	Präambellänge und -muster	16 Bits ± 1 bit of FM0 coded „1“ bits	(Konsistent mit EN 12253)

Punkt	Parameter	Wert(e)	Anmerkung
D13b	Präambelwellenform	Wechselnde Hoch-/Niedrigsequenz mit einer Impulsdauer von 2 µs. Toleranz gemäß D8a	(Konsistent mit EN 12253)
D13c	Nachlaufende Bits	Die RSU (REDCR) darf nach dem End-Flag maximal 8 Bits übertragen. Zur Berücksichtigung dieser zusätzlichen Bits ist keine OBU (DSRC-VU) erforderlich.	(Konsistent mit EN 12253)

(*) — Downlink-Parameter unterliegen Konformitätsprüfung gemäß relevanter Parameterprüfung aus EN 300 674-1

Tabelle 14.2

Uplink-Parameter

Punkt	Parameter	Wert(e)	Anmerkung
U1 (*)	Unterträgerfrequenzen	Eine OBU (DSRC-VU) unterstützt 1,5 MHz und 2,0 MHz Eine RSU (REDCR) unterstützt 1,5 MHz oder 2,0 MHz oder beides U1-0: 1,5 MHz U1-1: 2,0 MHz	Auswahl der Unterträgerfrequenz (1,5 MHz oder 2,0 MHz) abhängig vom ausgewählten EN-13372-Profil.
U1a (*)	Toleranz der Unterträgerfrequenzen	innerhalb von ± 0,1 %	(Konsistent mit EN 12253)
U1b	Nutzung von Seitenbändern	Gleiche Daten auf beiden Seiten	(Konsistent mit EN 12253)
U2 (*)	OBU (DSRC-VZ)-Sendespektrumsmaske	Gemäß EN 12253 1) Außenbandleistung: siehe ETSI EN 300 674-1 2) Innenbandleistung: [U4a] dBm auf 500 kHz 3) Emission auf beliebigem anderen Uplink- Kanal:U2(3)-1 = – 35 dBm auf 500 kHz	(Konsistent mit EN 12253)
U4a (*)	Max. Einseitenband-E.I. R.P. (Mittelachse)	Zwei Optionen: U4a-0: – 14 dBm U4a-1: – 21 dBm	Gemäß der deklarierten und veröffentlichten Spezifikation des Konstrukteurs der Ausrüstung
U4b (*)	Max. Einseitenband-E.I. R.P. (35°)	Zwei Optionen: — Nicht anwendbar — – 17 dBm	Gemäß der deklarierten und veröffentlichten Spezifikation des Konstrukteurs der Ausrüstung
U5	Polarisation	Linkszirkular	(Konsistent mit EN 12253)

Punkt	Parameter	Wert(e)	Anmerkung
U5a	Kreuzpolarisation	XPD: In Achsensicht: (REDCR) RSU r ≥ 15 δB (DSRC-VU) OBU t ≥ 10 δB Bei -3 dB: (REDCR) RSU r ≥ 10 δB (DSRC-VU) OBU t ≥ 6 δB	(Konsistent mit EN 12253)
U6	Unterträgermodulation	2-PSK Verschlüsselte Daten, mit Unterträger synchronisiert: Übergänge verschlüsselter Daten fallen mit Übergängen des Unterträgers zusammen.	(Konsistent mit EN 12253)
U6b	Arbeitszyklus	Arbeitszyklus: 50 % ± α, α ≤ 5 %	(Konsistent mit EN 12253)
U6c	Modulation auf Träger	Multiplikation von moduliertem Unterträger mit Träger.	(Konsistent mit EN 12253)
U7 (*)	Datenverschlüsselung	NRZI (kein Übergang bei Beginn von „1"-Bit, Übergang bei Beginn von „0"-Bit, kein Übergang innerhalb des Bits)	(Konsistent mit EN 12253)
U8 (*)	Bit-Rate	250 kBit/s	(Konsistent mit EN 12253)
U8a	Toleranz des Bit-Takts	Innerhalb von ± 1 000 ππμ	(Konsistent mit EN 12253)
U9	Bit-Fehlerquote (B.E.R.) für die Kommunikation	$\leq 10^{-6}$	(Konsistent mit EN 12253)
U11	Kommunikationsbereich	Raum, innerhalb dessen sich die DSRC-VU befindet, damit ihre Übertragungen von dem REDCR mit einer B.E.R. von weniger als dem Wert empfangen werden, der durch U9a vorgegeben wird.	(Konsistent mit EN 12253)
U12a (*)	Umwandlungsverstärkung (unterer Grenzwert)	1 dB für jedes Seitenband Winkelbereich: zirkular symmetrisch zwischen Mittelachse und ± 35° sowie	
		im Bereich von – 45° bis + 45° entsprechend der Ebene parallel zur Straßenoberfläche, wenn die DSRC-VU später im Fahrzeug installiert wird (Azimuth)	Größer als der angegebene Wertbereich für waagerechte Winkel bis ± 45° aufgrund der in diesem Anhang definierten Anwendungsfälle.
U12b (*)	Umwandlungsverstärkung (oberer Grenzwert)	10 dB für jedes Seitenband	Kleiner als der angegebene Wertbereich für jedes Seitenband innerhalb eines Kreiskegels um Mittelachse ± mit einem Öffnungswinkel von 45°.
U13	Präambel	Präambel vorgeschrieben.	(Konsistent mit EN 12253)

Punkt	Parameter	Wert(e)	Anmerkung
U13a	Präambel Länge und Muster	32 bis 36 µs lediglich mit Unterträger moduliert, anschließend 8 Bits NRZI-kodierter „0"-Bits.	(Konsistent mit EN 12253)
U13b	Nachlaufende Bits	Die DSRC-VU darf nach dem End-Flag maximal 8 Bits übertragen. Zur Berücksichtigung dieser zusätzlichen Bits ist keine RSU (REDCR) erforderlich.	(Konsistent mit EN 12253)

(*) — Uplink-Parameter unterliegen Konformitätsprüfung gemäß relevanter Parameterprüfung aus EN 300 674-1

5.3.3 *Antennendesign*

5.3.3.1 REDCR-Antenne

DSC_30 Das Design der *REDCR*-Antenne ergibt sich aus dem kommerziellen Design, innerhalb der in 5.3.2 definierten Grenzen und angepasst zur Optimierung der Leseleistung des *DSRC-REDCR* für spezielle Zwecke und Lesebedingungen, innerhalb derer das *REDCR* betrieben wird.

5.3.3.2 VU-Antenne

DSC_31 Das Design der *DSRC_VU*-Antenne ergibt sich aus dem kommerziellen Design, innerhalb der in 5.3.2 definierten Grenzen und angepasst zur Optimierung der Leseleistung des *DSRC-REDCR* für spezielle Zwecke und Lesebedingungen, innerhalb derer das *REDCR* betrieben wird.

DSC_32 Die VU-Antenne ist an oder in der Frontscheibe des Fahrzeugs gemäß 5.1 oben zu befestigen.

DSC_33 In der Prüfumgebung in einer Werkstatt (siehe Abschnitt 6.3) muss eine gemäß 5.1 oben angebrachte DSRC-VU-Antenne erfolgreich eine Verbindung mit einer standardmäßigen Prüfkommunikation herstellen und eine RTM-Transaktion gemäß dieser Anlage über eine Entfernung von 2–10 Metern, in mehr als 99 % der Fälle, gemittelt über 1 000 Leseabfragen bereitstellen.

5.4 **DSRC-Protokollanforderungen für RTM**

5.4.1 *Überblick*

DSC_34 Das Transaktionsprotokoll zum Herunterladen *der Daten* über die 5,8-GHz-DSRC-Schnittstellenverbindung muss folgende Schritte unterstützen. Dieser Abschnitt beschreibt den Transaktionsablauf unter Idealbedingungen ohne Rücktransaktionen oder Kommunikationsunterbrechungen.

HINWEIS Zweck der Initialisierungsphase (Schritt 1) ist es, die Kommunikation zwischen *REDCR* und denjenigen DSRC-VU, die in den 5,8-GHz-DSRC (Master-Slave)-Transaktionsbereich eingetreten sind, aber noch keine Kommunikation mit dem *REDCR* hergestellt haben, einzurichten und die Anwendungsprozesse zu informieren.

— **Schritt 1** Initialisieren. Das *REDCR* sendet einen Frame mit einer „Beacon Service Table" (BST) samt unterstützter Anwendungskennungen (AID) in der Dienstliste. In der RTM-Anwendung ist dies einfach der Dienst mit AID-Wert = 2 (Freight&Fleet). Die *DSRC-VU* wertet die empfangene BST aus und antwortet (siehe unten) mit der Liste unterstützter Anwendungen in der Domäne Freight&Fleet; wenn keine Anwendungen unterstützt werden, antwortet sie nicht. Wenn das *REDCR* nicht AID=2 anbietet, soll die DSRC-VU dem REDCR nicht antworten.

— **Schritt 2** Die *DSRC-VU* sendet einen Frame mit einer Anfrage nach Zuweisung eines privaten Fensters.

— **Schritt 3** Die *REDCR* sendet einen Frame mit Zuweisung eines privaten Fensters.

— **Schritt 4** Die *DSRC-VU* sendet mithilfe des zugewiesenen privaten Fensters einen Frame mit ihrer Fahrzeugdiensttabelle (Vehicle Service Table, VST). Diese VST enthält eine Liste aller unterschiedlichen Anwendungsinstanziierungen, die diese *DSRC-VU* im Rahmen von AID=2 unterstützt. Die verschiedenen Instanziierungen sind durch einzeln generierte EID zu identifizieren, von denen jede mit einem Anwendungskontextmarkierung-Parameterwert verbunden ist, der die Anwendung und die unterstützte Norm angibt.

— **Schritt 5** Anschließend analysiert das *REDCR* die angebotene VST und beendet entweder die Verbindung (RELEASE), da das Angebot der VST nicht interessant ist (d. h., es erhält von der *DSRC-VU* eine VST, die die RTM-Transaktion nicht unterstützt), oder es erhält eine passende VST und startet die Instanziierung der App.

— **Schritt 6** Dazu sendet das REDCR einen Frame mit einem Befehl zum Abruf der RTM-Daten, in dem die RTM-Anwendung durch Angabe der Kennung zur Instanziierung der RTM-Anwendung (wie von der DSRC-VU in der VST angegeben) und soll ein privates Fenster zuweisen.

— **Schritt 7** Die *DSRC-VU* sendet mit dem neu zugewiesenen privaten Fenster einen Frame, der die in der VST genannte adressierte Kennung zur Instanziierung der RTM-Anwendung gefolgt von dem Attribut *RtmData* (Nutzlast- + Sicherheitselement) enthält.

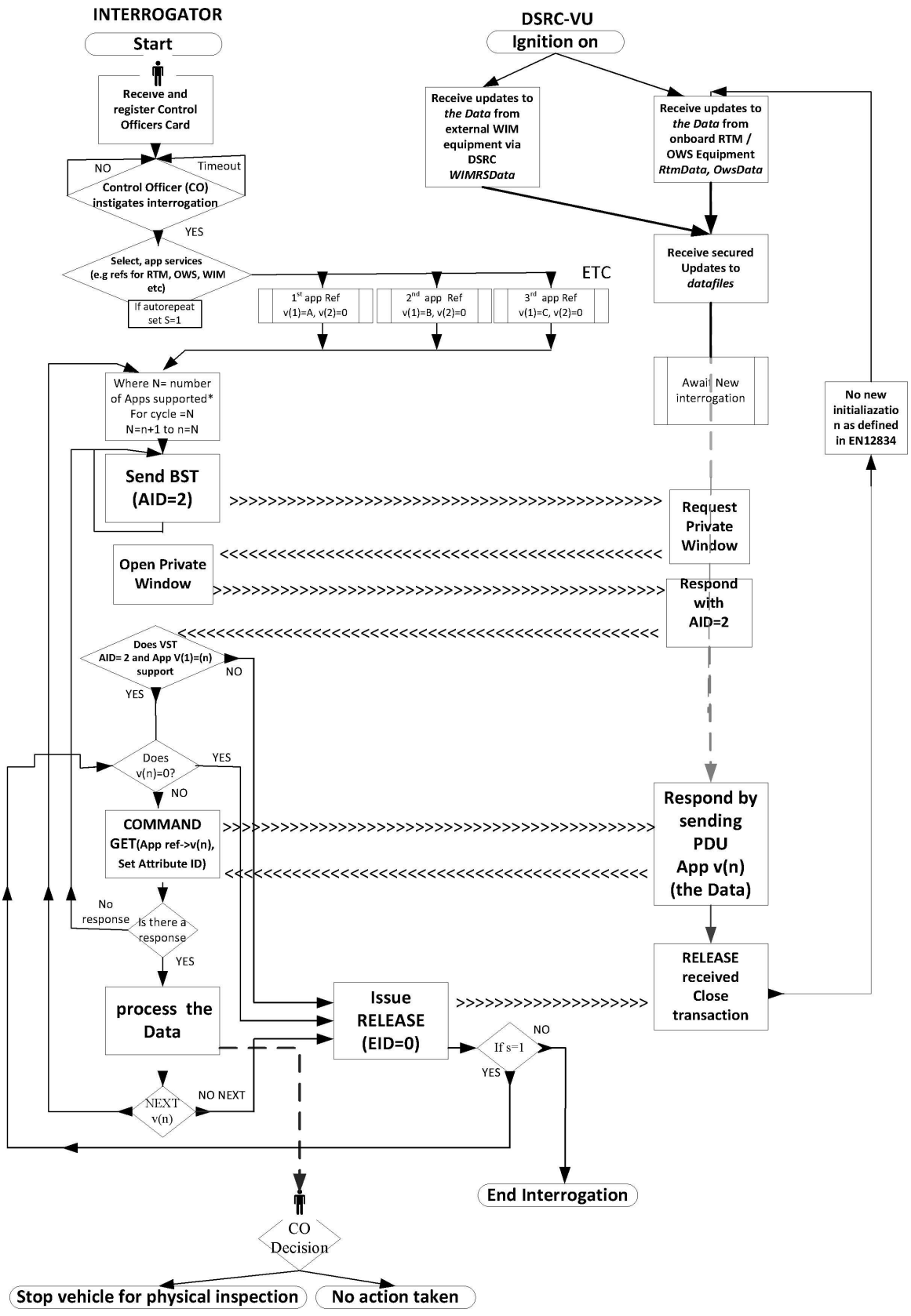
— **Schritt 8** Wenn mehrere Dienste angefragt werden, wird der Wert „n“ auf die nächste Dienstreferenznummer gesetzt und der Prozess wiederholt.

— **Schritt 9** Das *REDCR* bestätigt den Erhalt der Daten, indem es einen Frame sendet, der der *DSRC-VU* einen RELEASE-Befehl sendet, die Sitzung zu beenden, ODER wechselt, falls es den erfolgreichen Erhalt des LDPU nicht validieren konnte, zurück zu Schritt 6.

Siehe Abbildung 14.6 als bildliche Darstellung des Transaktionsprotokolls.

Abbildung 14.6

Ablauf RTM über 5,8-GHz-DSRC (HINWEIS: Abbildung soll nicht übersetzt werden)



5.4.2 *Befehle*

DSC_35 Nur die folgenden Befehle werden in einer RTM-Transaktionsphase verwendet:

— **INITIALISATION.request**: Vom REDCR in Form eines Broadcast ausgegebener Befehl mit der Definition der vom REDCR unterstützten Befehle.

— **INITIALISATION.response**: Antwort der DSRC-VU, die die Verbindung bestätigt und eine Liste unterstützter Anwendungsinstanzen und der Angaben, wie diese adressiert werden (EID), enthält.

— **GET.request**: Vom *REDCR* an die *DSRC-VU* ausgegebener Befehl, der die zu adressierende Anwendungsinstanziierung durch eine definierte EID, wie in der VST erhalten, angibt und die *DSRC-VU* anweist, das bzw. die ausgewählten Attribute mit den *Daten* zu senden. Ziel des GET-Befehls ist es, dass das *REDCR die Daten* von der *DSRC-VU* erhält.

— **GET.response**: Antwort der DSRC-VU mit den angeforderten *Daten*.

— **ACTION.request ECHO**: Befehl, der die *DSRC-VU* anweist, die von der *DSRC-VU* erhaltenen Daten an das *REDCR* zurückzusenden. Ziel des ECHO-Befehls ist es, Werkstätten oder Prüfeinrichtungen zur Typgenehmigung in die Lage zu versetzen, zu prüfen, ob der DSRC-Link funktioniert, ohne auf die Sicherheitsangaben zugreifen zu müssen.

— **ACTION**.response ECHO: Antwort der DSRC VU auf den ECHO-Befehl.

— **EVENT_REPORT.request** RELEASE: Befehl, der der *DSRC-VU* mitteilt, dass die Transaktion beendet ist. Ziel des RELEASE-Befehls ist es, die Sitzung mit der *DSRC-VU* zu beenden. Bei Erhalt von RELEASE darf die *DSRC-VU* nicht mehr auf weitere Abfragen im Rahmen der aktuellen Verbindung antworten. Hinweis: Gemäß EN 12834 stellt eine DSRC-VU nur dann eine zweite Verbindung zur selben Abfrageeinrichtung her, wenn sie sich 255 Sekunden lang außerhalb des Kommunikationsbereichs befunden hat oder wenn sich die Beacon-ID der Abfrageeinrichtung geändert hat.

5.4.3 *Abfragebefehlssequenz*

DSC_36 Aus Perspektive der Befehl-Antwort-Sequenz lässt sich die Transaktion wie folgt beschreiben:

Sequenz	Sender		Empfänger	Beschreibung	Handlung
1	REDCR	>	DSRC-VU	Initialisierung des Kommunikations-Links — Anforderung	REDCR sendet BST
2	*DSRC-VU*	>	*REDCR*	*Initialisierung des Kommunikations-Links — Antwort*	*Wenn die BST AID=2 unterstützt, dann fordert die DSCR-VU ein privates Fenster an*
3	REDCR	>	DSRC-VU	Gewährt ein privates Fenster	Sendet Frame mit Zuweisung eines privaten Fensters
4	*DSRC-VU*	>	*REDCR*	*Sendet VST*	*Sendet Frame mit VST*
5	REDCR	>	DSRC-VU	Sendet GET.request für in Attribut enthaltene Daten für spezifische EID	
6	*DSRC-VU*	>	*REDCR*	*Sendet GET.response mit angefordertem Attribut für spezifische EID*	*Sendet Attribut (RTMData, OWS-Data …) mit Daten für spezifische EID*

Sequenz	Sender		Empfänger	Beschreibung	Handlung
7	REDCR	>	DSRC-VU	Sendet GET.request für Daten anderer Attribute (falls zutreffend)	
8	*DSRC-VU*	>	*REDCR*	*Sendet GET.response mit angefordertem Attribut*	*Sendet Attribut mit Daten für spezifische EID*
9	REDCR	>	DSRC-VU	Bestätigt erfolgreichen Empfang der Daten	Sendet RELEASE-Befehl, der die Transaktion beendet
10	*DSRC-VU*			*Beendet Transaktion*	

Ein Beispiel für Transaktionssequenz und -inhalte der ausgetauschten Frames ist in den Abschnitten 5.4.7 und 5.4.8 enthalten.

5.4.4 *Datenstrukturen*

DSC_37 Die semantische Struktur *der Daten* bei der Weitergabe an die 5,8-GHz-DSRC-Schnittstelle muss den Ausführungen in dieser Anlage entsprechen. Die Strukturierung dieser Daten ist in diesem Abschnitt angegeben.

DSC_38 Die Nutzlast (RTM-Daten) besteht aus der Verkettung der

1. EncryptedTachographPayload-Daten, der Verschlüsselung von TachographPayload gemäß ASN.1 in Abschnitt 5.4.5. Die Verschlüsselungsmethode ist in Anlage 11 beschrieben.

2. DSRCSecurityData, angegeben in Anlage 11.

DSC_39 Die RTM-Daten werden als RTM-Attribut=1 adressiert und im RTM-Container =10 übertragen.

DSC_40 Die RTM-ContextMark soll das unterstützte Standardteil in der TARV-Normenreihe (RTM entspricht Teil 9) identifizieren.

Das ASN.1-Modul für die DSRC-Daten innerhalb der RTM-Anwendung ist wie folgt definiert:

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                      -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
            tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
            tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
            tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
            }
Rtm-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

 RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
 }
RtmTransferAck ::= INTEGER {
                Ok (1),
                NoK (2)
                } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elemente von RtmData, durchgeführte Aktionen und Definitionen*

DSC_41 Die durch die VU zu berechnenden und zur Aktualisierung der gesicherten Daten in der DSRC-VU verwendeten Daten sind nach den in Tabelle 14.3 definierten Regeln zu berechnen:

Tabelle 14.3

Elemente von RtmData, durchgeführte Aktionen und Definitionen

(1) RTM-Datenelement	(2) Von der VU durchzuführende Aktion		(3) ASN.1-Datendefinition
RTM1 **Kennzeichen des Fahrzeugs**	Die VU legt den Wert des *tp15638VehicleRegistrationPlate*-Datenelements RTM1 aus dem aufgezeichneten Wert des Datentyps *VehicleRegistrationIdentification* gemäß Anlage 1 *VehicleRegistrationIdentification*	Amtliches Kennzeichen des Fahrzeugs als Zeichenstring	tp15638VehicleRegstrationPlate LPN, – Amtliches Kennzeichen des Fahrzeugs, importiert aus ISO 14906 mit der in EN 15509 angegebenen Beschränkung; dabei handelt es sich um eine SEQUENZ mit dem Code für den Ländernamen gefolgt von einer alphabetischen Angabe, gefolgt von dem Kennzeichen selbst, stets 14 Oktetten (aufgefüllt mit Nullen), sodass die Länge des Typs EN 15509 LPN stets 17 Oktette beträgt, von denen 14 das „tatsächliche" Kennzeichen angeben.

(1) RTM-Datenelement	(2) Von der VU durchzuführende Aktion		(3) ASN.1-Datendefinition
RTM2 **Geschwindigkeitsüberschreitung**	Die VU erstellt einen booleschen Wert für das Datenelement RTM2 tp15638SpeedingEvent. Der Wert tp15638SpeedingEvent wird von der VU anhand der in der VU verzeichneten Anzahl an Geschwindigkeitsüberschreitungen an einem der letzten 10 Tage des Auftretens gemäß Definition in Anhang 1C berechnet. Wenn es in den letzten 10 Tagen des Auftretens mindestens ein tp15638SpeedingEvent gab, wird der Wert tp15638SpeedingEvent auf TRUE gesetzt. ELSE: Wenn es in den letzten 10 Tagen des Auftretens keine Ereignisse gab, wird tp15638SpeedingEvent auf FALSE gesetzt.	1 (TRUE) — Gibt „irregularities in speed“ in den letzten 10 Tagen des Auftretens an	`tp15638speedingEvent BOOLEAN,`
RTM3 **Fahren ohne gültige Karte**	Die VU erstellt einen booleschen Wert für das Datenelement RTM3 tp15638DrivingWithoutValidCard. Die VU weist der Variablen tp15638DrivingWithoutValidCard den Wert TRUE zu, wenn die VU in den letzten 10 Tagen des Auftretens mindestens ein Ereignis des Typs „Fahren ohne gültige Karte“ gemäß Anhang 1C aufgezeichnet hat. ELSE: Wenn es in den letzten 10 Tagen des Auftretens keine Ereignisse gab, wird die Variable tp15638DrivingWithoutValidCard auf FALSE gesetzt.	1 (TRUE) = gibt „invalid card usage1“ an	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Gültige Fahrerkarte**	Die VU erstellt einen booleschen Wert für das Datenelement RTM4 tp15638DriverCard auf Grundlage der in der VU gespeicherten Daten und gemäß Anlage 1. Wenn keine Fahrerkarte vorhanden ist, muss die VU die Variable auf TRUE setzen ELSE: Wenn eine gültige Fahrerkarte vorhanden ist, setzt die VU die Variable auf FALSE	0 (FALSE) = Gibt Gültige Fahrerkarte	`tp15638DriverCard BOOLEAN,`
RTM5 **Einstecken der Karte während des Lenkens**	Die VU generiert einen booleschen Wert für das Datenelement RTM5. Die VU weist der Variablen tp15638CardInsertion den Wert TRUE zu, wenn die VU in den letzten 10 Tagen des Auftretens mindestens ein Ereignis des Typs „Einstecken der Karte während des Lenkens“ gemäß Anhang 1C aufgezeichnet hat. ELSE: Wenn es in den letzten 10 Tagen des Auftretens keine derartigen Ereignisse gab, wird die Variable tp15638CardInsertion auf FALSE gesetzt.	1 (TRUE) = Gibt „card insertion while driving“ innerhalb der letzten 10 Tage des Auftretens an	`tp15638CardInsertion BOOLEAN,`
RTM6 **Bewegungsdatenfehler**	Die VU erstellt einen booleschen Wert für das Datenelement RTM6. Die VU weist der Variablen tp15638MotionDataError den Wert TRUE zu, wenn die VU in den letzten 10 Tagen des Auftretens mindestens ein Ereignis des Typs „Bewegungsdatenfehler“ gemäß Anhang 1C aufgezeichnet hat. ELSE: Wenn es in den letzten 10 Tagen des Auftretens keine derartigen Ereignisse gab, wird die Variable tp15638MotionDataError auf FALSE gesetzt.	1 (TRUE) = gibt „motion data error“ in den letzten 10 Tagen des Auftretens an	`tp15638motionDataError BOOLEAN,`

(1) RTM-Datenelement	(2) Von der VU durchzuführende Aktion		(3) ASN.1-Datendefinition
RTM7 **Datenkonflikt Fahrzeugbewegung**	Die VU erstellt einen booleschen Wert für das Datenelement RTM7. Die VU weist der Variablen tp15638vehicleMotionConflict den Wert TRUE zu, wenn die VU in den letzten 10 Tagen des Auftretens mindestens ein Ereignis des Typs Datenkonflikt Fahrzeugbewegung (Wert „0A"H) aufgezeichnet hat. ELSE: Wenn es in den letzten 10 Tagen des Auftretens keine Ereignisse gab, wird die Variable tp15638vehicleMotionConflict auf FALSE gesetzt.	1 (TRUE) = gibt „motion Conflict" in den letzten 10 Tagen des Auftretens an	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Zweite Fahrerkarte**	Die VU erstellt einen booleschen Wert für das Datenelement RTM8 auf Grundlage des Anhangs 1C (Fahrertätigkeitsdaten TEAM oder BEIFAHRER). Wenn eine zweite gültige Fahrerkarte vorhanden ist, setzt die VU die Variable auf TRUE ELSE: Wenn keine gültige zweite Fahrerkarte vorhanden ist, setzt die VU die Variable auf FALSE	1 (TRUE) = gibt „second driver card inserted" an	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Derzeitige Aktivität**	Die VU erstellt einen booleschen Wert für das Datenelement RTM9. Wenn die VU als derzeitige Aktivität eine andere Aktivität als „LENKEN" gemäß Anlage 1C aufzeichnet, muss die VU die Variable auf TRUE setzen ELSE: Wenn die derzeitige Aktivität in der VU als „LENKEN" aufgezeichnet wird, muss die VU die Variable auf FALSE setzen	1 (TRUE) = andere Aktivität ausgewählt; 0 (FALSE) = Lenken ausgewählt	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Letzter Vorgang abgeschlossen**	Die VU generiert einen booleschen Wert für das Datenelement RTM10. Wenn die letzte Kartensitzung nicht korrekt gemäß Anlage 1C abgeschlossen wird, muss die VU die Variable auf TRUE setzen. ELSE: Wenn die letzte Kartensitzung korrekt abgeschlossen wurde, setzt die VU die Variable auf FALSE	1 (TRUE) = nicht korrekt abgeschlossen 0 (FALSE) = korrekt abgeschlossen	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Unterbrechung der Stromversorgung**	Die VU generiert einen Integer-Wert für das Datenelement RTM11. Die VU weist der Variablen tp15638PowerSupplyInterruption einen Wert gleich der längsten Unterbrechung der Stromversorgung gemäß Artikel 9 der Verordnung (EU) Nr. 165/2014 des Typs „Unterbrechung der Stromversorgung" im Sinne von Anhang 1C zu. ELSE: Wenn es in den letzten 10 Tagen des Auftretens nicht zu einer Unterbrechung der Stromversorgung gekommen ist, wird der Integer-Wert auf 0 gesetzt.	— Anzahl der Unterbrechungen der Stromversorgung in den in den letzten 10 Tagen des Auftretens	`tp15638powerSupplyInterruption` `INTEGER (0..127)`

(1) RTM-Datenelement	(2) Von der VU durchzuführende Aktion		(3) ASN.1-Datendefinition
RTM12 **Sensorstörung**	Die VU generiert einen Integer-Wert für das Datenelement RTM12. Die VU weist der Variablen sensorFault einen der folgenden Werte zu: — 1 wenn in den letzten 10 Tagen ein Ereignis vom Typ „35"H Sensor-störung aufgezeichnet worden ist, — 2 wenn in den letzten 10 Tagen ein Ereignis des Typs GNSS-Empfängerstörung (intern oder extern mit den Enum-Werten „51"H oder „52"H) aufgezeichnet worden ist, — 3 wenn in den letzten 10 Tagen des Auftretens ein Ereignis des Typs „53"H Kommunikationsstörung des externen GNSS aufgezeichnet worden ist, — 4 wenn in den letzten 10 Tagen des Auftretens sowohl Sensorstörungen als auch GNSS-Empfängerstörungen aufgezeichnet worden sind, — 5 wenn in den letzten 10 Tagen des Auftretens sowohl Sensorstörungen als auch externe GNSS-Kommunikationsstörungen aufgezeichnet worden sind, — 6 wenn in den letzten 10 Tagen des Auftretens sowohl GNSS-Empfängerstörungen als auch externe GNSS-Kommunikationsstörungen aufgezeichnet worden sind, — 7 wenn in den letzten 10 Tagen des Auftretens alle drei Arten von Sensorstörungen aufgezeichnet worden sind. ELSE: Die FE muss einen Wert von 0 zuweisen, wenn in den letzten 10 Tagen des Auftretens keine Ereignisse aufgezeichnet worden sind	— Sensorstörung ein Oktett gemäß Datenglossar	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Zeiteinstellung**	Für das Datenelement RTM13 generiert die VU einen Integer-Wert (timeReal gemäß Anlage 1) auf Grundlage des Vorliegens von Zeiteinstellungsdaten gemäß Anhang 1C. Die VU weist den Zeitwert zu, an dem die letzte Zeiteinstellung erfolgt ist. ELSE: Wenn in der VU kein Ereignis „Zeiteinstellung" gemäß Anhang 1C vorhanden ist, muss die VU einen Wert von 0 festlegen.	Zeitpunkt von „last adjustment"	`tp15638TimeAdjustment` `INTEGER(0..4294967295)`
RTM14 **Sicherheitsverletzender Versuch**	Für das Datenelement RTM14 generiert die VU einen Integer-Wert (timeReal gemäß Anlage 1) auf Grundlage des Vorliegens eines Ereignisses „Versuch Sicherheitsverletzung" gemäß Anhang 1C. Die VU setzt den Wert auf den Zeitpunkt des letzten von der VU verzeichneten sicherheitsverletzenden Versuchs. ELSE: Wenn in der VU kein Ereignis „Versuch Sicherheitsverletzung" gemäß Anhang 1C vorhanden ist, muss die VU einen Wert von 0x00FF festlegen.	Zeitpunkt von „latest breach attempt" — Standardwert =0x00FF	`tp15638LatestBreachAttempt` `INTEGER(0..4294967295)`
RTM15 **Letzte Kalibrierung**	Für das Datenelement RTM15 generiert die VU einen Integer-Wert (timeReal gemäß Anlage 1) auf Grundlage des Vorliegens von letzten Kalibrierungsdaten gemäß Anhang 1C. Die VU setzt den Wert auf den Zeitpunkt der letzten beiden Kalibrierungen (RTM15 und RTM16) in VuCalibrationData gemäß Anlage 1 Die VU setzt den Wert für RTM15 auf timeReal des letzten Kalibrierungsdatensatzes.	Zeitpunkt des letzten Kalibrierungsdatensatzes	`tp15638LastCalibrationData` `INTEGER(0..4294967295)`

(1) RTM-Datenelement	(2) Von der VU durchzuführende Aktion		(3) ASN.1-Datendefinition
RTM16 **Vorherige Kalibrierung**	Für das Datenelement RTM16 generiert die VU einen Integer-Wert (timeReal gemäß Anlage 1) des Kalibrierungsdatensatzes vor der letzten Kalibrierung. ELSE: Wenn keine vorherige Kalibrierung vorliegt, setzt die VU den Wert von RTM16 auf 0.	Zeitpunkt von „previous calibration“ Daten	`tp15638PrevCalibrationData` `INTEGER(0..4294967295)`
RTM17 **Anschlussdatum des Fahrtenschreibers**	Für das Datenelement RTM17 generiert die VU einen Integer-Wert (timeReal gemäß Anlage 1). Die VU setzt den Wert auf den Zeitpunkt der Erstinstallation der VU. Die VU extrahiert diese Daten aus den VuCalibrationData (Anlage 1) der vuCalibrationRecords, wobei CalibrationPurpose gleich: „03“H	Anschlussdatum des Fahrtenschreibers	`tp15638DateTachoConnected` `INTEGER(0..4294967295)`
RTM18 **Aktuelle Geschwindigkeit**	Die VU generiert einen Integer-Wert für das Datenelement RTM18 Die VU setzt den Wert für RTM16 auf die bei der jüngsten Aktualisierung von RtmData zuletzt als aktuell aufgezeichnete Geschwindigkeit.	Zuletzt als aktuell aufgezeichnete Geschwindigkeit	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Zeitstempel**	Für das Datenelement RTM19 generiert die VU einen Integer-Wert (timeReal gemäß Anlage 1). Die VU setzt den Wert für RTM19 auf den Zeitpunkt der jüngsten Aktualisierung von RtmData.	Zeitstempel von „current TachographPayload record“	`tp15638Timestamp` `INTEGER(0..4294967295)`

5.4.6 *Mechanismus der Datenübertragung*

DSC_42 Die zuvor definierten Nutzlastdaten werden vom REDCR nach der Initialisierungsphase abgerufen und anschließend von der *DSRC-VU* im zugewiesenen Fenster übertragen. Zum Abrufen der Daten verwendet das REDCR den Befehl GET.

DSC_43 Bei jedem DSRC-Austausch werden die Daten mit PER (Packed Encoding Rules) verschlüsselt.

5.4.7 *Detaillierte Beschreibung der DSRC-Transaktion*

DSC_44 Die Initialisierung erfolgt gemäß DSC_44 bis DSC_48 und den Tabellen 14.4 bis 14.9. In der Einleitungsphase sendet das REDCR zunächst einen Frame mit einer BST (Beacon Service Table) gemäß EN 12834 und EN 13372, 6.2, 6.3, 6,4, und 7.1 mit den in der folgenden Tabelle 14.4 aufgeführten Einstellungen.

Tabelle 14.4

Initialisierung — BST-Frame-Einstellungen

Feld	Einstellungen
Link Identifier	Broadcast-Adresse
BeaconId	Gemäß EN 12834
Time	Gemäß EN 12834
Profile	Keine Erweiterung, 0 oder 1 verwenden
MandApplications	Keine Erweiterung, EID nicht vorhanden, Parameter nicht vorhanden, AID=2 Freight&Fleet
NonMandApplications	Nicht vorhanden
ProfileList	Keine Erweiterung, Anzahl Profile in Liste = 0
Fragmentation header	Keine Fragmentierung
Layer 2 settings	Befehls-PDU, UI-Befehl

Ein praktisches Beispiel der in Tabelle 14.4 angegebenen Einstellungen samt Angabe der Bit-Verschlüsselungen findet sich in der folgenden Tabelle 14.5.

Tabelle 14.5

Initialisierung — Beispiele für die Inhalte von BST-Frames

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Broadcast ID	1111 1111	Broadcast-Adresse
3	MAC Control Field	1010 0000	PDU-Befehl
4	LLC Control field	0000 0011	UI-Befehl
5	Fragmentation header	1xxx x001	Keine Fragmentierung

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
6	BST	1000	Initialisierungsanfrage
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand-Anwendungen nicht vorhanden
		xxx	Herstellerkennung
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27-Bit-ID für Hersteller verfügbar
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32-Bit-UNIX-Realtime
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127, …)	0000 0000	Keine Erweiterung. Beispielprofil 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	Keine Erweiterung, Anzahl mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID nicht vorhanden
	OPTION indicator	0	Parameter nicht vorhanden
	AID DSRCApplicationEntityID } }	00 0010	Keine Erweiterung. AID=2 Freight&Fleet

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
19	ProfileList SEQUENCE (0..127, …) OF Profile }	0000 0000	Keine Erweiterung, Anzahl Profile in Liste = 0
20	FCS	xxxx xxxx	Frame-Überprüfungssequenz
21		xxxx xxxx	
22	Flag	0111 1110	End-Flag

DSC_45 Eine *DSRC-VU* benötigt beim Empfang einer BST die Zuweisung eines privaten Fensters gemäß EN 12795 und EN 13372, 7.1.1, ohne spezifische RTM-Einstellungen. Tabelle 14.6 enthält ein Beispiel für die Bit-Verschlüsselung.

Tabelle 14.6

Initialisierung — Frame-Inhalte für die Anforderung einer Zuweisung eines privaten Fensters

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	0110 0000	Anforderung eines privaten Fensters
7	FCS	xxxx xxxx	Frame-Überprüfungssequenz
8		xxxx xxxx	
9	Flag	0111 1110	End-Flag

DSC_46 Das REDCR antwortet mit der Zuweisung eines privaten Fensters, wie durch EN 12795 und EN 13372, 7.1.1 angegeben, ohne spezifische RTM-Einstellungen.

Tabelle 14.7 enthält ein Beispiel für die Bit-Verschlüsselung.

Tabelle 14.7

Initialisierung — Frame-Inhalte für die Anforderung einer Zuweisung eines privaten Fensters

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	0010 s000	Zuweisung eines privaten Fensters
7	FCS	xxxx xxxx	Frame-Überprüfungssequenz
8		xxxx xxxx	
9	Flag	0111 1110	End-Flag

DSC_47 Wenn sie die Zuweisung des privaten Fensters erhält, sendet die *DSRC-VU* ihre VST (Vehicle Service Table) gemäß EN 12834 und EN 13372, 6.2, 6.3, 6.4 und 7.1 mit den Einstellungen aus Tabelle 14.8, unter Verwendung des zugewiesenen Übertragungsfensters.

Tabelle 14.8

Initialisierung — VST-Frame-Einstellungen

Feld	Einstellungen
Private LID	Gemäß EN 12834
VST-Parameter	Fill=0, anschließend für jede unterstützte Anwendung: EID vorhanden, Parameter vorhanden,AID=2, EID wie durch OBU generiert
Parameter	Keine Erweiterung, enthält die RTM-ContextMark
ObeConfiguration	Fakultativ kann das Feld „ObeStatus“ vorliegen, es soll nicht von REDCR verwendet werden.
Fragmentation header	Keine Fragmentierung
Layer 2 settings	Befehls-PDU, UI-Befehl

DSC_48 Die *DSRC-VU* muss die „Freight&Fleet"-Anwendung unterstützen, gekennzeichnet durch die Anwendungskennung „2". Es können weitere Anwendungskennungen unterstützt werden, die aber in dieser VST nicht vorhanden sein sollen, da die BST lediglich AID=2 erfordert. Das Feld „Applications" enthält eine Liste der unterstützten Anwendungsinstanzen in der *DSRC-VU*. Für jede unterstützte Anwendungsinstanziierung ist ein Verweis auf den jeweiligen Standard gegeben: Dieser besteht aus dem Rtm-ContextMark, zusammengesetzt aus einer OBJEKTKENNUNG für die zugehörige Norm, den entsprechenden Teil (9 für RTM) und möglicherweise die Version sowie einer EID, die von der DSRC-VU generiert wird und dieser Anwendungsinstanz zugeordnet ist.

Ein praktisches Beispiel der in Tabelle 14.8 angegebenen Einstellungen samt Angabe der Bit-Verschlüsselungen findet sich in Tabelle 14.9.

Tabelle 14.9

Initialisierung — Beispiele für die Inhalte von VST-Frames

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1100 0000	PDU-Befehl
7	LLC Control field	0000 0011	UI-Befehl
8	Fragmentation header	1xxx x001	Keine Fragmentierung
9	VST SEQUENCE {	1001	Initialisierungsantwort
	Fill BIT STRING (SIZE(4))	0000	Nicht verwendet und auf 0 gesetzt
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Keine Erweiterung. Beispielprofil 0
11		0000 0001	Keine Erweiterung, 1 Anwendung
12	SEQUENCE {		
	OPTION indicator	1	EID vorhanden
	OPTION indicator	1	Parameter vorhanden
	AID DSRCApplicationEntityID	00 0010	Keine Erweiterung. AID=2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Gemäß OBU definiert, kennzeichnet Anwendungsinstanz.

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
14	Parameter Container {	0000 0010	Keine Erweiterung, Containerwahl = 02, Oktett-String
15		0000 1000	Keine Erweiterung, Länge von Rtm-ContextMark = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Objektkennung des unterstützten Standards, Teil und Version. Beispiel: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1). Das erste Oktett ist 06H, die Objektkennung; das zweite Oktett ist 06H, die Länge. Die nachfolgenden 6 Oktette verschlüsseln die Objektkennung des Beispiels Hinweis: Nur ein Element der Sequenz liegt vor (das fakultative Element „RtmCommProfile“ wird weggelassen)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus nicht vorhanden
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Herstellerkennung für DSRC-VU gemäß ISO-14816-Register
27		xxxx xxxx	
28	FCS	xxxx xxxx	Frame-Überprüfungssequenz
29		xxxx xxxx	
30	Flag	0111 1110	End-Flag

DCS_49 Anschließend liest das REDCR die Daten durch die Ausgabe eines GET-Befehls gemäß der Definition in EN 13372, 6.2, 6.3, 6.4 und EN 12834 mit den Einstellungen gemäß Tabelle 14.10.

Tabelle 14.10

Präsentation — Frame-Einstellungen für GET-Anforderungen

Feld	Einstellungen
Invoker Identifier (IID)	Nicht vorhanden
Link Identifier (LID)	Link-Adresse der spezifischen DSRC-VU
Chaining	Nein

Feld	Einstellungen
Element Identifier (EID)	Gemäß VST. Keine Erweiterung
Access Credentials	Nein
AttributeIdList	Keine Erweiterung, 1 Attribut, AttributeID = 1 (RtmData)
Fragmentation	Nein
Layer2 settings	PDU-Befehl, Polled ACn-Befehl

Tabelle 14.11 zeigt ein Beispiel für das Lesen der RTM-Daten.

Tabelle 14.11

Präsentation — Frame-Beispiel für GET-Anforderungen

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1010 s000	PDU-Befehl
7	LLC Control field	n111 0111	Polled ACn-Befehl, n Bit
8	Fragmentation header	1xxx x001	Keine Fragmentierung
9	Get.request SEQUENCE {	0110	GET-Anforderung
	OPTION indicator	0	Zugangsdaten nicht vorhanden
	OPTION indicator	0	IID nicht vorhanden
	OPTION indicator	1	AttributeIdList vorhanden
	Fill BIT STRING(SIZE(1))	0	Auf 0 gesetzt.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID der RTM-Anwendungsinstanz, Gemäß VST. Keine Erweiterung
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Keine Erweiterung, Anzahl Attribute = 1
12		0000 0001	AttributeId=1, RtmData. Keine Erweiterung

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
13	FCS	xxxx xxxx	Frame-Überprüfungssequenz
14		xxxx xxxx	
15	Flag	0111 1110	End-Flag

DSC_50 Beim Erhalt der GET-Anforderung sendet die *DSRC-VU* eine GET-Antwort mit den angeforderten Daten gemäß der in EN 13372, 6.2, 6.3, 6.4 und EN 12834 definierten GET-Antwort und den Einstellungen gemäß Tabelle 14.12.

Tabelle 14.12

Präsentation — Frame-Einstellungen für GET-Antwort

Feld	Einstellungen
Invoker Identifier (IID)	Nicht vorhanden
Link Identifier (LID)	Gemäß EN 12834
Chaining	Nein
Element Identifier (EID)	Gemäß VST.
Access Credentials	Nein
Fragmentation	Nein
Layer2 settings	Antwort-PDU, Antwort verfügbar und Befehl akzeptiert, ACn-Befehl

Tabelle 14.13 zeigt ein Beispiel für das Lesen der RTM-Daten.

Tabelle 14.13

Präsentation — Beispiel für die Inhalte des Antwort-Frames

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
6	MAC Control Field	1101 0000	Antwort-PDU
7	LLC Control field	n111 0111	Antwort verfügbar, ACn-Befehl, n Bit
8	LLC Status field	0000 0000	Antwort verfügbar und Befehl akzeptiert
9	Fragmentation header	1xxx x001	Keine Fragmentierung
10	Get.response SEQUENCE {	0111	Get-Antwort
	OPTION indicator	0	IID nicht vorhanden
	OPTION indicator	1	Attributliste vorhanden
	OPTION indicator	0	Rückgabestatus nicht vorhanden
	Fill BIT STRING(SIZE(1))	0	Nicht verwendet
11	EID INTEGER(0..127,…)	xxxx xxxx	Antwort aus RTM-Anwendungsinstanz. Keine Erweiterung
12	AttributeList SEQUENCE OF {	0000 0001	Keine Erweiterung, Anzahl Attribute = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Keine Erweiterung, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Keine Erweiterung, Containerwahl = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Frame-Überprüfungssequenz
n+2		xxxx xxxx	
n+3	Flag	0111 1110	End-Flag

DSC_51 Anschließend schließt das REDCR die Verbindung durch Ausgabe eines EVENT_REPORT, RELEASE-Befehls gemäß EN 13372, 6.2, 6.3, 6.4 und EN 12834,7.3.8, ohne spezifische RTM-Einstellungen. Tabelle 14.14 zeigt das Beispiel einer Bit-Verschlüsselung des RELEASE-Befehls.

Tabelle 14.14

Beendigung. EVENT_REPORT Inhalte des Release-Frames

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1000 s000	Der Frame enthält eine Befehls-LPDU
7	LLC Control field	0000 0011	UI-Befehl
8	Fragmentation header	1xxx x001	Keine Fragmentierung
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Zugangsdaten nicht vorhanden
	OPTION indicator	0	Ereignisparameter nicht vorhanden
	OPTION indicator	0	IID nicht vorhanden
	Mode BOOLEAN	0	Keine Antwort erwartet
10	EID INTEGER (0..127,…)	0000 0000	Keine Erweiterung, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Ereignisart 0 = Release
12	FCS	xxxx xxxx	Frame-Überprüfungssequenz
13		xxxx xxxx	
14	Flag	0111 1110	End-Flag

DSC_52 Es wird nicht erwartet, dass die *DSRC-VU* auf den Release-Befehl antwortet. Die Kommunikation wird dann geschlossen.

5.4.8 *Beschreibung der DSRC-Prüftransaktion*

DSC_53 Vollständige Prüfungen, die eine Sicherung der Daten beinhalten, müssen gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen durch befugtes Personal mit Zugang zu den Sicherheitsverfahren unter Verwendung der normalen, oben definierten GET-Befehle durchgeführt werden.

DSC_54 Inbetriebnahme und regelmäßige Inspektionen, bei denen eine Entschlüsselung und ein Verständnis der entschlüsselten Daten erforderlich sind, müssen gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen und Anlage 9 Typgenehmigung — Mindestanforderungen an die durchzuführenden Prüfungen durchgeführt werden.

Die grundlegende DSRC-Kommunikation kann hingegen mit dem Befehl ECHO geprüft werden. Solche Prüfungen können bei der Inbetriebnahme, bei regelmäßigen Inspektionen oder auf Verlangen der zuständigen Kontrollbehörde oder gemäß der Verordnung (EU) Nr. 165/2014 (siehe 6 unten) erforderlich sein.

DSC_55 Zur Durchführung dieser Prüfung der grundlegenden Kommunikation wird der Befehl ECHO vom REDCR während einer Sitzung ausgegeben, d. h. nach erfolgreicher Durchführung einer Initialisierungsphase. Die Abfolge der Interaktionen ähnelt deshalb derjenigen einer Abfrage:

— Schritt 1 *Das REDCR* sendet eine „Beacon Service Table" (BST) mit den Anwendungskennungen (AID) in der unterstützten Dienstliste. In der RTM-Anwendung ist dies einfach der Dienst mit AID-Wert = 2.

Die *DSRC-VU* wertet die empfangene BST aus; sofern sie erkennt, dass die BST Freight&Fleet (AID = 2) anfragt, antwortet die *DSRC-VU*. Wenn das *REDCR* nicht AID=2 anbietet, beendet die *DSRC-VU* die Transaktion mit dem *REDCR*.

— Schritt 2 Die *DSRC-VU* sendet eine Anfrage nach Zuweisung eines privaten Fensters.

— Schritt 3 Die REDCR sendet die Zuweisung eines privaten Fensters.

— Schritt 4 Die *DSRC-VU* sendet mithilfe des zugewiesenen privaten Fensters ihre Fahrzeugdiensttabelle (Vehicle Service Table, VST). Diese VST enthält eine Liste aller unterschiedlichen Anwendungsinstanziierungen, die diese *DSRC-VU* im Rahmen von AID=2 unterstützt. Die verschiedenen Instanziierungen sind durch einzelne EID zu identifizieren, von denen jede mit einem Parameterwert verbunden ist, der die unterstützte Anwendungsinstanz angibt.

— Schritt 5 Anschließend analysiert das *REDCR* die angebotene VST und beendet entweder die Verbindung (RELEASE), weil das Angebot der VST nicht interessant ist (d. h., es erhält von der *DSRC-VU* eine VST, die keine RTM-VU ist), oder es erhält eine passende VST und startet die Instanziierung der App.

— Schritt 6 Das *REDCR* gibt einen Befehl (ECHO) an die jeweilige *DSRC-VU* aus und weist ein privates Fenster zu.

— Schritt 7 Die *DSRC-VU* sendet mithilfe des neu zugewiesenen privaten Fensters eine ECHO-Antwort.

Die folgenden Tabellen enthalten ein praktisches Beispiel für eine ECHO-Austauschsitzung.

DSC_56 Initialisierung erfolgt gemäß 5.4.7 (DSC_44 bis DSC_48) und den Tabellen 14.4 bis 14.9.

DSC_57 Das REDCR gibt anschließend einen ACTION-, ECHO-Befehl gemäß ISO 14906 ohne spezifische RTM-Einstellungen aus, der 100 Datenoktetten enthält. In Tabelle 14.15 sind die Inhalte des durch das REDCR gesendeten Frames dargestellt.

Tabelle 14.15

Beispiel für ACTION-, ECHO-Anfrage-Frame

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen DSRC-VU
3		xxxx xxxx	

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1010 s000	PDU-Befehl
7	LLC Control field	n111 0111	Polled ACn-Befehl, n Bit
8	Fragmentation header	1xxx x001	Keine Fragmentierung
9	ACTION.request SEQUENCE {	0000	Action request (ECHO)
	OPTION indicator	0	Zugangsdaten nicht vorhanden
	OPTION indicator	1	Aktionsparameter vorhanden
	OPTION indicator	0	IID nicht vorhanden
	Mode BOOLEAN	1	Antwort erwartet
10	EID INTEGER (0..127,…)	0000 0000	Keine Erweiterung, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Keine Erweiterung, Aktionstyp ECHO-Anfrage
12	ActionParameter CONTAINER {	0000 0010	Keine Erweiterung, Containerwahl = 2
13		0110 0100	Keine Erweiterung. String-Länge = 100 Oktette
14		xxxx xxxx	Echo-Daten
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Frame-Überprüfungssequenz
115		xxxx xxxx	
116	Flag	0111 1110	End-Flag

DSC_58 Beim Erhalt der ECHO-Anforderung sendet die *DSRC-VU* eine ECHO-Antwort mit 100 Datenoktetten durch Widerspiegelung des erhaltenen Befehls, gemäß ISO 14906, ohne spezifische RTM-Einstellungen. In Tabelle 14.16 ist ein Beispiel für eine Kodierung auf Bit-Ebene dargestellt.

Tabelle 14.16

Beispiel für ACTION-, ECHO-Anfrage-Frame

Oktett #	Attribut/Feld	Bits in Oktett	Beschreibung
1	FLAG	0111 1110	Start-Flag
2	Private LID	xxxx xxxx	Link-Adresse der spezifischen VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1101 0000	Antwort-PDU
7	LLC Control field	n111 0111	ACn-Befehl, n Bit
8	LLC status field	0000 0000	Antwort verfügbar
9	Fragmentation header	1xxx x001	Keine Fragmentierung
10	ACTION.response SEQUENCE {	0001	ACTION-Antwort (ECHO)
	OPTION indicator	0	IID nicht vorhanden
	OPTION indicator	1	Antwortparameter vorhanden
	OPTION indicator	0	Rückgabestatus nicht vorhanden
	Fill BIT STRING (SIZE (1))	0	Nicht verwendet
11	EID INTEGER (0..127,...)	0000 0000	Keine Erweiterung, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Keine Erweiterung, Containerwahl = 2
13		0110 0100	Keine Erweiterung. String-Länge = 100 Oktette
14		xxxx xxxx	Echo-Daten
...		...	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Frame-Überprüfungssequenz
115		xxxx xxxx	
116	Flag	0111 1110	End-Flag

5.5 **Unterstützung für Richtlinie 2015/71/EG des Rates**

5.5.1 *Überblick*

DSC_59 Um die Richtlinie Nr. 2015/719/EG über die maximalen Abmessungen und Gewichte von Nutzfahrzeugen zu unterstützen, entspricht das zum Herunterladen der OWS-Daten über die 5,8-GHz-DSRC-Schnittstellenverbindung derjenigen für die RTM-Daten (siehe 5.4.1); der einzige Unterschied besteht darin, dass die Objektkennung für die TARV-Norm die ISO 15638 (TARV) Teil 20 für WOB/OWS adressiert.

5.5.2 *Befehle*

DSC_60 Die für eine OWS-Transaktion verwendeten Befehle entsprechen denjenigen für eine RTM-Transaktion.

5.5.3 *Abfragebefehlssequenz*

DSC_61 Die Abfragebefehlssequenz für OWS-Daten entspricht derjenigen für RTM-Daten.

5.5.4 *Datenstrukturen*

DSC_62 Die Nutzlast (OWS-Daten) besteht aus der Verkettung der

1. EncryptedOwsPayload-Daten, d. h. der Verschlüsselung von OwsPayload gemäß ASN.1 in Abschnitt 5.5.5. Die Verschlüsselungsmethode entspricht derjenigen für RtmData, die in Anlage 11 angegeben ist.

2. DSRCSecurityData, berechnet mit demselben Algorithmus wie dem für RtmData angewandten, der in Anlage 11 angegeben ist.

5.5.5 *ASN.1-Modul für die OWS-DSRC-Transaktion*

DSC_63. Das ASN.1-Modul für die DSRC-Daten innerhalb der RTM-Anwendung ist wie folgt definiert:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
   goods vehicle                                                          -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
        integer                       [0]    INTEGER,
        bitstring                     [1]    BIT STRING,
        octetstring                   [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString               [3]    UniversalString,
        beaconId                      [4]    BeaconID,
        t-apdu                        [5]    T-APDUs,
        dsrcApplicationEntityId       [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                   [7]    Dsrc-EID,
        attrIdList                    [8]    AttributeIdList,
        attrList                      [9]    AttributeList{RtmContainer},
        reserved10                    [10]   NULL,
        OwsContextmark                [11]   Ows-ContextMark,
        OwsData                       [12]   OwsData,
        reserved13                    [13]   NULL,
        reserved14                    [14]   NULL,
        time                          [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.5.6 *Elemente von OswData, durchgeführte Aktionen und Definitionen*

Die Elemente von OwsData sind so definiert, dass die Richtlinie Nr. 2015/719/EG über die höchstzulässigen Abmessungen und Gewichte von Nutzfahrzeugen unterstützt wird. Bedeutung:

— recordedWeight entspricht dem gemessenen Gesamtgewicht des Nutzfahrzeugs mit einer Auflösung von 10 kg gemäß EN ISO 14906. Ein Wert von 2500 beispielsweise entspricht einem Gewicht von 25 Tonnen.

— axlesConfiguration entspricht der Nutzfahrzeugkonfiguration hinsichtlich der Achsenzahl. Die Konfiguration wird mit der Bitmaske von 20 Bits definiert (erweitert aus EN ISO 14906).

Eine Bitmaske von 2 Bit entspricht der Konfiguration einer Achse gemäß folgendem Format:

— Bei Wert 00B liegt kein Wert vor, da das Fahrzeug über keine zur Erfassung der Achslast notwendige Ausrüstung verfügt.

— Bei Wert 01B liegt die Achse nicht vor.

— Bei Wert 10B liegt die Achse vor, die Achslast wurde berechnet und erfasst und wird im Feld axlesRecordedWeight ausgegeben.

— Wert 11B ist für zukünftige Zwecke reserviert.

Die letzten vier Bits sind für zukünftige Zwecke reserviert.

Achsenzahl										
Achsenzahl Zugmaschine			Achsenzahl Anhänger							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 Bits)

— axlesRecordedWeight stellt das spezifische Gewicht pro Achse mit einer Auflösung von 10 kg dar. Pro Achse werden zwei Oktette verwendet. Ein Wert von 150 beispielsweise entspricht einem Gewicht von 1 500 kg.

Die anderen Datentypen sind in 5.4.5 festgelegt.

5.5.7 *Mechanismen der Datenübertragung*

DSC_64 Der Mechanismus für die Übermittlung der OWS-Daten zwischen Abfrageeinrichtung und DSRC-Einrichtung im Fahrzeug entspricht demjenigen für die eRTM-Daten (siehe 5.4.6).

DSC_65 Die Datenübermittelung zwischen der Plattform zur Erfassung der Daten über das höchstzulässige Gewicht und der DSRC-Einrichtung im Fahrzeug basiert auf der physischen Verbindung und den in Abschnitt 5.6 definierten Schnittstellen und Protokollen.

5.6 **Datenübermittelung zwischen DSRC-VU und VU**

5.6.1 *Physische Verbindung und Schnittstellen*

DSC_66 Die Verbindung zwischen *VU* und *DSRC-VU* kann entweder über eine Kabelverbindung oder eine Kurzbereich-Drahtloskommunikation basierend auf Bluetooth v4.0 BLE erfolgen.

DSC_67 Unabhängig von der Wahl von Verbindung und Schnittstelle müssen die folgenden Anforderungen erfüllt sein:

DSC_68 a) Damit unterschiedliche Hersteller für die Lieferung der VU und DSRC-VU und auch unterschiedlicher Lose der DSRC-VU gewählt werden können, muss die Verbindung zwischen VU und DSRC-VU nach einem offenen Standard erfolgen. Die VU wird auf eine der folgenden Arten mit der DSRC-VU verbunden:

i) über ein mindestens 2 m langes Festkabel mit geradem H11-Stecker (11-polig) nach DIN 41612 von der DSRC-VU auf eine passende Buchse mit DIN/ISO-Zulassung vom VU-Gerät

ii) über Bluetooth Low Energy (BLE)

iii) über eine standardmäßige ISO-11898- oder SAE-J1939-Verbindung

DSC_69 b) Die Definition der Schnittstellen und Verbindung zwischen VU und DSRC-VU muss die in 5.6.2. definierten Befehle des Anwendungsprotokolls erfüllen, und

DSC_70 c) VU und DSRC-VU müssen die Datenübermittlung über die Verbindung im Hinblick auf Leistung und Stromversorgung unterstützen.

5.6.2 *Anwendungsprotokoll*

DSC_71 Das Anwendungsprotokoll zwischen VU-Fernkommunikationseinrichtung und DSRC-VU ist für die regelmäßige Übertragung der Fernkommunikationsdaten von der VU zur DSRC verantwortlich.

DSC_72 Die folgenden wichtigsten Befehle werden identifiziert:

1. Initialisierung des Kommunikationslinks — Anforderung
2. Initialisierung des Kommunikationslinks — Antwort
3. Senden der Daten samt Kennung der RTM-Anwendung und der durch die RTM-Daten definierten Nutzlast
4. Quittierung der Daten
5. Beendigung des Kommunikationslinks — Anforderung
6. Beendigung des Kommunikationslinks — Antwort

DSC_73 In ASN1.0 können die vorherigen Befehle wie folgt definiert sein:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Die Beschreibung der Befehle und Parameter lautet wie folgt:

— `RCDT-Communication Link Initialization – Request` dient zur Initialisierung des Kommunikationslinks. Der Befehl wird von der VU an die DSRC-VU gesendet. Der LinkIdentifier wird von der VU an die DSRC-VU gesendet, um einen bestimmten Kommunikationslink zu protokollieren.

(Hinweis: Dies dient dazu, zukünftige Links und andere Anwendungen/Module wie Wiegen an Bord zu unterstützen).

— `RCDT-Communication Link Initialization – Response` wird von der DSRC-VU für die Antwort auf die Anfrage zur Initialisierung des Kommunikationslinks verwendet. Der Befehl wird von der DSRC-VU an die VU gesendet. Der Befehl stellt das Ergebnis der Initialisierung als Antwort = 1 (Erfolg) oder = 0 (Fehler) dar.

DSC_75 Die Initialisierung des Kommunikationslinks erfolgt nach Installation, Kalibrierung und Anlassen des Motors/Einschalten der VU.

— `RCDT-Send Data` wird von der VU dazu verwendet, die signierten RCDT-Daten (d. h. *die Fernkommunikationsdaten*) an die DSRC-VU zu senden. Die Daten werden alle 60 Sekunden gesendet. Der Parameter DataTransactionId kennzeichnet die jeweilige Datenübertragung. Außerdem wird durch LinkIdentifier sichergestellt, dass der entsprechende Link korrekt ist.

— `RCDT-Data Acknowledgment` wird von der DSRC-VU gesendet, um der VU Rückmeldung über den Erhalt der Daten infolge eines Befehls `RCDT-Send Data` zu geben, gekennzeichnet durch den Parameter DataTransactionId. Der Antwortparameter lautet 1 (Erfolg) oder = 0 (Fehler). Wenn eine VU mehr als drei Antworten gleich 0 erhält oder wenn die VU kein RCDT Data Acknowledgment für einen bestimmten zuvor gesendeten RCDT-Send Data mit spezifischer DataTransactionId erhält, muss die VU ein Ereignis generieren und aufzeichnen.

— `RCDT-Communication Link Termination request` request wird von der VU an die DSRC-VU gesendet, um einen Link für einen spezifischen LinkIdentifier zu beenden.

DSC_76 Beim Neustart der DSRC-VU oder einer VU müssen alle bestehenden Kommunikationslinks gelöscht werden, da aufgrund eines abrupten Herunterfahrens einer VU „bezuglose“ Links vorhanden sein könnten.

— `RCDT-Communication Link Termination – Response` wird von der DSRC-VU an die VU gesendet, um die Aufforderung zur Beendigung des Links durch die VU für den spezifischen LinkIdentifier zu bestätigen.

5.7 **Fehlerbehandlung**

5.7.1 *Aufzeichnung und Kommunikation der Daten in der DSRC-VU*

DSC_77 *Die Daten* sind, stets gesichert, von der *VUSM*-Funktion der *DSRC-VU* bereitzustellen. Die *VUSM* stellt sicher, dass die Aufzeichnung der Daten in der *DSRC-VU* korrekt verläuft. Die Aufzeichnung und Protokollierung von Fehlern bei der Datenübermittlung von der *VU* in den Speicher der *DSRC-VU* muss mit dem Typ EventFaultType und dem Enum-Kommunikationsfehlerwert „62“H Remote Communication Facility zusammen mit dem Zeitstempel erfolgen.

DSC_78 Die *VU* führt eine Datei, die durch einen eindeutigen, von den Kontrolleuren leicht zuzuordnenden Namen gekennzeichnet ist, um VU-interne Kommunikationsfehler zu protokollieren.

DSC_79 Wenn die VUPM vergebens versucht, VU-Daten vom Sicherheitsmodul abzurufen (um diese an die VU-DSRC weiterzuleiten), muss sie diesen Fehler mit dem Typ EventFaultType und dem Enum-Kommunikationsfehlerwert *„62“H Remote Communication Facility* samt Zeitstempel aufzeichnen. Der Kommunikationsfehler wird erkannt, wenn mehr als drei Mal in Folge keine Nachricht `RCDT Data Acknowledgment` für die zugehörigen (d. h. mit der gleichen DataTransactionId `in den Send-Data- und Acknowledgment` -Nachrichten versehenen) `RCDT Send Data` eingeht.

5.7.2 *Fehler in der Drahtloskommunikation*

DSC_80 Die Behandlung von Kommunikationsfehlern muss mit derjenigen gemäß zugehörigen DSRC-Normen, nämlich EN 300 674-1, EN 12253, EN 12795, EN 12834 und den entsprechenden Parametern von EN 13372, übereinstimmen.

5.7.2.1 *Verschlüsselungs- und Signaturfehler*

DSC_81 Verschlüsselungs- und Signaturfehler sind gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen zu behandeln und sind in den Fehlernachrichten zur DSRC-Datenübermittlung nicht vorhanden.

5.7.2.2 *Aufzeichnung von Fehlern*

Das DSRC-Medium ist eine dynamische Drahtloskommunikation in einer Umgebung mit unsicheren atmosphärischen und Interferenzbedingungen, insbesondere in den an dieser Anwendung beteiligten Kombinationen „tragbares REDCR" und „Fahrzeug in Bewegung". Deshalb muss zwischen den Bedingungen „Lesefehler" und „Fehler" ein Unterschied bestehen. Bei einer Transaktion über eine Drahtlosschnittstelle sind Lesefehler gängig; anschließend wird in der Regel ein neuer Versuch gestartet, d. h. die BST erneut gesendet und die Sequenz wiederholt. Meist verläuft dieser erneute Kommunikationsversuch dann erfolgreich und die Daten werden übertragen, sofern das Fahrzeug sich nicht in der zur Wiederübertragung erforderlichen Zeit aus dem Empfangsbereich bewegt. (Eine „erfolgreiche" Instanz eines Lesevorgangs umfasst mitunter mehrere Versuche und Wiederholungen).

Ein Lesefehler kann auftreten, weil die Antennen nicht richtig gekoppelt sind (Fehler beim „Ausrichten"), weil eine der Antennen abgeschirmt ist (dies kann gewollt sein, aber auch durch die Nähe eines anderen Fahrzeugs verursacht sein), durch Funkstörung (insbesondere durch Wifi- oder andere öffentliche Drahtloskommunikation im Bereich von ca. 5,8 GHz), Radarinterferenz oder schwierige atmosphärische Bedingungen (z. B. während eines Unwetters) oder einfach dadurch, dass das Fahrzeug den Bereich der DSRC-Kommunikation verlässt. Die einzelnen Instanzen der Lesefehler lassen sich nicht aufzeichnen, da die Kommunikation schlichtweg nicht stattgefunden hat.

Wenn aber der Mitarbeiter der zuständigen Kontrollbehörde ein Fahrzeug anvisiert und versucht, dessen *DSRC-VU* abzufragen, die Daten jedoch nicht erfolgreich übermittelt werden, kann dieser Fehler auf eine gewollte Manipulation zurückzuführen sein. Deshalb muss der Mitarbeiter der zuständigen Kontrollbehörde den Fehler protokollieren und die an der Maßnahme beteiligten Kollegen über einen möglichen Verstoß informieren. Die Kollegen können dann das Fahrzeug anhalten und physisch überprüfen. Da aber keine erfolgreiche Kommunikation stattgefunden hat, kann die DSRC-VU keine Daten über den Fehler liefern. Eine solche Protokollierung ist deshalb abhängig vom Design des REDCR-Geräts.

Ein „Lesefehler" ist technisch gesehen etwas anderes als ein „Fehler" In diesem Kontext bedeutet „Fehler", dass ein falscher Wert erfasst wurde.

Die an die *DSRC-VU* gelieferten Daten sind bereits gesichert und müssen deshalb durch den Lieferanten der Daten verifiziert werden (siehe 5.4).

Anschließend über die Luftschnittstelle übermittelte Daten werden durch zyklische Redundanzprüfungen (CRC) auf der Kommunikationsebene geprüft. Wenn diese Prüfung erfolgreich verläuft, sind die Daten korrekt. Andernfalls werden die Daten erneut übertragen. Die Wahrscheinlichkeit, dass Daten eine CRC-Prüfung fälschlicherweise erfolgreich bestehen, ist statistisch so verschwindend gering, dass sie unberücksichtigt bleiben kann.

Wenn die CRC-Prüfung fehlschlägt und keine Zeit für ein erneutes Senden und Empfangen der korrekten Daten mehr bleibt, führt dies nicht zu einem Fehler, sondern zu einer Instanziierung einer bestimmten Art von Lesefehler.

Die einzige aussagekräftige „Fehlerinformation", die sich aufzeichnen lässt, ist die Anzahl erfolgreicher Initiierungen von Transaktionen, die nicht zu einer erfolgreichen Datenübermittlung an das REDCR geführt haben.

DSC_82 Das *REDCR* hat deshalb die Anzahl der Fälle mit Zeitstempel aufzuzeichnen, in denen die „Initialisierungsphase" einer DSRC-Abfrage erfolgreich verläuft, die Transaktion aber abbricht, bevor das REDCR *die Daten* erfolgreich abrufen konnte. Diese Daten sind dem Mitarbeiter der zuständigen Kontrollbehörde zur Verfügung zu stellen und im Speicher des REDCR-Geräts abzulegen. Wie dies geschieht, ist eine Frage des Produktdesigns oder der Festlegung durch die zuständige Kontrollbehörde.

Die einzige aussagekräftige „Fehlerinformation", die sich aufzeichnen lässt, ist die Anzahl der Fälle, in der das REDCR die empfangenen *Daten* nicht entschlüsseln konnte. Dies bezieht sich allerdings nur auf die Effizienz der REDCR-Software. Unter Umständen werden Daten technisch entschlüsselt, ergeben aber keinen semantischen Sinn.

DSC_83 Deshalb muss das *REDCR* mit einem Zeitstempel die Anzahl der Fälle mit Zeitstempel aufzeichnen, in denen das Gerät vergeblich versucht hat, die über die DSRC-Schnittstelle empfangenen Daten zu entschlüsseln.

6 INBETRIEBNAHME- UND REGELMÄSSIGE INSPEKTIONSPRÜFUNGEN DER FERNKOMMUNIKATIONSFUNKTION

6.1 **Allgemein**

DSC_84 Für die Fernkommunikationsfunktion sind zwei Arten von Prüfungen vorgesehen:

1) ECHO-Prüfung, um den Drahtloskommunikationskanal *DSRC-REDCR* >>-:-<*DSRC-VU wireless* zu überprüfen.
2) Ende-zu-Ende-Sicherheitsprüfung, um zu gewährleisten, dass eine Werkstattkarte auf die von der VU erzeugten verschlüsselten und signierten und über den Drahtloskommunikationskanal übermittelten Dateninhalte zugreifen kann.

6.2 **ECHO**

Die Spezifikationen dieses Abschnitts geben an, wie geprüft wird, dass die Verbindung *DSRC-REDCR* >>-:-<*DSRC-VU* in funktioneller Hinsicht aktiv ist.

Ziel des ECHO-Befehls ist es, Werkstätten oder Prüfeinrichtungen zur Typgenehmigung in die Lage zu versetzen, zu prüfen, ob der DSRC-Link funktioniert, ohne auf die Sicherheitsangaben zugreifen zu müssen. Die Ausrüstung des Prüfers muss deshalb nur in der Lage sein, eine DSRC-Kommunikation (durch Senden einer BST mit AID=2) einzuleiten, anschließend den Befehl ECHO zu senden und, bei funktionierender DSRC, die ECHO-Antwort zu empfangen. Zu Einzelheiten siehe 5.4.8. Wenn diese Antwort korrekt empfangen wird, kann bestätigt werden, dass die DSRC-Verbindung (*DSRC-REDCR* >>-:-<*DSRC-VU*) korrekt funktioniert.

6.3 **Prüfungen zur Validierung sicherer Dateninhalte**

DSC_85 Mit dieser Prüfung wird der sichere Ende-zu-Ende-Datenfluss überprüft. Für diese Prüfung wird ein DSRC-Prüflesegerät benötigt. Dieses DSRC-Prüflesegerät bietet die gleiche Funktionalität und wird mit denselben Spezifikationen wie das Lesegerät der Kontrollbehörden eingerichtet. Der einzige Unterschied besteht darin, dass anstelle einer Kontrollkarte eine Werkstattkarte benutzt wird, um den Benutzer des DSRC-Prüflesegeräts zu authentisieren. Die Prüfung kann im Anschluss an die Erstaktivierung eines intelligenten Fahrtenschreibers oder am Ende des Kalibrierungsverfahrens durchgeführt werden. Nach der Aktivierung generiert die Fahrzeugeinheit die gesicherten Früherkennungsdaten und übermittelt diese an die DSRC-VU.

DSC_86 Das Werkstattpersonal positioniert das DSRC-Prüflesegerät in einem Abstand von 2–10 Metern vor dem Fahrzeug.

DSC_87 Anschließend steckt das Werkstattpersonal eine Werkstattkarte in das DSRC-Prüflesegerät ein und fragt von der Fahrzeugeinheit die Früherkennungsdaten ab. Nach erfolgreicher Abfrage greift das Werkstattpersonal auf die empfangenen Daten zu, um zu überprüfen, ob deren Integrität erfolgreich validiert und die Daten entschlüsselt wurden.

Anlage 15

MIGRATION: VERWALTUNG GLEICHZEITIG VORHANDENER AUSRÜSTUNGSGENERATIONEN

INHALTSVERZEICHNIS

1. BEGRIFFSBESTIMMUNGEN 497

2. ALLGEMEINE BESTIMMUNGEN 497

2.1. Übersicht über die Umstellung 497

2.2. Interoperabilität zwischen VU und Karten 498

2.3. Interoperabilität zwischen VU und Bewegungssensoren 498

2.4. Interoperabilität zwischen Fahrzeugeinheiten, Fahrtenschreiberkarten und Geräte für das Herunterladen von Daten 498

2.4.1 Direktes Herunterladen von der Karte durch das IDE 498

2.4.2 Herunterladen von der Karte über eine Fahrzeugeinheit 499

2.4.3 Datendownload von Fahrzeugeinheiten 499

2.5. Interoperabilität zwischen VU und Kalibrierungsgeräten 499

3. WESENTLICHE SCHRITTE IM ZEITRAUM VOR DEM EINFÜHRUNGSDATUM 499

4. BESTIMMUNGEN FÜR DEN ZEITRAUM NACH DEM EINFÜHRUNGSDATUM 499

1. BEGRIFFSBESTIMMUNGEN

Im Sinne dieser Anlage gelten folgende Begriffsbestimmungen:

Intelligentes Fahrtenschreibersystem: gemäß Definition in diesem Anhang (Kapitel 1: Begriffsbestimmung bbb);

Fahrtenschreibersystem der 1. Generation: gemäß Definition in dieser Verordnung (Artikel 2: Begriffsbestimmung 1);

Fahrtenschreibersystem der 2. Generation: gemäß Definition in dieser Verordnung (Artikel 2: Begriffsbestimmung 7);

Einführungsdatum: gemäß Definition in diesem Anhang (Kapitel 1: Begriffsbestimmung ccc);

Intelligent Dedicated Equipment (IDE): Gerät, das zum Herunterladen von Daten verwendet wird, wie in Anlage 7 dieses Anhangs definiert.

2. ALLGEMEINE BESTIMMUNGEN

2.1. Übersicht über die Umstellung

Die Präambel dieses Anhangs bietet eine Übersicht über die Umstellung von Fahrtenschreibersystemen der 1. Generation auf solche der 2. Generation.

Über die Bestimmungen dieser Präambel hinaus gilt Folgendes:

— Bewegungssensoren der 1. Generation sind nicht interoperabel mit Fahrzeugeinheiten der 2. Generation.

— Bewegungssensoren der 2. Generation werden zum selben Zeitpunkt in Fahrzeugen eingebaut wie Fahrzeugeinheiten der 2. Generation.

— Geräte zum Herunterladen von Daten und zur Kalibrierung müssen weiterentwickelt werden, um beide Generationen von Kontrollgeräten und Fahrtenschreiberkarten zu unterstützen.

2.2. **Interoperabilität zwischen VU und Karten**

Fahrtenschreiberkarten der 1. Generation sind interoperabel mit Fahrzeugeinheiten der 1. Generation (gemäß Anhang 1B dieser Verordnung); Fahrtenschreiberkarten der 2. Generation wiederum sind interoperabel mit Fahrzeugeinheiten der 2. Generation (gemäß Anhang 1C dieser Verordnung). Zusätzlich gelten die nachfolgenden Bestimmungen.

MIG_001 Mit Ausnahme der in den Randnummern MIG_004 und MIG_005 genannten Fälle dürfen Fahrtenschreiberkarten der 1. Generation bis zu ihrem Ablaufdatum in Fahrzeugeinheiten der 2. Generation weiterverwendet werden. Ihre Inhaber können jedoch die Ersetzung durch Fahrtenschreiberkarten der 2. Generation fordern, sobald diese verfügbar sind.

MIG_002 Fahrzeugeinheiten der 2. Generation müssen in der Lage sein, eingesteckte gültige Fahrer-, Kontroll- und Unternehmenskarten der 1. Generation zu nutzen.

MIG_003 Diese Fähigkeit kann in solchen Fahrzeugeinheiten durch Werkstätten endgültig unterdrückt werden, sodass Fahrtenschreiberkarten der 1. Generation nicht mehr akzeptiert werden. Dies darf erst geschehen, nachdem die Europäische Kommission ein Verfahren eingeleitet hat, das Werkstätten hierzu auffordert, beispielsweise während der regelmäßigen Nachprüfung der Fahrtenschreiber.

MIG_004 Fahrzeugeinheiten der 2. Generation dürfen nur Werkstattkarten der 2. Generation nutzen können.

MIG_005 Zur Bestimmung der Betriebsart dürfen Fahrzeugeinheiten der 2. Generation nur die Art der gültigen eingesteckten Karten berücksichtigen, nicht aber ihre Generation.

MIG_006 Jede gültige Fahrtenschreiberkarte der 2. Generation muss in Fahrzeugeinheiten der 1. Generation genauso genutzt werden können wie eine Fahrtenschreiberkarte gleicher Art der 1. Generation.

2.3. **Interoperabilität zwischen VU und Bewegungssensoren**

Bewegungssensoren der 1. Generation sind interoperabel mit Fahrzeugeinheiten der 1. Generation; Bewegungssensoren der 2. Generation wiederum sind interoperabel mit Fahrzeugeinheiten der 2. Generation. Zusätzlich gelten die nachfolgenden Bestimmungen.

MIG_007 Fahrzeugeinheiten der 2. Generation können nicht mit Bewegungssensoren der 1. Generation gekoppelt und verwendet werden.

MIG_008 Bewegungssensoren der 2. Generation können entweder ausschließlich mit Fahrzeugeinheiten der 2. Generation gekoppelt und verwendet werden oder mit beiden Generationen von Fahrzeugeinheiten.

2.4. **Interoperabilität zwischen Fahrzeugeinheiten, Fahrtenschreiberkarten und Geräte für das Herunterladen von Daten**

MIG_009 Geräte für das Herunterladen von Daten können entweder ausschließlich mit einer Generation von Fahrzeugeinheiten verwendet werden oder mit beiden.

2.4.1 *Direktes Herunterladen von der Karte durch das IDE*

MIG_010 Daten werden durch das IDE von den in ihre Kartenlesegeräte eingesteckten Fahrtenschreiberkarten einer Generation unter Verwendung der Sicherheitsmechanismen und Datendownload-Protokolle dieser Generation heruntergeladen; heruntergeladene Daten müssen das für diese Generation festgelegte Format aufweisen.

MIG_011 Damit auch Nicht-EU-Kontrollbehörden Fahrer kontrollieren können, muss es möglich sein, Fahrer- (und Werkstatt-) Karten der 2. Generation genauso herunterzuladen wie Karten der 1. Generation. Heruntergeladen werden können müssen unter anderem:

— nicht signierte EF `IC` und `ICC`,

— nicht signierte EF (1. Generation) `Card_Certificate` und `CA_Certificate`,

— sonstige Anwendungsdaten-EF (innerhalb des TACHO DF), die durch das Download-Protokoll von Karten der 1. Generation angefordert werden. Diese Information wird entsprechend den Sicherheitsmechanismen der 1. Generation durch eine digitale Signatur gesichert.

Der entsprechende Download darf keine Anwendungsdaten-EF umfassen, die nur in Fahrer- (und Werkstatt-) Karten der 2. Generation vorhanden sind (Anwendungsdaten-EF innerhalb der TACHO_G2 DF).

2.4.2 *Herunterladen von der Karte über eine Fahrzeugeinheit*

MIG_012 Für den Datendownload von einer Karte der 2. Generation, die in eine Fahrzeugeinheit der 1. Generation eingesteckt ist, wird das Datendownload-Protokoll der 1. Generation verwendet. Die Karte antwortet auf Befehle der Fahrzeugeinheit in genau der gleichen Weise wie eine Karte der 1. Generation; heruntergeladene Daten müssen das gleiche Format aufweisen wie Daten, die von einer Karte der 1. Generation heruntergeladen werden.

MIG_013 Für den Datendownload von einer Karte der 1. Generation, die in eine Fahrzeugeinheit der 2. Generation eingesteckt ist, wird das in Anlage 7 dieses Anhangs definierte Datendownload-Protokoll verwendet. Die Fahrzeugeinheit sendet Befehle an die Karte in genau der gleichen Weise wie eine Fahrzeugeinheit der ersten Generation; heruntergeladene Daten müssen das für Karten der 1. Generation definierte Format einhalten.

2.4.3 *Datendownload von Fahrzeugeinheiten*

MIG_014 Für den Datendownload von Fahrzeugeinheiten der 2. Generation werden die Sicherheitsmechanismen der 2. Generation und das in Anlage 7 dieses Anhangs angegebene Datendownload-Protokoll verwendet.

MIG_015 Damit auch Nicht-EU-Kontrollbehörden Fahrer kontrollieren und Werkstätten in nicht EU-Ländern Daten von Fahrzeugeinheiten herunterladen können, ist es optional möglich, Daten von Fahrzeugeinheiten der 2. Generation unter Verwendung der Sicherheitsmechanismen und des Datendownload-Protokolls der 1. Generation herunterzuladen. Die heruntergeladenen Daten müssen das gleiche Format aufweisen wie Daten, die von einer Fahrzeugeinheit der 1. Generation heruntergeladen werden. Diese Funktion kann durch entsprechende Menübefehle ausgewählt werden.

2.5. **Interoperabilität zwischen VU und Kalibrierungsgeräten**

MIG_016 Kalibrierungsgeräte müssen in der Lage sein, Fahrtenschreiber jeder Generation unter Verwendung des Kalibrierungsprotokolls der entsprechenden Generation zu kalibrieren. Kalibrierungsgeräte können entweder ausschließlich mit Fahrtenschreibern einer einzigen Generation verwendet werden oder mit beiden.

3. WESENTLICHE SCHRITTE IM ZEITRAUM VOR DEM EINFÜHRUNGSDATUM

MIG_017 Prüfschlüssel und Zertifikate müssen den Herstellern spätestens **30 Monate** vor dem Einführungsdatum zur Verfügung stehen.

MIG_018 Die Interoperabilitätsprüfungen müssen bei Anfrage durch die Hersteller spätestens **15 Monate** vor dem Einführungsdatum gestartet werden können.

MIG_019 Offizielle Schlüssel und Zertifikate müssen den Herstellern spätestens **12 Monate** vor dem Einführungsdatum zur Verfügung stehen.

MIG_020 Die Mitgliedstaaten müssen Werkstattkarten der 2. Generation spätestens **3 Monate** vor dem Einführungsdatum ausgeben können.

MIG_021 Die Mitgliedstaaten müssen alle Arten von Fahrtenschreiberkarten der 2. Generation spätestens **1 Monat vor dem Einführungsdatum** ausgeben können.

4. BESTIMMUNGEN FÜR DEN ZEITRAUM NACH DEM EINFÜHRUNGSDATUM

MIG_022 Nach dem Einführungsdatum dürfen die Mitgliedstaaten nur noch Fahrtenschreiberkarten der 2. Generation ausgeben.

MIG_023 Hersteller von Fahrzeugeinheiten/Bewegungssensoren dürfen so lange Fahrzeugeinheiten/Bewegungssensoren der 1. Generation fertigen, wie diese in der Praxis eingesetzt werden, sodass defekte Komponenten ersetzt werden können.

MIG_024 Hersteller von Fahrzeugeinheiten/Bewegungssensoren können die Beibehaltung einer Typgenehmigung von Fahrzeugeinheiten/Bewegungssensoren der 1. Generation, die bereits über eine Typgenehmigung verfügen, beantragen und erlangen.

Anlage 16

ADAPTER FÜR FAHRZEUGE DER KLASSEN M1 UND N1

INHALTSVERZEICHNIS

1. ABKÜRZUNGEN UND REFERENZDOKUMENTE 501

1.1. Abkürzungen 501

1.2. Referenznormen 501

2. ALLGEMEINE EIGENSCHAFTEN UND FUNKTIONEN DES ADAPTERS 502

2.1. Allgemeine Beschreibung des Adapters 502

2.2. Funktionen 502

2.3. Sicherheit 502

3. VORSCHRIFTEN FÜR DAS KONTROLLGERÄT BEI NUTZUNG EINES ADAPTERS 502

4. BAUART UND FUNKTIONSMERKMALE DES ADAPTERS 503

4.1. Entgegennahme und Anpassung eingehender Geschwindigkeitsimpulse 503

4.2. Einspeisung der Eingangsimpulse in den eingebetteten Bewegungssensor 503

4.3. Eingebetteter Bewegungssensor 503

4.4. Sicherheitsanforderungen 503

4.5. Leistungsmerkmale 504

4.6. Werkstoffe 504

4.7. Markierungen 504

5. EINBAU DES KONTROLLGERÄTS BEI NUTZUNG EINES ADAPTERS 504

5.1. Einbau 504

5.2. Plombierung 505

6. EINBAUPRÜFUNGEN, NACHPRÜFUNGEN UND REPARATUREN 505

6.1. Regelmäßige Nachprüfungen 505

7. TYPGENEHMIGUNG FÜR DAS KONTROLLGERÄT BEI NUTZUNG EINES ADAPTERS 505

7.1. Allgemeines 505

7.2. Funktionszertifikat 506

1. ABKÜRZUNGEN UND REFERENZDOKUMENTE

1.1. **Abkürzungen**

NF Noch festzulegen

VU Fahrzeugeinheit

1.2. **Referenznormen**

ISO 16844-3 Road vehicles — Tachograph systems — Part 3: Motion sensor interface (Straßenfahrzeuge — Fahrtschreiber (Kontrollgeräte) — Teil 3: Schnittstelle Bewegungssensor)

2. ALLGEMEINE EIGENSCHAFTEN UND FUNKTIONEN DES ADAPTERS

2.1. **Allgemeine Beschreibung des Adapters**

ADA_001 Der Adapter stellt gesicherte, permanent die Fahrzeuggeschwindigkeit und die zurückgelegte Wegstrecke darstellende Daten für eine angeschlossene VU bereit.

Der Adapter ist nur für die Fahrzeuge bestimmt, die mit Kontrollgeräten nach Maßgabe dieser Verordnung ausgestattet sein müssen.

Der Adapter wird nur in den unter Begriffsbestimmung yy) „Adapter" von Anhang IC bestimmten Fahrzeugen eingebaut und genutzt, in denen der Einbau eines bestehenden Bewegungssensors anderer Art, der ansonsten den Bestimmungen dieses Anhangs und dessen Anlagen 1 bis 16 entspricht, mechanisch unmöglich ist.

Der Adapter wird nicht mechanisch mit einem bewegten Fahrzeugteil verbunden, sondern an die durch integrierte Sensoren oder alternative Schnittstellen generierten Geschwindigkeits-/Entfernungsimpulse angeschlossen.

ADA_002 Ein typgenehmigter Bewegungssensor (gemäß den Bestimmungen dieses Anhangs IC Abschnitt 8 – Typgenehmigung von Kontrollgeräten und Fahrtenschreiberkarten) ist im Adaptergehäuse anzubringen, das daneben einen Impulskonverter enthält, der die Eingangsimpulse in den eingebetteten Bewegungssensor einspeist. Der eingebettete Bewegungssensor ist an die VU anzuschließen, sodass die Schnittstelle zwischen der VU und dem Adapter den Anforderungen der Norm ISO 16844-3 entspricht.

2.2. **Funktionen**

ADA_003 Der Adapter muss folgende Funktionen erfüllen:

— Entgegennahme und Anpassung der eingehenden Geschwindigkeitsimpulse,

— Einspeisung der Eingangsimpulse in den eingebetteten Bewegungssensor,

— sämtliche Funktionen des eingebetteten Bewegungssensors unter Bereitstellung gesicherter Bewegungsdaten an die VU.

2.3. **Sicherheit**

ADA_004 Für den Adapter erfolgt keine Sicherheitszertifizierung gemäß den in Anlage 10 dieses Anhangs definierten allgemeinen Sicherheitsanforderungen für Bewegungssensoren. Stattdessen gelten die in Abschnitt 4.4 dieses Anhangs festgelegten sicherheitsbezogenen Anforderungen.

3. VORSCHRIFTEN FÜR DAS KONTROLLGERÄT BEI NUTZUNG EINES ADAPTERS

Die Vorschriften in den folgenden Kapiteln geben Hinweise für die Auslegung der Vorschriften dieses Anhangs bei der Nutzung eines Adapters. Die entsprechenden Randnummern von Anhang IC sind in Klammern angegeben.

ADA_005 Das Kontrollgerät eines mit einem Adapter ausgestatteten Fahrzeugs muss — sofern in dieser Anlage nicht anders angegeben — allen Bestimmungen dieser Anlage entsprechen.

ADA_006 Ist ein Adapter eingebaut, so besteht das Kontrollgerät aus Verbindungskabeln, dem Adapter (anstelle eines Bewegungssensors) und einer VU [01].

ADA_007 Die Funktion zur Feststellung von Ereignissen und/oder Störungen des Kontrollgeräts wird wie folgt geändert:

— Das Ereignis „Unterbrechung der Stromversorgung" wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet, von der VU bei einer 200 Millisekunden überschreitenden Unterbrechung der Stromversorgung des eingebetteten Bewegungssensors ausgelöst [79].

— Das Ereignis „Datenfehler Bewegung" wird von der VU bei einer Unterbrechung des normalen Datenflusses zwischen dem eingebetteten Bewegungssensor und der VU und/oder bei einem Datenintegritäts- oder Datenauthentizitätsfehler während des Datenaustauschs zwischen dem eingebetteten Bewegungssensor und der VU ausgelöst [83].

— Das Ereignis „Versuch Sicherheitsverletzung“ wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet, von der VU bei jedem anderen die Sicherheit des eingebetteten Bewegungssensors berührenden Ereignis ausgelöst [85].

— Die Störung „Kontrollgerät“ wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet, von der VU bei jeder Störung des eingebetteten Bewegungssensors ausgelöst [88].

ADA_008 Die mit dem eingebetteten Bewegungssensor zusammenhängenden Störungen des Adapters müssen durch das Kontrollgerät feststellbar sein [88].

ADA_009 Die Kalibrierungsfunktion der VU muss die automatische Koppelung des eingebetteten Bewegungssensors mit der Fahrzeugeinheit erlauben [202, 204].

4. BAUART UND FUNKTIONSMERKMALE DES ADAPTERS

4.1. **Entgegennahme und Anpassung eingehender Geschwindigkeitsimpulse**

ADA_011 Die Eingangsschnittstelle des Adapters nimmt Frequenzimpulse entgegen, die die Fahrzeuggeschwindigkeit und die zurückgelegte Wegstrecke darstellen. Elektrische Eigenschaften der Eingangsimpulse: *Durch den Hersteller NF.* Erforderlichenfalls kann die korrekte Verbindung der Eingangsschnittstelle des Adapters mit dem Fahrzeug durch Anpassungen ermöglicht werden, zu denen ausschließlich der Adapterhersteller und die zugelassene Werkstatt, die den Adapter einbaut, befugt sind.

ADA_012 Die Eingangsschnittstelle des Adapters muss gegebenenfalls die Frequenzimpulse der eingehenden Geschwindigkeitsimpulse mit einem festen Faktor multiplizieren oder durch einen festen Faktor dividieren können, um das Signal an einen Wert in der durch diesen Anhang festgelegten Spanne für den Parameter „Kfactor“ (4 000 bis 25 000 Imp/km) anzupassen. Dieser feste Faktor darf nur vom Adapterhersteller und der zugelassenen Werkstatt, die den Adapter einbaut, programmiert werden.

4.2. **Einspeisung der Eingangsimpulse in den eingebetteten Bewegungssensor**

ADA_013 Die Eingangsimpulse werden — gegebenenfalls wie oben ausgeführt angepasst — in den eingebetteten Bewegungssensor eingespeist, sodass jeder Eingangsimpuls vom Bewegungssensor erfasst wird.

4.3. **Eingebetteter Bewegungssensor**

ADA_014 Der eingebettete Bewegungssensor wird durch die Eingangsimpulse stimuliert und kann auf diese Weise — als wäre er mechanisch mit einem bewegten Fahrzeugteil verbunden — Bewegungsdaten generieren, die die Fahrzeugbewegung exakt darstellen.

ADA_015 Die Kenndaten des eingebetteten Bewegungssensors werden von der VU zur Identifizierung des Adapters genutzt [95].

ADA_016 Die im eingebetteten Bewegungssensor gespeicherten Einbaudaten werden als Informationen zum Einbau des Adapters betrachtet [122].

4.4. **Sicherheitsanforderungen**

ADA_017 Das Adaptergehäuse muss so konstruiert sein, dass es nicht geöffnet werden kann. Es muss plombiert sein, damit jeder Versuch der physischen Manipulation leicht erkennbar ist (z. B. durch Sichtprüfung, siehe ADA_035). Für die Plomben gelten die gleichen Bestimmungen wie für Bewegungssensorplomben [398 bis 406]

ADA_018 Die Entfernung des eingebetteten Bewegungssensors aus dem Adapter darf nicht ohne Zerstörung der Plombe(n) des Adaptergehäuses oder der Plombe zwischen dem Bewegungssensor und dem Adaptergehäuse möglich sein (siehe ADA_034).

ADA_019 Der Adapter stellt sicher, dass nur vom Adaptereingang stammende Bewegungsdaten angenommen und verarbeitet werden.

4.5. **Leistungsmerkmale**

ADA_020 Der Adapter muss in dem vom Hersteller festgelegten Temperaturbereich voll einsatzbereit sein.

ADA_021 Der Adapter muss bei einer Luftfeuchtigkeit von 10 % bis 90 % voll einsatzbereit sein [214].

ADA_022 Der Adapter muss gegen Überspannung, Falschpolung der Stromversorgung und Kurzschluss geschützt sein [216].

ADA_023 Der Adapter muss entweder

— auf ein Magnetfeld, das die Ermittlung von Fahrzeugbewegungsdaten stört, reagieren — unter diesen Umständen registriert und speichert die Fahrzeugeinheit eine Sensorstörung [88] — oder

— über einen Sensor verfügen, der vor Magnetfeldern geschützt oder dagegen unempfindlich ist [217].

ADA_024 Der Adapter muss der internationalen UN/ECE-Regelung R 10 zur elektromagnetischen Verträglichkeit entsprechen und gegen elektrostatische Entladungen und Störgrößen geschützt sein [218].

4.6. **Werkstoffe**

ADA_025 Der Adapter muss den Schutzgrad *(vom Hersteller in Abhängigkeit von der Einbauposition NF) erfüllen* [220, 221].

ADA_026 Das Adaptergehäuse muss gelb sein.

4.7. **Markierungen**

ADA_027 Am Adapter ist ein Typenschild mit folgenden Angaben anzubringen:

— Name und Anschrift des Adapterherstellers,

— Teilnummer und Baujahr des Adapters,

— Prüfzeichen des Adaptertyps oder des Typs des Kontrollgeräts, das den Adapter enthält,

— Einbaudatum des Adapters,

— Identifizierungsnummer des Fahrzeugs, in das der Adapter eingebaut ist.

ADA_028 Das Typenschild muss daneben folgende Angaben enthalten (sofern diese nicht unmittelbar an der Außenseite des eingebetteten Bewegungssensors ersichtlich sind):

— Name des Herstellers des eingebetteten Bewegungssensors,

— Teilnummer und Baujahr des eingebetteten Bewegungssensors,

— Prüfzeichen des eingebetteten Bewegungssensors.

5. EINBAU DES KONTROLLGERÄTS BEI NUTZUNG EINES ADAPTERS

5.1. **Einbau**

ADA_029 Der Einbau von Adaptern in Fahrzeuge darf nur von Fahrzeugherstellern oder zugelassenen Werkstätten, die zum Einbau, zur Aktivierung und zur Kalibrierung digitaler und intelligenter Fahrtenschreiber autorisiert sind, vorgenommen werden.

ADA_030 Die zugelassenen Werkstätten, die den Einbau von Adaptern vornehmen, passen die Eingangsschnittstelle an und wählen gegebenenfalls das Umrechnungsverhältnis für das Eingangssignal.

ADA_031 Die zugelassenen Werkstätten, die den Einbau von Adaptern vornehmen, plombieren das Adaptergehäuse.

ADA_032 Der Adapter muss möglichst nahe an dem Fahrzeugteil angebracht werden, das ihm die Eingangsimpulse bereitstellt.

ADA_033 Die Anschlusskabel für den Adapter müssen rot (Stromversorgung) und schwarz (Masse) sein.

5.2. **Plombierung**

ADA_034 Für die Plombierung gelten folgende Vorschriften:

— Das Adaptergehäuse muss plombiert sein (siehe ADA_017).

— Das Gehäuse des eingebetteten Bewegungssensors muss plombiert sein, es sei denn, der eingebettete Bewegungssensor kann nicht ohne Zerstörung der Plombe(n) des Adaptergehäuses entfernt werden (siehe ADA_018).

— Die Befestigung des Adaptergehäuses am Fahrzeug muss plombiert sein.

— Die Verbindung zwischen dem Adapter und dem Gerät, dass diesem seine Eingangsimpulse bereitstellt, muss (soweit nach vernünftigem Ermessen möglich) an beiden Enden plombiert sein.

6. EINBAUPRÜFUNGEN, NACHPRÜFUNGEN UND REPARATUREN

6.1. **Regelmäßige Nachprüfungen**

ADA_035 Bei Verwendung eines Adapters ist bei jeder regelmäßigen Nachprüfung (d. h. entsprechend den Randnummern [409] bis [413] von Anhang 1C) des Kontrollgeräts Folgendes zu überprüfen:

— Vorhandensein der entsprechenden Prüfzeichen auf dem Adapter,

— Unversehrtheit der Plomben des Adapters und seiner Anschlüsse,

— Einbau des Adapters gemäß der Angabe auf dem Einbauschild,

— Einbau des Adapters gemäß den Adapter- und/oder Fahrzeugherstellerspezifikationen,

— Zulässigkeit des Einbaus eines Adapters in das überprüfte Fahrzeug.

ADA_036 Bestandteil dieser Überprüfungen müssen eine Kalibrierung sowie ein Austausch der Plomben unabhängig von deren Zustand sein.

7. TYPGENEHMIGUNG FÜR DAS KONTROLLGERÄT BEI NUTZUNG EINES ADAPTERS

7.1. **Allgemeines**

ADA_037 Kontrollgeräte sind zusammen mit dem Adapter zur Typgenehmigung vorzulegen [425].

ADA_038 Adapter können entweder als eigenständiges Gerät oder als Bauteil eines Kontrollgeräts zur Typgenehmigung vorgelegt werden.

ADA_039 Die Typgenehmigung muss Funktionsprüfungen umfassen, die sich auch auf den Adapter erstrecken. Die positiven Ergebnisse der einzelnen Prüfungen werden in einem geeigneten Zertifikat ausgewiesen [426].

7.2. **Funktionszertifikat**

ADA_040 Ein Funktionszertifikat für einen Adapter oder ein Kontrollgerät, das einen Adapter einschließt, wird dem Adapterhersteller erst erteilt, nachdem die folgenden Mindestfunktionsprüfungen erfolgreich bestanden wurden:

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1.	**Administrative Prüfung**		
1.1	Dokumentation	Richtigkeit der Dokumentation zum Adapter	
2.	**Sichtprüfung**		
2.1.	Übereinstimmung des Adapters mit der Dokumentation		
2.2.	Kennung/Markierungen des Adapters		ADA_027, ADA_028
2.3	Werkstoffe des Adapters		[219] bis [223] ADA_026
2.4.	Plombierung		ADA_017, ADA_018, ADA_034
3.	**Funktionsprüfungen**		
3.1	Einspeisung der Geschwindigkeitsimpulse in den eingebetteten Bewegungssensor		ADA_013
3.2	Entgegennahme und Anpassung eingehender Geschwindigkeitsimpulse		ADA_011, ADA_012
3.3	Messgenauigkeit Wegstrecke/Geschwindigkeit		[30] bis [35], [217]
4.	**Umweltprüfungen**		
4.1	Prüfergebnisse des Herstellers	Ergebnisse der Umweltprüfung des Herstellers.	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMV**		
5.1	Störaussendung und Störanfälligkeit	Prüfung auf Einhaltung der Richtlinie 2006/28/EG	ADA_024
5.2	Prüfergebnisse des Herstellers	Ergebnisse der Umweltprüfung des Herstellers.	ADA_024