II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2018/502 DER KOMMISSION

vom 28. Februar 2018

zur Änderung der Durchführungsverordnung (EU) 2016/799 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 über eine Anbindung an ein globales Satellitennavigationssystem (GNSS-Ausrüstung), eine Ausrüstung für Fernabfragen (Früherkennung) sowie eine optionale Schnittstelle zu intelligenten Verkehrssystemen verfügen.

(2) Die technischen Vorschriften über Bauart, Prüfung, Einbau, Betrieb und Reparatur von Fahrtenschreibern und ihren Komponenten sind in der Durchführungsverordnung (EU) 2016/799 der Kommission ([2]) festgelegt.

(3) Gemäß den Artikeln 8, 9 und 10 der Verordnung (EU) Nr. 165/2014 dürfen Fahrzeuge, die am oder nach dem 15. Juni 2019 erstmals zugelassen werden, nur noch mit intelligenten Fahrtenschreibern ausgerüstet sein. Die Durchführungsverordnung (EU) 2016/799 ist daher zu ändern, damit die darin enthaltenen technischen Vorschriften ab diesem Datum gelten.

(4) Um Artikel 8 der Verordnung (EU) Nr. 165/2014 zu entsprechen, wonach der Standort des Fahrzeugs nach jeweils drei Stunden kumulierter Lenkzeit aufzuzeichnen ist, sollte die Durchführungsverordnung (EU) 2016/799 geändert werden, sodass Informationen über den Fahrzeugstandort mit dreistündiger Frequenz unter Verwendung eines nicht rücksetzbaren Messsystems gespeichert werden können und Verwechslungen mit der „ununterbrochenen Lenkzeit", bei der es sich um eine Messgröße mit anderer Funktion handelt, vermieden werden.

(5) Die Fahrzeugeinheit kann aus einem Einzelgerät oder aus mehreren im Fahrzeug verteilten Geräten bestehen. Die GNSS-Ausrüstung und die Ausrüstung für die dedizierte Nahbereichskommunikation („DSRC") können daher innerhalb oder außerhalb des Hauptgehäuses der Fahrzeugeinheit untergebracht sein. Bei externer Unterbringung sollte es möglich sein, für die beiden Ausrüstungen und das Hauptgehäuse der Fahrzeugeinheit jeweils als Komponenten eigene Typgenehmigungen zu erteilen, um das Typgenehmigungsverfahren für intelligente Fahrtenschreiber an die Erfordernisse des Marktes anzupassen.

(6) Die Vorschriften über die Speicherung von Zeitkonflikt-Ereignissen und Zeiteinstellungen müssen geändert werden, um zwischen automatischen Zeiteinstellungen, die nach einem eventuellen Manipulationsversuch oder einer Fehlfunktion des Fahrtenschreibers ausgelöst werden, und den Zeiteinstellungen, die aus anderen Gründen wie etwa der Instandhaltung erfolgen, differenzieren zu können.

(7) Anhand der Datenkennungen sollte es möglich sein, zwischen Daten, die von intelligenten Fahrtenschreibern heruntergeladen werden, und von Fahrtenschreibern einer früheren Generation heruntergeladenen Daten zu unterscheiden.

([1]) ABl. L 60 vom 28.2.2014, S. 1.

([2]) 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 (ABl. L 139 vom 26.5.2016, S. 1).

(8) Die Gültigkeitsdauer der Unternehmenskarte muss von zwei auf fünf Jahre verlängert werden, um sie an die Gültigkeitsdauer der Fahrerkarte anzugleichen.

(9) Die Beschreibung bestimmter Störungen und Ereignisse, die Validierung der Eingaben des Orts des Beginns bzw. Endes des Arbeitstages, die Zustimmung des Fahrers zur Verwendung der Schnittstelle zu intelligenten Verkehrssystemen („ITS“) für Daten, die von der Fahrzeugeinheit über das Fahrzeugnetzwerk übertragen werden, sowie andere technische Fragen sollten präzisiert werden.

(10) Um sicherzustellen, dass die Zertifizierung der Plomben von Fahrtenschreibern dem neuesten Stand entspricht, müssen diese an die neue Norm über die Sicherheit mechanischer Plomben zur Verwendung bei Fahrtenschreibern angepasst werden.

(11) In dieser Verordnung werden Bauart, Prüfung, Einbau und Betrieb von Systemen behandelt, die auch Funkanlagen umfassen können, die in der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates [1] geregelt sind. Die Richtlinie regelt das Inverkehrbringen und die Inbetriebnahme elektronischer und elektrischer Geräte, die Funkwellen für die Kommunikation und/oder Funkortung auf horizontaler Ebene nutzen, wobei insbesondere der elektrischen Sicherheit, der Kompatibilität mit anderen Systemen, dem Zugang zu Funkfrequenzen sowie dem Zugang zu Notrufdiensten und/oder etwaigen Bestimmungen anderer delegierter Rechtsakte Rechnung getragen wird. Um die effiziente Nutzung von Funkfrequenzen zu gewährleisten, schädliche funktechnische Störungen zu verhindern, die Sicherheit und die elektromagnetische Verträglichkeit von Funkanlagen zu gewährleisten und andere spezifische delegierte Vorschriften zu erfüllen, sollte die vorliegende Verordnung die genannte Richtlinie unberührt lassen.

(12) Die Durchführungsverordnung (EU) 2016/799 sollte daher geändert werden.

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

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Die Durchführungsverordnung (EU) 2016/799 wird wie folgt geändert:

1. Artikel 1 wird wie folgt geändert:

a) Die Absätze 2 und 3 erhalten folgende Fassung:

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

3. Andere als intelligente Fahrtenschreiber müssen – hinsichtlich Bauart, Prüfung, Einbau, Nachprüfung, Betrieb und Reparatur – weiterhin den Anforderungen des Anhangs I der Verordnung (EU) Nr. 165/2014 bzw. des Anhangs IB der Verordnung (EWG) Nr. 3821/85 des Rates (*) genügen.

(*) 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).“

b) Folgender Absatz 5 wird angefügt:

„5. Diese Verordnung berührt nicht die Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates (*).

(*) Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62).“

2. Artikel 2 wird wie folgt geändert:

a) Begriffsbestimmung 3 erhält folgende Fassung:

„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 IC dieser Verordnung sowie Zeichnungen, Fotografien und anderer relevanter Unterlagen;“

[1] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62).

b) Begriffsbestimmung 7 erhält folgende Fassung:

„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 IC dieser Verordnung;"

c) Begriffsbestimmung 8 erhält folgende Fassung:

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

d) folgende Begriffsbestimmung 10 wird eingefügt:

„10) ‚Fahrzeugeinheit' ist der Fahrtenschreiber ohne den Bewegungssensor und ohne die Verbindungskabel zum Bewegungssensor.

Sie kann aus einem Einzelgerät oder aus mehreren im Fahrzeug verteilten Geräten bestehen und umfasst eine Verarbeitungseinheit, einen Massenspeicher, eine Zeitmessfunktion, zwei Chipkarten-Schnittstellengeräte für Fahrer und Beifahrer, einen Drucker, eine Datenanzeige, Steckverbinder und Bedienelemente für Nutzereingaben, einen GNSS-Empfänger und eine Ausrüstung zur Fernkommunikation.

Die Fahrzeugeinheit kann aus folgenden typgenehmigungspflichtigen Teilen bestehen:

— Fahrzeugeinheit als Einzelkomponente (einschließlich GNSS-Empfänger und Fernkommunikationsausrüstung),

— Hauptgehäuse der Fahrzeugeinheit (einschließlich Fernkommunikationsausrüstung) und externer GNSS-Ausrüstung,

— Hauptgehäuse der Fahrzeugeinheit (einschließlich GNSS-Empfänger) und externer Fernkommunikationsausrüstung,

— Hauptgehäuse der Fahrzeugeinheit, externer GNSS-Ausrüstung und externer Fernkommunikationsausrüstung.

Besteht die Fahrzeugeinheit aus mehreren im Fahrzeug verteilten Geräten, so sind im Hauptgehäuse der Fahrzeugeinheit die Verarbeitungseinheit, der Massenspeicher und die Zeitmessfunktion untergebracht.

Das Kürzel ‚VU' (vehicle unit) wird für ‚Fahrzeugeinheit' oder ‚Hauptgehäuse der Fahrzeugeinheit' verwendet";

3. Artikel 6 dritter Absatz erhält folgende Fassung:

„Der Anhang IC gilt jedoch ab dem 15. Juni 2019, ausgenommen Anlage 16, die ab dem 2. März 2016 gilt."

4. Anhang IC wird gemäß Anhang I der vorliegenden Verordnung geändert.

5. Anhang II wird gemäß Anhang II der vorliegenden Verordnung geändert.

Artikel 2

Inkrafttreten

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

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

Brüssel, den 28. Februar 2018

Für die Kommission
Der Präsident
Jean-Claude JUNCKER

ANHANG I

Anhang IC der Verordnung (EU) 2016/799 wird wie folgt geändert:

1. Das Inhaltsverzeichnis wird wie folgt geändert:

   a) Nummer 3.12.5 erhält folgende Fassung:

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

   b) Nummer 4.5.3.2.16 erhält folgende Fassung:

   „4.5.3.2.16 Ortsdaten zu drei Stunden kumulierter Lenkzeit“

   c) Nummer 4.5.4.2.14 erhält folgende Fassung:

   „4.5.4.2.14 Ortsdaten zu drei Stunden kumulierter Lenkzeit“

   d) Nummer 6.2 erhält folgende Fassung:

   „6.2 Prüfung neuer oder reparierter Komponenten“

2. Abschnitt 1 wird wie folgt geändert:

   a) Die Begriffsbestimmung ll erhält folgende Fassung:

   „ll) ‚Ausrüstung zur Fernkommunikation‘ oder ‚Ausrüstung zur Früherkennung per Fernkommunikation‘

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

   b) Die Begriffsbestimmung tt erhält folgende Fassung:

   „tt) ‚Zeiteinstellung‘

   die Einstellung der aktuellen Zeit; diese Einstellung kann automatisch in regelmäßigen Abständen anhand der vom GNSS-Empfänger gelieferten Zeitangabe oder in der Betriebsart Kalibrierung vorgenommen werden;“

   c) Der erste Gedankenstrich der Begriffsbestimmung yy erhält folgende Fassung:

   „— ausschließlich in Fahrzeuge der Klassen M1 und N1 (gemäß der Begriffsbestimmung in Anhang II der Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates (*) in der zuletzt geänderten Fassung) eingebaut ist und eingesetzt wird;“

   d) Die folgende neue Begriffsbestimmung fff wird angefügt:

   „fff) ‚kumulierte Lenkzeit‘

   Anzahl der insgesamt akkumulierten Minuten Lenkzeit in einem bestimmten Fahrzeug.

   Der Wert der kumulierten Lenkzeit ist eine frei laufende Zählung aller Minuten, die die Funktion ‚Überwachung der Lenktätigkeiten‘ des Kontrollgeräts als LENK-Zeit betrachtet, und dient nur dazu, die Aufzeichnung der Fahrzeugposition immer dann auszulösen, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht. Die Akkumulierung beginnt mit der Aktivierung des Kontrollgeräts. Sie bleibt von jeder anderen Bedingung, wie z. B. ‚Kontrollgerät nicht erforderlich‘ oder ‚Fährüberfahrt/Zugfahrt‘, unberührt.

   Der Wert der kumulierten Lenkzeit ist nicht für die Anzeige, den Druck oder das Herunterladen bestimmt;“

3. In Abschnitt 2.3 Absatz 13 erhält der letzte Gedankenstrich folgende Fassung:

„— die Fahrzeugeinheiten haben eine normale Gültigkeitsdauer von 15 Jahren ab dem Certificate Effective Date für die Fahrzeugeinheit; die Fahrzeugeinheiten können jedoch für weitere 3 Monate nur für das Herunterladen von Daten verwendet werden."

4. Abschnitt 2.4 Absatz 1 erhält folgende Fassung:

„Durch die Systemsicherheit soll folgender Schutz gewährleistet sein: Schutz des Massenspeichers, sodass 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 der Fahrzeugeinheit und der externen GNSS-Ausrüstung (soweit vorhanden) 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."

5. In Abschnitt 3.2 Absatz 27 erhält der zweite Gedankenstrich folgende Fassung:

„— Positionen, an denen die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht;"

6. Abschnitt 3.4 Absatz 49 erhält folgende Fassung:

„49) Bei der ersten Tätigkeitsänderung auf UNTERBRECHUNG/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 (sodass möglicherweise der Wechsel auf ARBEIT aufgehoben wird)."

7. Abschnitt 3.6.1 Absatz 59 erhält folgende Fassung:

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

Unter den folgenden Bedingungen wird die bei der letzten Kartenentnahme vorgenommene temporäre Eingabe validiert (und kann somit nicht mehr überschrieben werden):

— Eingabe eines Orts, an dem der aktuelle Arbeitstag beginnt, bei manueller Eingabe gemäß Randnummer 61;

— nächste Eingabe eines Orts, an dem der aktuelle Arbeitstag beginnt, wenn der Karteninhaber bei der manuellen Eingabe gemäß Randnummer 61 keinen Ort eingibt, an dem der Arbeitstag beginnt oder endete.

Unter den folgenden Bedingungen wird die bei der letzten Kartenentnahme vorgenommene temporäre Eingabe überschrieben und der neue Wert validiert:

— nächste Eingabe eines Orts, an dem der aktuelle Arbeitstag endet, wenn der Karteninhaber bei der manuellen Eingabe gemäß Randnummer 61 keinen Ort eingibt, an dem der Arbeitstag beginnt oder endete."

8. In Abschnitt 3.6.2 erhalten der sechste und der siebte Gedankenstrich folgende Fassung:

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

— für die betreffende Zeit einen Ort einzugeben, an dem der aktuelle Arbeitstag beginnt (wodurch die bei der letzten Kartenentnahme erfolgte temporäre Eingabe validiert wird)."

9. Abschnitt 3.9.15 erhält folgende Fassung:

„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 seit mindestens 30 Tagen kein gültiges GNSS-Signal feststellen konnte."

10. In Abschnitt 3.9.17 wird folgender Gedankenstrich angefügt:

„— (ggf.) Störung der ITS-Schnittstelle"

11. Abschnitt 3.10 wird wie folgt geändert:

i) Der Text vor der Tabelle in Absatz 89 erhält folgende Fassung:

„Mithilfe der Funktion ‚Integrierte Tests und Selbsttests' muss das Kontrollgerät zur Störungserkennung anhand der folgenden Tabelle in der Lage sein:"

ii) In die Tabelle wird die folgende Zeile eingefügt:

„ITS-Schnittstelle (optional)	Ordnungsgemäßer Betrieb"	

12. In Abschnitt 3.12 erhält der zweite Gedankenstrich folgende Fassung:

„— gelten als durchschnittliche Zahl der Positionen je Tag mindestens 6 Positionen, an denen die tägliche Arbeitszeit beginnt, 6 Positionen, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht, und 6 Positionen, an denen die tägliche Arbeitszeit endet, sodass ‚365 Tage' mindestens 6570 Positionen umfassen;"

13. Abschnitt 3.12.5 wird wie folgt geändert:

a) Die Überschrift und Absatz 108 erhalten folgende Fassung:

„3.12.5. Orte und Positionen, an denen die tägliche Arbeitszeit beginnt, endet und/oder eine kumulierte 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 kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht,

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

b) In Absatz 110 erhält der vierte Gedankenstrich folgende Fassung:

„— Art der Eingabe (Beginn, Ende oder kumulierte Lenkzeit von 3 Stunden),"

c) Absatz 111 erhält folgende Fassung:

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

14. Abschnitt 3.12.7 Absatz 116 erhält folgende Fassung:

„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."

15. In Abschnitt 3.12.8 wird die Tabelle wie folgt geändert:

a) Zwischen den Einträgen „Fehlende Positionsdaten des GNSS-Empfängers" und „Bewegungsdatenfehler" wird folgender Eintrag eingefügt:

„Ereignis ‚Kommunikationsfehler mit der externen GNSS-Ausrüstung'	— 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."

b) Der Eintrag „Zeitkonflikt" erhält folgende Fassung:

„Zeitkonflikt	— das schwerwiegendste Ereignis an jedem der letzten 10 Tage des Auftretens (d. h. die Ereignisse mit dem größten Unterschied zwischen Datum und Uhrzeit des Kontrollgeräts und GNSS-Datum und -Uhrzeit), — die 5 schwerwiegendsten Ereignisse in den letzten 365 Tagen.	— Datum und Uhrzeit Kontrollgerät, — 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."

16. Abschnitt 3.20 Absatz 200 erhält folgende Fassung:

„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 VU-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.

Die Zustimmung des Fahrers gilt nicht für die vom Kontrollgerät in das Fahrzeugnetzwerk übertragenen Daten. Werden in das Fahrzeugnetzwerk eingegebene personenbezogene Daten außerhalb des Fahrzeugnetzwerks weiterverarbeitet, muss der Fahrzeughersteller dafür sorgen, dass die Datenverarbeitung der Verordnung (EU) 2016/679 (‚Datenschutz-Grundverordnung') entspricht.

Die Zustimmung des Fahrers gilt auch nicht für Fahrtenschreiberdaten, die in einem entfernt angeschlossenen Unternehmen heruntergeladen werden, (Randnummer 193), da dieses Szenario von den Datenzugriffsrechten der Betriebsart Unternehmen erfasst wird.

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 muss in der Lage sein, den Fahrerzustimmungsstatus an andere Plattformen im Fahrzeugnetzwerk zu übertragen.

Bei eingeschalteter Zündung werden diese Daten ständig ausgesendet."

17. Abschnitt 3.23 Absatz 211 erhält folgende Fassung:

„211) Die Zeit der Systemuhr der Fahrzeugeinheit wird automatisch alle 12 Stunden neu eingestellt. Ist diese Neueinstellung nicht möglich, da 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."

18. In Abschnitt 3.26 erhalten die Absätze 225 und 226 folgende Fassung:

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

— Name und Anschrift des Herstellers,

— Teilnummer und Baujahr,

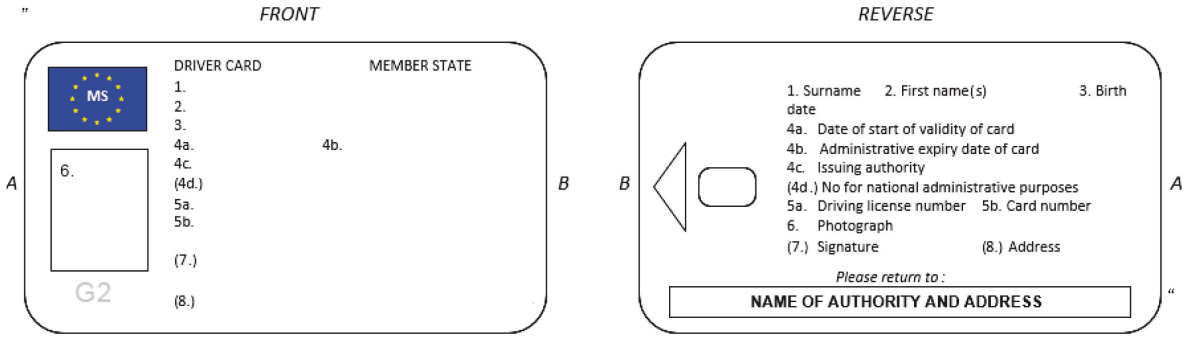
— Seriennummer,

— Typgenehmigungszeichen.

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

19. In Abschnitt 4.1 wird die Zeichnung der Vorder- und Rückseite der Fahrerkarte durch folgende Zeichnung ersetzt:

”



“

20. In Abschnitt 4.5.3.1.8 Absatz 263 erhält der erste Gedankenstrich folgende Fassung:

„— Störung Karte (wenn die Karte Gegenstand der Störung ist),“

21. In Abschnitt 4.5.3.2.8 Absatz 288 erhält der erste Gedankenstrich folgende Fassung:

„— Störung Karte (wenn die Karte Gegenstand der Störung ist),“

22. Abschnitt 4.5.3.2.16 erhält folgende Fassung:

„4.5.3.2.16 Ortsdaten zu drei Stunden kumulierter Lenkzeit

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

— Datum und Uhrzeit, wann die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht,

— Position des Fahrzeugs,

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

— Kilometerstand.

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

23. Abschnitt 4.5.4.2.14 erhält folgende Fassung:

„4.5.4.2.14 Ortsdaten zu drei Stunden kumulierter Lenkzeit

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

— Datum und Uhrzeit, wann die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht,

— Position des Fahrzeugs,

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

— Kilometerstand.

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

24. Abschnitt 5.2 Absatz 396 erhält folgende Fassung:

„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,

— externe GNSS-Ausrüstung (vorhanden/nicht vorhanden),

— ggf. Seriennummer der externen GNSS-Ausrüstung,

— ggf. 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."

25. Abschnitt 5.3 wird wie folgt geändert:

a) Nach Absatz 398 wird ein neuer Absatz 398a eingefügt.

„398a) Die vorstehend genannten Plombierungen müssen nach EN 16882:2016 zertifiziert sein."

b) Absatz 401 Unterabsatz 2 erhält folgende Fassung:

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

c) Absatz 403 erhält folgende Fassung:

„403) Die Plombenhersteller werden in einer speziellen Datenbank registriert, wenn eines ihrer Plombenmodelle nach EN 16882:2016 zertifiziert wird, und veröffentlichen die Nummern der Plomben nach einem von der Europäischen Kommission festzulegenden Verfahren."

d) Absatz 404 erhält folgende Fassung:

„404) Die zugelassenen Werkstätten und Fahrzeughersteller verwenden im Rahmen der Verordnung (EU) Nr. 165/2014 ausschließlich nach EN 16882:2016 zertifizierte Plomben von Herstellern, die in der vorstehend genannten Datenbank registriert sind."

26. Abschnitt 6.2 erhält folgende Fassung:

„6.2 Prüfung neuer oder reparierter Komponenten

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 geprüft."

27. Abschnitt 6.3 Absatz 408 erhält folgende Fassung:

„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. Die Gesamtanlage ist gemäß Kapitel 5.3 zu plombieren und muss eine Kalibrierung umfassen."

28. Abschnitt 8.1 wird wie folgt geändert:

a) In Abschnitt 8.1 erhält der einleitende Text vor Absatz 425 folgende Fassung:

„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 externen 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 jeder anderen Komponente des Kontrollgeräts die Typgenehmigung beantragen, sofern jede Komponente den Vorschriften dieses Anhangs entspricht. Alternativ kann der Hersteller auch die Typgenehmigung für das Kontrollgerät beantragen.

Wie in der Begriffsbestimmung 10 des Artikels 2 dieser Verordnung beschrieben, können die Komponenten der Fahrzeugeinheiten unterschiedlich zusammengestellt sein. Unabhängig von der Zusammenstellung der Fahrzeugeinheitkomponenten sind die externe Antenne und (sofern vorhanden) der mit dem GNSS-Empfänger oder der Fernkommunikationsausrüstung verbundene Antennensplitter nicht Bestandteil der Typgenehmigung der Fahrzeugeinheit.

Gleichwohl müssen Hersteller, die eine Typgenehmigung für das Kontrollgerät erhalten haben, eine öffentlich zugängliche Liste der Antennen und Splitter vorhalten, die mit den Fahrzeugeinheiten, externen GNSS-Ausrüstungen und externen Fernkommunikationsausrüstungen, die über eine Typgenehmigung verfügen, kompatibel sind."

b) Absatz 427 erhält folgende Fassung:

„427) Die Typgenehmigungsbehörden der Mitgliedstaaten erteilen erst dann eine Typgenehmigung, wenn ihnen

— ein Sicherheitszertifikat (sofern nach diesem Anhang erforderlich),

— ein Funktionszertifikat und

— ein Interoperabilitätszertifikat (sofern nach diesem Anhang erforderlich)

für das Kontrollgerät oder die Fahrtenschreiberkarte, für die die Typgenehmigung beantragt wurde, vorliegen."

29. Anlage 1 wird wie folgt geändert:

a) Das Inhaltsverzeichnis wird wie folgt geändert:

i) Nummer 2.63 erhält folgende Fassung:

„2.63. Reserviert für künftige Verwendung"

ii) Nummer 2.78 erhält folgende Fassung:

„2.78. GNSSAccumulatedDriving"

iii) Nummer 2.79 erhält folgende Fassung:

„2.79. GNSSAccumulatedDrivingRecord"

iv) Nummer 2.111 erhält folgende Fassung:

„2.111. NoOfGNSSADRecords"

v) Nummer 2.160 erhält folgende Fassung:

„2.160. Reserviert für künftige Verwendung"

vi) Nummer 2.203 erhält folgende Fassung:

„2.203. VuGNSSADRecord"

vii) Nummer 2.204 erhält folgende Fassung:

„2.204. VuGNSSADRecordArray"

viii) Nummer 2.230 erhält folgende Fassung:

„2.230. Reserviert für künftige Verwendung"

ix) Nummer 2.231 erhält folgende Fassung:

„2.231. Reserviert für künftige Verwendung"

b) In Abschnitt 2 wird vor dem Unterabschnitt 2.1 folgender Wortlaut eingefügt:

„Bei Kartendatentypen, die für Anwendungen der 1. und der 2. Generation verwendet werden, bezieht sich die in dieser Anlage angegebene Größe auf Anwendungen der 2. Generation. Es wird angenommen, dass das Abfragegerät die Größe für Anwendungen der 1. Generation bereits kennt. Die sich auf diese Datentypen beziehenden Randnummern von Anhang IC umfassen Anwendungen der 1. und der 2. Generation."

c) Abschnitt 2.19 erhält folgende Fassung:

„2.19. **CardEventData**

1. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Ereignissen im Zusammenhang mit dem Karteninhaber (Anhang IC Randnummern 260 und 318).

```
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. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Ereignissen im Zusammenhang mit dem Karteninhaber (Anhang IC Randnummern 285 und 341).

```
CardEventData ::= SEQUENCE SIZE(11) 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)."

d) Abschnitt 2.30 erhält folgende Fassung:

„2.30 **CardRenewalIndex**

Ein Kartenerneuerungsindex (Begriffsbestimmung i)).

```
CardRenewalIndex::= IA5String(SIZE(1))
```

Wertzuweisung: (siehe Kapitel 7 in diesem Anhang).

‚0' Erstausstellung.

Reihenfolge für die Erhöhung: ‚0, …, 9, A, …, Z'"

e) In Abschnitt 2.61 erhält der Text nach der Überschrift „2. Generation“ folgende Fassung:

```
„DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

Zusätzlich zur 1. Generation werden folgende Datenelemente verwendet:

noOfGNSSADRecords — Anzahl der kumulierten GNSS-Lenkzeitendatensätze, die die Karte speichern kann.

noOfSpecificConditionRecords — Anzahl der Datensätze mit Bezug auf spezifische Bedingungen, die die Karte speichern kann.

noOfGNSSADRecords — Anzahl der Datensätze mit Informationen zu den genutzten Fahrzeugeinheiten, die die Karte speichern kann.“

f) Abschnitt 2.63 erhält folgende Fassung:

„2.63. **Reserviert für künftige Verwendung**“

g) In Abschnitt 2.67 erhält der Text unter der Überschrift „2. Generation“ folgende Fassung:

„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
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Hinweis 1: 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.

Hinweis 2: Im Feld CardHolderAuthorisation (CHA) eines Zertifikats der 2. Generation sind die Werte (1), (2) und (6) als Angabe eines Zertifikats für die gegenseitige Authentisierung für den jeweiligen Gerätetyp zu verstehen. Zur Angabe des jeweiligen Zertifikats für die Erstellung einer digitalen Signatur sind die Werte (17), (18) oder (19) zu verwenden.“

h) In Abschnitt 2.70 erhält der Text unter der Überschrift „2. Generation“ folgende Fassung:

„2. Generation:

'Ox'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	Datenfehler Weg und Geschwindigkeit,
'0A'H	Datenkonflikt Fahrzeugbewegung,
'0B'H	Zeitkonflikt (zwischen GNSS und Systemuhr der VU),
'0C'H	Kommunikationsfehler mit der Fernkommunikationsausrüstung,
'0D'H	Fehlende Positionsdaten des GNSS-Empfängers
'0E'H	Kommunikationsfehler mit der externen GNSS-Ausrüstung
'0F'H	RFU,
'1x'H	‚Versuch Sicherheitsverletzung‘ an der Fahrzeugeinheit,
'10'H	Keine weiteren Angaben,
'11'H	Fehlgeschlagene Authentisierung des Bewegungssensors,
'12'H	Authentisierungsfehler der Fahrtenschreiberkarte,
'13'H	Unbefugte Veränderung des Bewegungssensors,
'14'H	Integritätsfehler der Kartendateneingabedaten
'15'H	Integritätsfehler der gespeicherten Benutzerdaten,
'16'H	Interner Datenübertragungsfehler,
'17'H	Unberechtigtes Öffnen des Gehäuses,
'18'H	Hardwaremanipulation,
'19'H	Manipulationserkennung beim GNSS,
'1A'H	Authentisierungsfehler der externen GNSS-Ausrüstung,
'1B'H	Abgelaufenes Zertifikat der externen GNSS-Ausrüstung,
'1C'H bis '1F'H	RFU,
'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 bis '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	Interner GNSS-Empfänger,
'37'H	Externe GNSS-Ausrüstung,
'38'H	Fernkommunikationsausrüstung,
'39'H	ITS-Schnittstelle,
'3A'H bis '3F'H	RFU,
'4x'H	Kartenstörungen,
'40'H	Keine weiteren Angaben,
'41'H bis '4F'H	RFU,
'50'H bis '7F'H	RFU,
'80'H bis 'FF'H	Herstellerspezifisch.“

i) Abschnitt 2.71 erhält folgende Fassung:

„2.71. **ExtendedSealIdentifier**

2. Generation:

Der erweiterte Plombenbezeichner dient der eindeutigen Identifizierung von Plomben (Anhang IC Randnummer 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                OCTET STRING (SIZE(2)),
   sealIdentifier                  OCTET STRING (SIZE(8))
}
```

manufacturerCode — ein Code des Plombenherstellers.

sealIdentifier — ein Bezeichner für die Plombe, der für den Hersteller eindeutig sein muss."

j) Die Abschnitte 2.78 und 2.79 erhalten folgende Fassung:

„2.78 **GNSSAccumulatedDriving**

2. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Informationen im Zusammenhang mit der GNSS-Position des Fahrzeugs, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht (Anhang IC Randnummern 306 und 354).

```
GNSSAccumulatedDriving := SEQUENCE {
   gnssADPointerNewestRecord       INTEGER(0..NoOfGNSSADRecords -1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord — Index des zuletzt aktualisierten kumulierten GNSS-Lenkzeitendatensatzes.

Wertzuweisung — Zahl, die dem Zähler des kumulierten GNSS-Lenkzeitendatensatzes entspricht, beginnend mit ‚0' für das erste Auftreten des kumulierten GNSS-Lenkzeitendatensatzes in der Struktur.

gnssAccumulatedDrivingRecords — Datensätze mit Datum und Uhrzeit, wann die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht, sowie Informationen zur Position des Fahrzeugs.

2.79. **GNSSAccumulatedDrivingRecord**

2. Generation:

Auf einer Fahrer- oder Werkstattkarte gespeicherte Informationen im Zusammenhang mit der GNSS-Position des Fahrzeugs, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht (Anhang IC Randnummern 305 und 353).

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                    TimeReal,
  gnssPlaceRecord              GNSSPlaceRecord,
  vehicleOdometerValue         OdometerShort
}
```

timeStamp — Datum und Uhrzeit, wann die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht.

gnssPlaceRecord — Informationen zur Position des Fahrzeugs.

vehicleOdometerValue — Kilometerstand, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht."

k) Abschnitt 2.86 erhält folgende Fassung:

„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, einer Fahrtenschreiberkarte oder einer externen GNSS-Ausrüstung.

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.“

l) Abschnitt 2.92 erhält folgende Fassung:

„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(16)),
}“;
```

m) Abschnitt 2.111 erhält folgende Fassung:

„2.111. **NoOfGNSSADRecords**

2. Generation:

Anzahl der kumulierten GNSS-Lenkzeitendatensätze, die die Karte speichern kann.

$$\texttt{NoOfGNSSADRecords ::= INTEGER (0..}2^{16}\texttt{-1)}$$

Wertzuweisung: siehe Anlage 2.“

n) In Abschnitt 2.120 Absatz 1 erhält die Wertzuweisung „16H“ folgende Fassung:

„'16'H VuGNSSADRecord “

o) Abschnitt 2.160 erhält folgende Fassung:

„2.160. **Reserviert für künftige Verwendung**“

p) Abschnitt 2.162 erhält folgende Fassung:

„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. UTC ausgedrückt sind.

```
TimeReal {INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)
```

Wertzuweisung — Oktettanordnung: Anzahl der Sekunden seit dem 1. Januar 1970, 0.00 Uhr UTC.

Spätestmögliche(s) Datum/Uhrzeit ist im Jahr 2106."

q) Abschnitt 2.179 erhält folgende Fassung:

„2.179 **VuCardRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Information zu einer verwendeten Fahrtenschreiberkarte (Anhang IC Randnummer 132).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation — vollständige Kartennummer und Generation der verwendeten Karte (Datentyp 2.74).

cardExtendedSerialNumber — ausgelesen aus der Datei EF_ICC unter MF der Karte.

cardStructureVersion — ausgelesen aus der Datei EF_Application_Identification unter DF_Tachograph_G2.

cardNumber — ausgelesen aus der Datei EF_Identification unter DF_Tachograph_G2."

r) Die Abschnitte 2.203 und 2.204 erhalten folgende Fassung:

„2.203 **VuGNSSADRecord**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Informationen zur GNSS-Position des Fahrzeugs, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht (Anhang IC Randnummern 108 und 110).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp — Datum und Uhrzeit, wann die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht.

cardNumberAndGenDriverSlot — identifiziert die im Steckplatz Fahrer eingesteckte Karte und ihre Generation.

cardNumberAndGenCodriverSlot — identifiziert die im Steckplatz Beifahrer eingesteckte Karte und ihre Generation.

gnssPlaceRecord — Informationen zur Position des Fahrzeugs.

vehicleOdometerValue — Kilometerstand, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht.

2.204. **VuGNSSADRecordArray**

2. Generation:

In einer Fahrzeugeinheit gespeicherte Informationen zur GNSS-Position des Fahrzeugs, wenn die kumulierte Lenkzeit ein Vielfaches von drei Stunden erreicht (Anhang IC Randnummern 108 und 110).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType — Art des Datensatzes (VuGNSSADRecord).

Wertzuweisung: siehe RecordType.

recordSize — die Größe von VuGNSSADRecord in Byte.

noOfRecords — Anzahl der Datensätze in der Menge der Datensätze.

records — Menge der kumulierten GNSS-Lenkzeitendatensätze.“

s) Die Abschnitte 2.230 und 2.231 erhalten folgende Fassung:

„2.230. Reserviert für künftige Verwendung.

2.231. Reserviert für künftige Verwendung“

t) In Abschnitt 2.234 erhält der Text unter der Überschrift „2. Generation“ folgende Fassung:

```
„WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId               EquipmentType,
    cardStructureVersion                 CardStructureVersion,
    noOfEventsPerType                    NoOfEventsPerType,
    noOfFaultsPerType                    NoOfFaultsPerType,
    activityStructureLength              CardActivityLengthRange,
    noOfCardVehicleRecords               NoOfCardVehicleRecords,
    noOfCardPlaceRecords                 NoOfCardPlaceRecords,
    noOfCalibrationRecords               NoOfCalibrationRecords,
    noOfGNSSADRecords                    NoOfGNSSADRecords,
    noOfSpecificConditionRecords         NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords           NoOfCardVehicleUnitRecords
}
```

Zusätzlich zur 1. Generation werden folgende Datenelemente verwendet:

noOfGNSSADRecords — Anzahl der kumulierten GNSS-Lenkzeitendatensätze, die die Karte speichern kann.

noOfSpecificConditionRecords — Anzahl der Datensätze mit Bezug auf spezifische Bedingungen, die die Karte speichern kann.

noOfCardVehicleUnitRecords — Anzahl der Datensätze mit Informationen zu den genutzten Fahrzeugeinheiten, die die Karte speichern kann."

30. Anlage 2 wird wie folgt geändert:

a) In Abschnitt 1.1 werden folgende Abkürzungen eingefügt:

„CHA Certificate Holder Authorisation (Autorisierung des Zertifikatsinhabers)

DO Datenobjekt"

b) Abschnitt 3.3 wird wie folgt geändert:

i) Der Absatz TCS_24 erhält folgende Fassung:

„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. Der Ausdruck ‚Nicht zutreffend' wird verwendet, wenn der Befehl von keiner Randnummer unterstützt wird. Der Befehl kann dann gegebenenfalls unterstützt werden, aber die Zugriffsbedingung ist nicht anwendbar."

ii) Die Tabelle in Absatz TCS_25 erhält folgende Fassung:

„Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmenskarte
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

„Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmenskarte
PERFORM 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“

iii) Die Tabelle in Absatz TCS_26 erhält folgende Fassung:

„Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmenskarte
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
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	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
PERFORM 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“

iv) Die Tabelle in Absatz TCS_27 erhält folgende Fassung:

„Befehl	Fahrerkarte	Werkstattkarte	Kontrollkarte	Unternehmenskarte
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
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	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PSO: Hash	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PERFORM HASH OF FILE	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Verify	Nicht zutreffend	ALW	Nicht zutreffend	Nicht zutreffend“

c) In Abschnitt 3.4 erhält der Absatz TCS_29 folgende Fassung:

„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‘.

SW1	SW2	Bedeutung
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	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)
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

Weitere in ISO/IEC 7816-4 definierte Statusbytes können zurückgesendet werden, wenn ihr Verhalten in dieser Anlage nicht ausdrücklich erwähnt wird.

Zum Beispiel können die folgenden Statusbytes optional zurückgesendet werden:

6881: Logischer Kanal nicht unterstützt

6882: Secure Messaging nicht unterstützt“

d) In Abschnitt 3.5.1.1 Absatz TCS_38 erhält der letzte Gedankenstrich folgende Fassung:

„— Wird die ausgewählte Anwendung als verfälscht betrachtet (weil in den Dateiattributen ein Integritätsfehler festgestellt wurde), lautet der zurückgesendete Verarbeitungsstatus ‚**6400**‘ oder ‚**6500**‘.“

e) In Abschnitt 3.5.1.2 Absatz TCS_41 erhält der letzte Gedankenstrich folgende Fassung:

„— Wird die ausgewählte Datei als verfälscht betrachtet (weil in den Dateiattributen ein Integritätsfehler festgestellt wurde), lautet der zurückgesendete Verarbeitungsstatus ‚**6400**‘ oder ‚**6500**‘.“

f) In Abschnitt 3.5.2.1 Absatz TCS_43 erhält der sechste Gedankenstrich folgende Fassung:

„— 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 ‚**6500**‘.“

g) Abschnitt 3.5.2.1.1 wird wie folgt geändert:

i) Die Tabelle in Absatz TCS_45 erhält folgende Fassung:

„Byte	Länge	Wert	Beschreibung
#1	1	‚81h‘	T_{PV}: Tag für 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‘	Klardatenwert
#(2+L+NN)	1	‚99h‘	Tag für Verarbeitungsstatus (SW1-SW2) — optional für Secure Messaging der 1. Generation
#(3+L+NN)	1	‚02h‘	Länge des Verarbeitungsstatus — optional für Secure Messaging der 1. Generation
#(4+L+NN) - #(5+L+NN)	2	‚XX XXh‘	Verarbeitungsstatus der ungeschützten APDU-Antwort — optional für Secure Messaging der 1. Generation
#(6+L+NN)	1	‚8Eh‘	TCC: Tag für kryptografische Prüfsumme
#(7+L+NN)	1	‚XXh‘	LCC: 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)

Byte	Länge	Wert	Beschreibung
#(8+L+NN) - #(7+M+L+NN)	M	‚XX..XXh'	Kryptografische Prüfsumme
SW	2	‚XXXXh'	Statusbytes (SW1, SW2)"

ii) Die Tabelle in Absatz TCS_46 erhält folgende Fassung:

„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 LPI 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 — optional für Secure Messaging der 1. Generation
#(4+L+MM) - #(5+L+MM)	2	‚XX XXh'	Verarbeitungsstatus der ungeschützten APDU-Antwort – optional für Secure Messaging der 1. Generation
#(6+L+MM)	1	‚8Eh'	TCC: Tag für kryptografische Prüfsumme
#(7+L+MM)	1	‚XXh'	LCC: 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)"

h) In Abschnitt 3.5.2.2 Absatz TCS_50 erhält der sechste Gedankenstrich folgende Fassung:

„— 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 ‚**6500**'."

i) Abschnitt 3.5.2.3 Absatz TCS_52 wird wie folgt geändert:

i) Die letzte Zeile der Tabelle erhält folgende Fassung:

„Le	1	‚XXh'	Gemäß ISO/IEC 7816-4"

ii) Folgender Satz wird angefügt:

„Ist T=0, geht die Karte vom Wert Le = ‚00h' aus, sofern kein Secure Messaging angewandt wird.

Bei T=1 lautet der zurückgesendete Verarbeitungsstatus ‚6700', falls Le= ‚01h'."

j) In Abschnitt 3.5.2.3 Absatz TCS_53 erhält der sechste Gedankenstrich folgende Fassung:

„— 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 ‚**6500**'."

k) In Abschnitt 3.5.3.2 Absatz TCS_63 erhält der sechste Gedankenstrich folgende Fassung:

„— 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 ‚**6500**'."

l) In Abschnitt 3.5.5 erhält der Absatz TCS_72 folgende Fassung:

„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)."

m) Abschnitt 3.5.8 Absatz TCS_95 erhält folgende Fassung:

„TCS_95 Ist der Befehl INTERNAL AUTHENTICATE erfolgreich, wird der aktuelle Sitzungsschlüssel der 1. Generation, sofern vorhanden, gelöscht und ist nicht mehr verfügbar. Um einen neuen Sitzungsschlüssel der 1. Generation zur Verfügung zu haben, muss der Befehl EXTERNAL AUTHENTICATE für den Authentisierungsmechanismus der 1. Generation erfolgreich ausgeführt werden.

Hinweis: Für Sitzungsschlüssel der 2. Generation siehe Anlage 11 CSM_193 und CSM_195. Werden Sitzungsschlüssel der 2. Generation erstellt und erhält die Fahrtenschreiberkarte den APDU-Klartextbefehl INTERNAL AUTHENTICATE, bricht sie die Secure-Messaging-Sitzung der 2. Generation ab und vernichtet die Sitzungsschlüssel der 2. Generation."

n) Abschnitt 3.5.9 Absatz TCS_97 erhält folgende Fassung:

„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). Ist der Befehl EXTERNAL AUTHENTICATE der 2. Generation erfolgreich, wird der aktuelle Sitzungsschlüssel der 1. Generation, sofern vorhanden, gelöscht und ist nicht mehr verfügbar.

Hinweis: Für Sitzungsschlüssel der 2. Generation siehe Anlage 11 CSM_193 und CSM_195. Werden Sitzungsschlüssel der 2. Generation erstellt und erhält die Fahrtenschreiberkarte den APDU-Klartextbefehl EXTERNAL AUTHENTICATE, bricht sie die Secure-Messaging-Sitzung der 2. Generation ab und vernichtet die Sitzungsschlüssel der 2. Generation."

o) In Abschnitt 3.5.10 Absatz TCS_101 wird in der Tabelle die folgende Zeile angefügt:

„5 + L + 1	1	‚00h'	Gemäß ISO/IEC 7816-4"

p) In Abschnitt 3.5.11.2.3 Absatz TCS_114 werden folgende Unterabsätze angefügt:

„— Weist der Wert currentAuthenticatedTime der Karte einen späteren Zeitpunkt als das Ablaufdatum des ausgewählten öffentlichen Schlüssels auf, lautet der zurückgesendete Verarbeitungsstatus ‚**6A88**'.

Hinweis: Im Fall eines Befehls MSE:SET AT für die VU-Authentisierung ist der Schlüssel, auf den verwiesen wird, ein öffentlicher VU_MA-Schlüssel. Die Karte legt, falls in ihrem Speicher vorhanden, den öffentlichen VU_MA-Schlüssel für die Nutzung fest, der der im Befehlsdatenfeld angegebenen Referenz des Zertifikatinhabers (Certificate Holder Reference, CHR) entspricht (die Karte kann öffentliche VU_MA-Schlüssel anhand des CHA-Felds des Zertifikats identifizieren). Die Karte sendet ‚6A 88' auf diesen Befehl zurück, falls nur der öffentliche Schlüssel VU_Sign oder kein öffentlicher Schlüssel der Fahrzeugeinheit verfügbar ist. Siehe die Definition des CHA-Felds in Anlage 11 sowie des Datentyps EquipmentType in Anlage 1.

Ebenso ist der Schlüssel, auf den verwiesen wird, immer ein EQT_Sign-Schlüssel, der für die Verifizierung einer digitalen Signatur zu verwenden ist, wenn ein Befehl MSE: SET DST, der auf ein Gerät (EQT) (d. h. auf eine Fahrzeugeinheit oder Karte) verweist, an eine Kontrollkarte gesendet wird. Nach Anlage 11 Abbildung 13 hat die Kontrollkarte den relevanten öffentlichen Schlüssel EQT_Sign immer gespeichert. In manchen Fällen kann die Kontrollkarte auch den entsprechenden öffentlichen Schlüssel EQT_MA gespeichert haben. Die Kontrollkarte muss den zu verwendenden öffentlichen Schlüssel EQT_Sign immer festlegen, wenn sie einen Befehl MSE: SET DST erhält."

q) Abschnitt 3.5.13 wird wie folgt geändert:

i) Der Absatz TCS_121 erhält folgende Fassung:

„TCS_121 Der temporär gespeicherte ‚hash of file'-Wert ist zu löschen, wenn mithilfe des Befehls PERFORM HASH of FILE ein neuer Hashwert berechnet wird, wenn ein DF ausgewählt wird und wenn die Fahrtenschreiberkarte zurückgesetzt wird."

ii) Der Absatz TCS_123 erhält folgende Fassung:

„TCS_123 Die Fahrtenschreiberanwendung der 2. Generation muss den Algorithmus SHA-2, SHA-256, SHA-384 oder SHA-512 unterstützen, der durch die Cipher Suite in Anlage 11 Teil B für den Kartensignaturschlüssel Card_Sign spezifiziert wird."

iii) Die Tabelle in Absatz TCS_124 erhält folgende Fassung:

„Byte	Länge	Wert	Beschreibung
CLA	1	‚80h'	CLA
INS	1	‚2Ah'	Perform Security Operation
P1	1	‚90h'	Tag: Hash
P2	1	‚00h'	Algorithmus implizit bekannt Für die Fahrtenschreiberanwendung der 1. Generation: SHA-1 Für die Fahrtenschreiberanwendung der 2. Generation: SHA-2-Algorithmus (SHA-256, SHA-384 oder SHA-512) entsprechend der Cipher Suite in Anlage 11 Teil B für den Kartensignaturschlüssel Card_Sign"

r) Abschnitt 3.5.14 wird wie folgt geändert:

Der Text unter der Überschrift bis Absatz TCS_126 erhält folgende Fassung:

„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. Im Falle einer Fahrtenschreiberanwendung der 2. Generation haben nur die Fahrerkarte und die Werkstattkarte einen Signaturschlüssel der 2. Generation, während andere Karten den Befehl nicht erfolgreich ausführen können und mit einem geeigneten Fehlercode abschließen.

Der Befehl kann in MF gegebenenfalls zur Verfügung stehen. Steht der Befehl in MF nicht zur Verfügung, schließt er mit einem geeigneten Fehlercode ab.

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-8. Die Verwendung des Befehls ist jedoch im Vergleich zur entsprechenden Norm eingeschränkt."

s) Abschnitt 3.5.15 wird wie folgt geändert:

i) Die Tabelle in Absatz TCS_133 erhält folgende Fassung:

„Byte	Länge	Wert	Beschreibung
CLA	1	‚00h'	CLA
INS	1	‚2Ah'	Perform Security Operation
P1	1	‚00h'	
P2	1	‚A8h'	Tag: Datenfeld enthält für die Verifizierung relevante DO
Lc	1	‚XXh'	Länge Lc des nachfolgenden Datenfelds
#6	1	‚9Eh'	Tag für digitale Signatur
#7 oder #7 – #8	L	‚NNh' oder ‚81 NNh'	Länge der digitalen Signatur (L gleich 2 Bytes, wenn die Länge der digitalen Signatur mehr als 127 Bytes beträgt): 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).
#(7+L) – #(6+L+NN)	NN	‚XX..XXh'	Inhalt der digitalen Signatur"

ii) In Absatz TCS_134 wird folgender Gedankenstrich angefügt:

„— Weist der (zur Verifizierung der digitalen Signatur verwendete) ausgewählte öffentliche Schlüssel einen CHA.LSB (CertificateHolderAuthorisation.equipmentType) auf, der nicht für die Verifizierung der digitalen Signatur gemäß Anlage 11 geeignet ist, lautet der zurückgesendete Verarbeitungsstatus ‚**6985**'."

t) Abschnitt 3.5.16 wird wie folgt geändert:

i) In Absatz TCS_138 wird in die Tabelle die folgende Zeile eingefügt:

„5 + L + 1	1	‚00h'	Gemäß ISO/IEC 7816-4"

ii) In Absatz TCS_139 wird folgender Unterabsatz angefügt:

„— ‚**6985**' gibt an, dass der 4-Byte-Zeitstempel im Befehlsdatenfeld vor dem Zeitpunkt cardValidityBegin oder nach dem cardExpiryDate liegt."

u) Abschnitt 4.2.2 wird wie folgt geändert:

i) In der Datenstruktur in Absatz TCS_154 erhalten die Zeilen von DF Tachograph G2 bis EF CardMA_Certificate sowie die Zeilen von EF GNSS_Places bis zum Ende des Absatzes folgende Fassung:

"

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
└DF Tachograph_G2		*20268*	*40316*	
├EF Application_Identification		*17*	*17*	
└DriverCardApplicationIdentification		*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 00}
├noOfGNSSADRecords		2	2	{00 00}
├noOfSpecificConditionRecords		2	2	{00 00}
└noOfCardVehicleUnitRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	

...

EF GNSS_Places		*4538*	*6050*	
└GNSSContinuousDriving		*4538*	*6050*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		4536	6048	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
└vehicleOdometerValue		3	3	{00..00}

"

ii) In Absatz TCS_155 erhält der Punkt NoOfGNSSCDRecords der Tabelle folgende Fassung:

„n_8	NoOfGNSSADRecords	252	336“

v) In Abschnitt 4.3.1 Absatz TCS_156 erhält der Text zur Abkürzung SC4 folgende Fassung:

„**SC4** Für den Befehl READ BINARY mit geradem INS-Byte:

(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“

w) Abschnitt 4.3.2 wird wie folgt geändert:

i) In der Datenstruktur in Absatz TCS_162 erhalten die Zeilen von DF Tachograph G2 bis EF CardMA_Certificate, die Zeilen von EF Calibration bis extendedSealIdentifier und die Zeilen von EF GNSS_Places bis vehicleOdometerValue folgende Fassung:

”

Datei/Datenelement	Anzahl Datensätze	Größe (Bytes) Min.	Max.	Standardwerte
DF Tachograph_G2	*1878*		*49787*	
EF Application_Identification	*19*		*19*	
WorkshopCardApplicationIdentificatio	*19*		*19*	
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 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	*204*		*341*	
...				
EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
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		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

“

ii) Der Eintrag NoOfGNSSCDRecords der Tabelle in Absatz TCS_163 erhält folgende Fassung:

„n_8	NoOfGNSSADRecords	18	24“

31. Anlage 3 Abschnitt 2 wird wie folgt geändert:

a) Nach der Zeile mit den Piktogrammen „Ort des Beginns des Arbeitstages“ und „Ort des Endes des Arbeitstages“ wird folgende Zeile eingefügt:

„ Position nach 3 Stunden kumulierter Lenkzeit“

b) Die Piktogrammkombination „Zeiteinstellung (durch Werkstatt)“ erhält folgende Fassung:

„ Zeitkonflikt oder Zeiteinstellung (durch Werkstatt)“

c) Der Ereignisliste werden folgende Piktogrammkombinationen hinzugefügt:

„ Fehlende Positionsdaten des GNSS-Empfängers oder Kommunikationsfehler mit der externen GNSS-Ausrüstung

Kommunikationsfehler mit der Fernkommunikationsausrüstung“

32. Anlage 4 wird wie folgt geändert:

a) Abschnitt 2 wird wie folgt geändert:

i) Block Nummer 11.4 erhält folgende Fassung:

„11.4 *Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages*

pi = Piktogramm Ort Beginn/Ende, Uhrzeit, Land, Region	pihh:mm Cou Reg
Längengrad der aufgezeichneten Position	lon ±DDD°MM.M’
Breitengrad der aufgezeichneten Position	lat ± DD°MM.M’
Zeitstempel der Positionsfeststellung	hh:mm
Kilometerstand	x xxx xxx **km**“

ii) Block Nummer 11.5 erhält folgende Fassung:

„11.5 *Positionen nach 3 Stunden kumulierter Lenkzeit*
pi=Position nach 3 Stunden kumulierter Lenkzeit
Längengrad der aufgezeichneten Position
Breitengrad der aufgezeichneten Position
Zeitstempel der Positionsfeststellung
Kilometerstand

```
pihh:mm
lon  ± DDD°MM.M'
lat ± DD°MM.M '
hh:mm
x xxx xxx km“
```

b) In Abschnitt 3.1 erhält Punkt 11.5 zum Format des täglichen Ausdrucks folgende Fassung:

„11.5	Positionen nach 3 Stunden kumulierter Lenkzeit in chronologischer Reihenfolge“

c) In Abschnitt 3.2 erhält das Format des täglichen Ausdrucks folgende Fassung:

„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 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	Positionen nach 3 Stunden kumulierter Lenkzeit in chronologischer Reihenfolge
11.7	Gesamtwerte Tätigkeiten
11.2	Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Beifahrer
11.4	Eingegebene Orte in chronologischer Reihenfolge
11.5	Positionen nach 3 Stunden kumulierter Lenkzeit in chronologischer Reihenfolge

11.8	Gesamtwerte Tätigkeiten
11.3	Zusammenfassung der Tätigkeiten für einen Fahrer, beide Steckplätze
11.4	Von diesem Fahrer eingegebene Orte in chronologischer Reihenfolge
11.5	Positionen nach 3 Stunden kumulierter Lenkzeit in chronologischer Reihenfolge
11.9	Gesamtwerte Tätigkeiten für diesen Fahrer
13.1	Begrenzungszeichen Ereignisse/Störungen
13.4	Datensätze Ereignis/Störung (die letzten 5 in der VU gespeicherten oder andauernden Ereignisse/Störungen)
22.1	Kontrollort
22.2	Unterschrift des Kontrolleurs
22.3	Anfangszeit (Platz für die Angabe der zutreffenden Zeitabschnitte durch einen Fahrer ohne Karte)
22.4	Endzeit
22.5	Unterschrift des Fahrers“

d) In Abschnitt 3.7 erhält der Absatz PRT_014 folgende Fassung:

„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“

33. Anlage 7 wird wie folgt geändert:

a) Abschnitt 1.1 erhält folgende Fassung:

„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.

Daten, die von einer VU heruntergeladen werden, werden gemäß Anlage 11 (Gemeinsame Sicherheitsmechanismen Teil B, Fahrtenschreibersystem der 2. Generation) unterzeichnet, außer wenn Fahrer von einer Nicht-EU-Kontrollbehörde mit einer Kontrollkarte der 1. Generation kontrolliert werden; in diesem Fall werden die Daten im Einklang mit Anlage 15 (Migration) Randnummer MIG_015 gemäß Anlage 11 (Gemeinsame Sicherheitsmechanismen Teil A, Fahrtenschreibersystem der 1. Generation) unterzeichnet.

In dieser Anlage werden daher zwei Arten des Datendownloads von VU spezifiziert:

— VU-Datendownload der 2. Generation mit Datenstruktur der 2. Generation und Unterzeichnung gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen Teil B,

— VU-Datendownload der 1. Generation mit Datenstruktur der 1. Generation und Unterzeichnung gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen Teil A.

Ebenso gibt es, wie in den Abschnitten 3 und 4 dieser Anlage ausgeführt, zwei Arten von Datendownloads von in VU eingesetzten Fahrerkarten der 2. Generation."

b) Abschnitt 2.2.2 wird wie folgt geändert:

i) Die Tabelle erhält folgende Fassung:

„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 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	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
Transfer Data Request								
Overview	80	EE	F0	02	36	01 oder 21		97
Activities	80	EE	F0	06	36	02 oder 22	Datum	CS
Events & Faults	80	EE	F0	02	36	03 oder 23		99
Detailed Speed	80	EE	F0	02	36	04 oder 24		9A
Technical Data	80	EE	F0	02	36	05 oder 25		9B
Card download	80	EE	F0	02	36	06	Slot	CS

Nachrichtenstruktur	Max. 4 Bytes Kopf				Max. 255 Bytes Daten			1 Byte Prüfsumme
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	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“

ii) Den Anmerkungen nach der Tabelle werden folgende Gedankenstriche angefügt:

„— TRTP 21 bis 25 werden für VU-Datendownload-Anforderungen der 2. Generation verwendet und TRTP 01 bis 05 für Anfragen für VU-Datendownload-Anforderungen der 1. Generation, die von der VU nur akzeptiert werden können, wenn Fahrer von einer Nicht-EU-Kontrollbehörde mit einer Kontrollkarte der 1. Generation kontrolliert werden.

— TRTP 11 bis 19 und 31 bis 39 sind für herstellerspezifische Download-Anforderungen reserviert.“

c) Abschnitt 2.2.2.9 wird wie folgt geändert:

i) Absatz DDP_011 erhält folgende Fassung:

„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. Beim VU-Datendownload können für jede Übertragungsart zwei unterschiedliche TRTP-Werte verwendet werden:

Datenübertragungsart	TRTP-Wert für VU-Datendownloads der 1. Generation	TRTP-Wert für VU-Datendownloads der 2. Generation
Überblick	01	21
Tätigkeiten eines bestimmten Tages	02	22
Ereignisse und Störungen	03	23
Genaue Geschwindigkeitsangaben	04	24
Technische Daten	05	25

Datenübertragungsart	TRTP-Wert
Kartendownload	06“

ii) Absatz DDP_054 erhält folgende Fassung:

„DDP_054 Die IDE muss beim Herunterladen eine Überblicks-Datenübertragung (TRTP 01 oder 21) 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 oder 22) schließt die Nachricht Transfer Data Request die Angabe des herunterzuladenden Kalendertags (Format `TimeReal`) ein.“

d) Abschnitt 2.2.2.10 Absatz DDP_055 erhält folgende Fassung:

„DDP_055 Im ersten Fall (TREP 01 oder 21) 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.“

e) Abschnitt 2.2.2.16 Absatz DDP_018 letzter Gedankenstrich erhält folgende Fassung:

„— FA data not available

Das Datenobjekt einer Datenübertragungsanforderung ist in der VU nicht verfügbar (z. B. keine Karte eingesetzt, VU-Datendownload-Anforderung der 1. Generation außerhalb des Rahmens von Fahrerkontrollen durch eine Nicht-EU-Kontrollbehörde, …).“

f) Abschnitt 2.2.6.1 wird wie folgt geändert:

i) Absatz DDP_029 Unterabsatz 1 erhält folgende Fassung:

„Das Datenfeld der Nachricht Positive Response Transfer Data Overview liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 01 oder 21 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:“

ii) Die Überschrift „Datenstruktur der 1. Generation“ erhält folgende Fassung:

„Datenstruktur der 1. Generation (TREP 01 Hex)“

iii) Die Überschrift „Datenstruktur der 2. Generation“ erhält folgende Fassung:

„Datenstruktur der 2. Generation (TREP 21 Hex)“

g) Abschnitt 2.2.6.2 wird wie folgt geändert:

i) Absatz DDP_030 Unterabsatz 1 erhält folgende Fassung:

„Das Datenfeld der Nachricht Positive Response Transfer Data Activities liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 02 oder 22 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:“

ii) Die Überschrift „Datenstruktur der 1. Generation“ erhält folgende Fassung:

„Datenstruktur der 1. Generation (TREP 02 Hex)“

iii) Die Überschrift „Datenstruktur der 2. Generation“ erhält folgende Fassung:

„Datenstruktur der 2. Generation (TREP 22 Hex)“

iv) Der Eintrag VuGNSSCDRecordArray unter der Überschrift „Datenstruktur der 2. Generation (TREP 22 Hex)“ erhält folgende Fassung:

„VuGNSSADRecordArray	GNSS-Position des Fahrzeugs, wenn die kumulierte Lenkzeit des Fahrzeugs ein Vielfaches von drei Stunden erreicht. Ist der Abschnitt leer, wird ein Array-Kopf mit noOfRecords = 0 gesendet.“

h) Abschnitt 2.2.6.3 wird wie folgt geändert:

i) Absatz DDP_031 Unterabsatz 1 erhält folgende Fassung:

„Das Datenfeld der Nachricht Positive Response Transfer Data Events and Faults liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 03 oder 23 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:“

ii) Die Überschrift „Datenstruktur der 1. Generation“ erhält folgende Fassung:

„Datenstruktur der 1. Generation (TREP 03 Hex)“

iii) Die Überschrift „Datenstruktur der 2. Generation“ erhält folgende Fassung:

„Datenstruktur der 2. Generation (TREP 23 Hex)“

iv) Der Eintrag VuTimeAdjustmentGNSSRecordArray unter der Überschrift „Datenstruktur der 2. Generation (TREP 23 Hex)“ wird gestrichen.

i) Abschnitt 2.2.6.4 wird wie folgt geändert:

i) Absatz DDP_032 Unterabsatz 1 erhält folgende Fassung:

„Das Datenfeld der Nachricht Positive Response Transfer Data Detailed Speed liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 04 oder 24 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:“

ii) Die Überschrift „Datenstruktur der 1. Generation“ erhält folgende Fassung:

„Datenstruktur der 1. Generation (TREP 04)“

iii) Die Überschrift „Datenstruktur der 2. Generation“ erhält folgende Fassung:

„Datenstruktur der 2. Generation (TREP 24)“

j) Abschnitt 2.2.6.5 wird wie folgt geändert:

i) Absatz DDP_033 Unterabsatz 1 erhält folgende Fassung:

„Das Datenfeld der Nachricht Positive Response Transfer Data Technical Data liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 05 oder 25 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:“

ii) Die Überschrift „Datenstruktur der 1. Generation“ erhält folgende Fassung:

„Datenstruktur der 1. Generation (TREP 05)“

iii) Die Überschrift „Datenstruktur der 2. Generation“ erhält folgende Fassung:

„Datenstruktur der 2. Generation (TREP 25)“

k) Abschnitt 3.3 Absatz DDP_035 erhält folgende Fassung:

„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.

— (für Fahrtenschreiberkarten der 1. und 2. Generation) Herunterladen der EF innerhalb der `Tachograph DF`:

— Herunterladen der EF `Card_Certificate` 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 `Tachograph DF`) außer EF `Card_Download`. Diese Informationen werden mit einer digitalen Signatur gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen Teil B gesichert.

— Bei jedem Download-Vorgang ist zumindest das Herunterladen der EF `Application_Identification` und `Identification` obligatorisch.

— Beim Herunterladen einer Fahrerkarte ist zudem der Download folgender EF obligatorisch:

— `Events_Data`,

— `Faults_Data`,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— (nur für Fahrtenschreiberkarten der 2. Generation) Herunterladen der EF innerhalb der Tachograph_G2 DF, außer im Fall von Datendownloads einer in eine VU eingesteckten Fahrerkarte bei Kontrollen durch eine Nicht-EU-Kontrollbehörde mit einer Kontrollkarte der 1. Generation:

— Herunterladen der EF CardSignCertificate, CA_Certificate und Link_Certificate (falls vorhanden). 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 Tachograph_G2 DF) außer EF Card_Download. Diese Informationen werden mit einer digitalen Signatur gemäß Anlage 11 Gemeinsame Sicherheitsmechanismen Teil B gesichert.

— Bei jedem Download-Vorgang ist zumindest das Herunterladen der EF Application_Identification und Identification obligatorisch.

— Beim Herunterladen einer Fahrerkarte ist zudem der Download folgender EF obligatorisch:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— VehicleUnits_Used,

— GNSS Places.

— Beim Herunterladen einer Fahrerkarte wird das Datum LastCardDownload in der EF Tachograph und DF Tachograph und gegebenenfalls Tachograph_G2 aktualisiert.

— Beim Herunterladen einer Werkstattkarte ist der Kalibrierungszähler in der EF Card_Download in den DF Tachograph und gegebenenfalls Tachograph_G2 zurückzusetzen.

— Beim Herunterladen einer Werkstattkarte ist `Sensor_Installation_Data` in den DF `Tachograph` und gegebenenfalls `Tachograph_G2` nicht herunterzuladen."

l) Abschnitt 3.3.2 Unterabsatz 1 Absatz DDP_037 erhält folgende Fassung:

„Die Sequenz für das Herunterladen der EF ICC, IC, Card_Certificate (oder CardSignCertificate für DF Tachograph_G2), CA_Certificate und Link_Certificate (nur für DF Tachograph_G2) lautet folgendermaßen:"

m) Die Tabelle in Abschnitt 3.3.3 erhält folgende Fassung:

„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 Teil A oder B. 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"

n) Abschnitt 3.4.2 Absatz DDP_046 erhält folgende Fassung:

„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) in Tachograph oder für gemeinsame Informationen der Karte	3 Bytes
FID (2 Bytes) || ‚01'	Tag für Signatur der EF (FID) in DF Tachograph	3 Bytes
FID (2 Bytes) || ‚02'	Tag für Signatur der EF (FID) in DF Tachograph_G2	3 Bytes
FID (2 Bytes) || ‚03'	Tag für Signatur der EF (FID) in DF Tachograph_G2	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 (in DF Tachograph)
05 05 01	00 80	Signatur von EF Vehicles_Used (in DF Tachograph)
05 05 02	0A 2E	Daten von EF Vehicles_Used in DF Tachograph_G2
05 05 03	xx xx	Signatur von EF Vehicles_Used in DF Tachograph_G2 “

o) Abschnitt 4 Absatz DDP_049 erhält folgende Fassung:

„DDP_049 Fahrerkarten der 1. Generation: Für den Datendownload wird das Datendownload-Protokoll der 1. Generation verwendet, und die heruntergeladenen Daten haben das gleiche Format wie die von einer Fahrzeugeinheit der 1. Generation heruntergeladenen Daten.

Fahrerkarten der 2. Generation: 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.“

34. In Anlage 8 Abschnitt 2 erhält der Absatz unter der Überschrift „Referenzdokumente“ folgende Fassung:

„ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer.

First edition: 1999.“

35. Anlage 9 wird wie folgt geändert:

a) Nummer 6 des Inhaltsverzeichnisses erhält folgende Fassung:

„6. PRÜFUNGEN DER EXTERNEN AUSRÜSTUNG ZUR FERNKOMMUNIKATION“

b) Abschnitt 1.1 erster Gedankenstrich erhält folgende Fassung:

„— einer **Sicherheitszertifizierung** auf Grundlage der Spezifizierung Allgemeiner Kriterien anhand einer Sicherheitsvorgabe in völliger Übereinstimmung mit Anlage 10 dieses Anhangs,“

c) Die Tabelle in Abschnitt 2 über Funktionsprüfungen an der Fahrzeugeinheit erhält folgende Fassung:

„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		02, 03, 04, 05, 07, 382
3.2	Betriebsarten		09 bis 11*, 134, 135
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*, 134
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, 134
3.8	Überwachung des Status der Fahrzeugführung		54, 55, 134
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, 134

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
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	Kilometerstanddaten		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		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Anzeige		90, 134, 151 bis 168, PIC_001, DIS_001
3.29	Drucken		90, 134, 169 bis 181, PIC_001, PRT_001 bis PRT_014
3.30	Warnung		134, 182 bis 191, PIC_001
3.31	Herunterladen von Daten auf externe Datenträger		90, 134, 192 bis 196
3.32	Fernkommunikation für gezielte Straßenkontrollen		197 bis 199
3.33	Datenausgabe an zusätzliche externe Geräte		200, 201
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

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
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
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

Nr.	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/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 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 — 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
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

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
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 = + 37 V Ri = 2 Ohm Impuls 2b: Vs = + 20 V Ri = 0,05 Ohm Impuls 3a: Vs = – 150 V Ri = 50 Ohm Impuls 3b: Vs = + 150 V 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 = – 75 V Ri = 10 Ohm Impuls 2a: Vs = + 37 V Ri = 2 Ohm Impuls 2b: Vs = + 10 V Ri = 0,05 Ohm Impuls 3a: Vs = – 112 V Ri = 50 Ohm Impuls 3b: Vs = + 75 V Ri = 50 Ohm Impuls 4: Vs = – 6 V Va = – 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“

d) Abschnitt 6 erhält folgende Fassung:

„6. PRÜFUNGEN DER EXTERNEN 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		224 bis 226
2.3	Werkstoffe		219 bis 223
2.4	Plombierung		398, 401 bis 405
2.5	Externe Schnittstellen		
3.	**Funktionsprüfungen**		
3.1	Fernkommunikation für gezielte Straßenkontrollen		4, 197 bis 199

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
3.2	Aufzeichnung und Speicherung von Daten im Massenspeicher		91
3.3	Kommunikation mit der Fahrzeugeinheit		Anlage 14 DSC_66 bis DSC_70, DSC_71 bis DSC_76
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	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

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
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 = + 37 V Ri = 2 Ohm Impuls 2b: Vs = + 20 V Ri = 0,05 Ohm Impuls 3a: Vs = – 150 V Ri = 50 Ohm Impuls 3b: Vs = + 150 V 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 = – 75 V Ri = 10 Ohm Impuls 2a: Vs = + 37 V Ri = 2 Ohm Impuls 2b: Vs = + 10 V Ri = 0,05 Ohm Impuls 3a: Vs = – 112 V Ri = 50 Ohm Impuls 3b: Vs = + 75 V 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“

e) Die Tabelle in Abschnitt 8 (Interoperabilitätsprüfungen) erhält folgende Fassung:

„Nr.	Prüfung	Beschreibung
	8.1 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 Schreibvorgänge in so vielen EF wie bei der Karte möglich 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.

Nr.	Prüfung	Beschreibung
8.2 Interoperabilitätsprüfungen zwischen Fahrzeugeinheiten und Bewegungssensoren		
1	Koppelung	Prüfen, dass die Koppelung 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 so vieler Ereignisse 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.
8.3 Interoperabilitätsprüfungen zwischen Fahrzeugeinheiten und externen GNSS-Ausrüstungen (soweit vorhanden)		
1	Gegenseitige Authentisierung	Prüfen, dass die gegenseitige Authentisierung zwischen der Fahrzeugeinheit und dem externen GNSS-Modul normal abläuft.
2	Tätigkeitsprüfungen	Ausführung eines typischen Tätigkeitsszenarios an der externen GNSS-Ausrüstung. Das Szenario hat eine normale Tätigkeit sowie die Erstellung so vieler Ereignisse 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.“

36. Anlage 11 wird wie folgt geändert:

a) Abschnitt 8.2.3 Absatz CSM_49 erhält folgende Fassung:

„CSM_49 Fahrzeugeinheiten, Fahrtenschreiberkarten und externe GNSS-Ausrüstung unterstützen die Algorithmen SHA-256, SHA-384 und SHA-512 gemäß Referenzdokument SHS.“

b) Abschnitt 9.1.2 Absatz CSM_58 Unterabsatz 1 erhält folgende Fassung:

„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 und 3 Monate. Dies wird auch in Abbildung 1 (Abschnitt 9.1.7) gezeigt.“

c) Abschnitt 9.1.4 Absatz CSM_72 erhält folgende Fassung:

„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 ihre MSCA, um das entsprechende durch die MSCA signierte VU-Zertifikat zu erhalten. Der private Schlüssel darf nur durch die Fahrzeugeinheit genutzt werden.“

d) Abschnitt 9.1.5 wird wie folgt geändert:

i) Absatz CSM_83 erhält folgende Fassung:

„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 ihre MSCA, um das entsprechende durch die MSCA signierte Kartenzertifikat zu erhalten. Der private Schlüssel darf nur durch die Fahrtenschreiberkarte genutzt werden."

ii) Absatz CSM_88 erhält folgende Fassung:

„CSM_88 Die Gültigkeitsdauer des Card-MA-Zertifikats beträgt für

— Fahrerkarten: 5 Jahre

— Unternehmenskarten: 5 Jahre

— Kontrollkarten: 2 Jahre

— Werkstattkarten: 1 Jahr"

iii) In Absatz CSM_91 wird folgender Text angefügt:

„— Zusätzlich für Kontrollkarten, Unternehmenskarten und Werkstattkarten und nur, wenn solche Karten in den ersten drei Monaten der Gültigkeitsdauer eines neuen EUR-Zertifikats ausgestellt werden: das EUR-Zertifikat, das zwei Generationen älter ist, falls vorhanden.

Hinweis zum letzten Gedankenstrich: Beispielsweise müssen die genannten Karten in den ersten drei Monaten der Gültigkeit des ERCA(3)-Zertifikats (siehe Abbildung 1) das ERCA(1)-Zertifikat enthalten. Dies ist erforderlich, damit diese Karten für den Datendownload von ERCA(1)-Fahrzeugeinheiten verwendet werden können, deren normale Gültigkeitsdauer von 15 Jahren zuzüglich der drei Monate für das Herunterladen von Daten in diesen Monaten abläuft (siehe Anhang IC Randnummer 13 letzter Gedankenstrich)."

e) Abschnitt 9.1.6 wird wie folgt geändert:

i) Absatz CSM_93 erhält folgende Fassung:

„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, übermittelt die erzeugende Partei den öffentlichen Schlüssel an ihre MSCA, um das entsprechende durch die MSCA signierte EGF-MA-Schlüsselpaar zu erhalten. Der private Schlüssel darf nur durch die externe GNSS-Ausrüstung genutzt werden."

ii) Absatz CSM_95 erhält folgende Fassung:

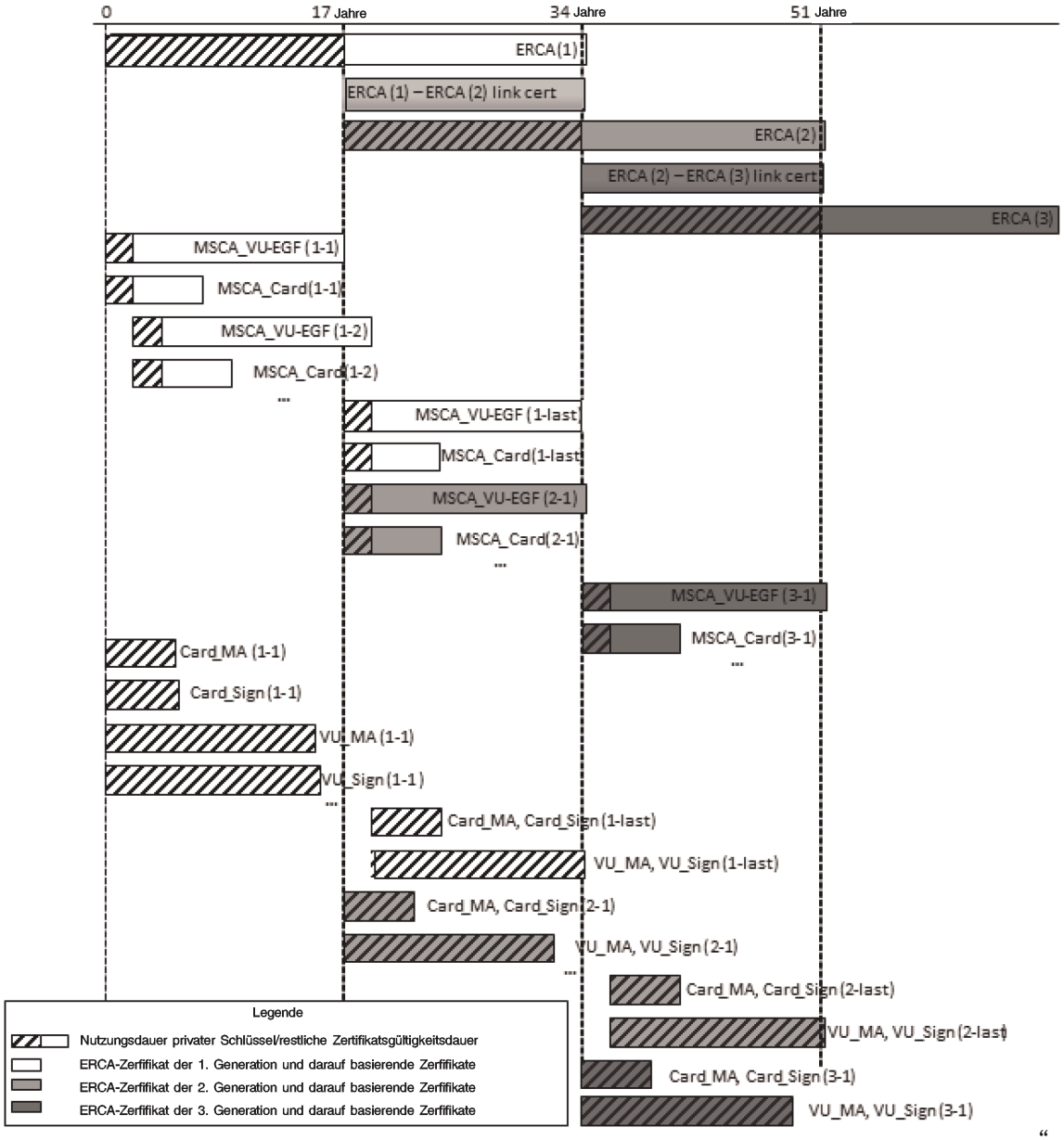
„CSM_95 Externe GNSS-Ausrüstung darf ihr aus dem privaten Schlüssel EGF_MA.SK und dem öffentlichen Schlüssel EGF_MA.PK bestehendes EGF_MA-Schlüsselpaar ausschließlich dazu verwenden, die gegenseitige Authentisierung und Sitzungsschlüsselvereinbarung gegenüber Fahrzeugeinheiten durchzuführen, wie in Abschnitt 11.4 dieser Anlage beschrieben."

f) Abschnitt 9.1.7 wird wie folgt geändert:

i) Abbildung 1 erhält folgende Fassung:

„*Abbildung 1*

Ausgabe und Nutzung der verschiedenen Generationen von ERCA-Wurzelzertifikaten, ERCA-Linkzertifikaten, MSCA-Zertifikaten und Ausrüstungszertifikaten



“

ii) Nummer 6 der Hinweise zu Abbildung 1 erhält folgende Fassung:

„6. Aus Platzgründen ist die unterschiedliche Gültigkeitsdauer der Zertifikate Card_MA und Card_Sign nur für die 1. Generation angegeben.“

g) Abschnitt 9.2.1.1 wird wie folgt geändert:

i) Absatz CSM_106 erster Gedankenstrich erhält folgende Fassung:

„— Für 128-Bit-Bewegungssensor-Hauptschlüssel: CV = ‚B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83'"

ii) Absatz CSM_107 Unterabsatz 1 erhält folgende Fassung:

„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."

iii) Absatz CSM_108 erhält folgende Fassung:

„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}."

h) Abschnitt 9.2.2.1 wird wie folgt geändert:

i) Absatz CSM_123 erhält folgende Fassung:

„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`.

Hinweis:

— Die VU-Seriennummer muss mit dem Element ‚vuSerialNumber' von VuIdentification (siehe Anlage 1) und mit der Certificate Holder Reference in den Zertifikaten der VU übereinstimmen.

— Die VU-Seriennummer ist zu dem Zeitpunkt, zu dem der Hersteller einer Fahrzeugeinheit die VU-spezifischen DSRC-Schlüssel beantragt, unter Umständen nicht bekannt. In diesem Fall sendet der Hersteller der VU stattdessen die bei der Beantragung der VU-Zertifikate verwendete eindeutige Kennung für den Zertifikatsantrag (siehe CSM_153). Diese Kennung des Zertifikatsantrags muss deshalb mit der Certificate Holder Reference in den Zertifikaten der VU übereinstimmen."

ii) In Absatz CSM_124 Schritt 2 erhält die Info-Anforderung folgende Fassung:

„info = VU-Seriennummer oder Kennung des Zertifikatsantrags gemäß CSM_123"

iii) Absatz CSM_128 erhält folgende Fassung:

„CSM_128 Die MSCA muss Aufzeichnungen aller von ihr erzeugten VU-spezifischen DSRC-Schlüssel samt Versionsnummer und der zu ihrer Ableitung verwendeten VU-Seriennummer oder Kennung des Zertifikatsantrags führen."

i) Abschnitt 9.3.1 Absatz CSM_135 Unterabsatz 1 erhält folgende Fassung:

„Zur Kodierung der Datenobjekte innerhalb der Zertifikate sind die Distinguished Encoding Rules (DER) gemäß ISO 8825-1 zu verwenden. Tabelle 4 zeigt die vollständige Kodierung der Zertifikate, einschließlich aller Tags und Längenbytes."

j) Abschnitt 9.3.2.3 Absatz CSM_141 erhält folgende Fassung:

„CSM_141 Mit ‚Certificate Holder Authorisation' wird die Zertifikatart angegeben. Sie besteht aus den sechs höchstwertigen Bytes der Fahrtenschreiberanwendungs-ID, verkettet mit dem Gerätetyp, der die Art des Geräts angibt, für die das Zertifikat vorgesehen ist. Bei VU-Zertifikaten, Fahrerkarten- oder Werkstattkartenzertifikaten wird der Gerätetyp auch verwendet, um zwischen einem Zertifikat für die gegenseitige Authentisierung und einem Zertifikat für die Erzeugung digitaler Signaturen zu unterscheiden (siehe Abschnitt 9.1 und Anlage 1, Datentyp EquipmentType)."

k) In Abschnitt 9.3.2.5 Absatz CSM_146 wird folgender Unterabsatz angefügt:

„*Hinweis:* Bei Kartenzertifikaten muss der Wert der CHR dem Wert von ‚cardExtendedSerialNumber' in EF_ICC entsprechen (siehe Anlage 2). Bei EGF-Zertifikaten muss der Wert der CHR dem Wert von ‚sensorGNSSSerialNumber' in EF_ICC entsprechen (siehe Anlage 14). Bei VU-Zertifikaten muss der Wert der CHR dem Element „vuSerialNumber" von ‚VuIdentification' entsprechen (siehe Anlage 1), es sei denn, dem Hersteller ist die herstellerspezifische Seriennummer zum Zeitpunkt der Beantragung des Zertifikats nicht bekannt."

l) Abschnitt 9.3.2.6 Absatz CSM_148 erhält folgende Fassung:

„CSM_148 Certificate Effective Date gibt Anfangsdatum und -uhrzeit der Gültigkeitsdauer des Zertifikats an."

m) Abschnitt 9.3.3 wird wie folgt geändert:

i) Absatz CSM_151 Unterabsatz 1 erhält folgende Fassung:

„Beim Beantragen eines Zertifikats muss die MSCA der ERCA die folgenden Daten übermitteln:"

ii) Absatz CSM_153 erhält folgende Fassung:

„CSM_153 Der Gerätehersteller muss der MSCA in einem Zertifikatsantrag die folgenden Daten übermitteln, damit Letztgenannte die Certificate Holder Reference des neuen Gerätezertifikats erstellen kann:

— falls bekannt (siehe CSM_154), die Seriennummer des Geräts zur eindeutigen Identifizierung von Hersteller, Gerätetyp und 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."

n) Abschnitt 10.2.1 wird wie folgt geändert:

i) In Absatz CSM_157 erhält der Text vor den Hinweisen zu Abbildung 4 folgende Fassung:

„Die Fahrzeugeinheiten verifizieren mithilfe des in Abbildung 4 dargestellten Protokolls die Zertifikatkette einer Fahrtenschreiberkarte. Bei jedem aus der Karte ausgelesenem Zertifikat überprüft die VU die Richtigkeit des Feldes Certificate Holder Authorisation (CHA):

— Im Feld CHA des Kartenzertifikats muss ein Kartenzertifikat für die gegenseitige Authentisierung angegeben sein (siehe Anlage 1, Datentyp EquipmentType).

— In der CHA des Card.CA-Zertifikats muss eine MSCA angegeben sein.

— In der CHA des Card.Link-Zertifikats muss die ERCA angegeben sein.“

ii) In Absatz CSM_159 wird folgender Satz angefügt:

„Während die Speicherung aller anderen Arten von Zertifikaten optional ist, muss ein von einer Karte vorgelegtes neues Linkzertifikat von der VU gespeichert werden.“

o) Abschnitt 10.2.2 wird wie folgt geändert:

i) In Absatz CSM_161 erhält der Text vor Abbildung 5 folgende Fassung:

„Die Fahrtenschreiberkarten verifizieren mithilfe des in Abbildung 5 dargestellten Protokolls die Zertifikatkette einer VU. Bei jedem von der VU vorgelegtem Zertifikat überprüft die Karte die Richtigkeit des Feldes Certificate Holder Authorisation (CHA):

— In der CHA des VU.Link-Zertifikats muss die ERCA angegeben sein.

— In der CHA des VU.CA-Zertifikats muss eine MSCA angegeben sein.

— Im Feld CHA des VU-Zertifikats muss ein VU-Zertifikat für die gegenseitige Authentisierung angegeben sein (siehe Anlage 1, Datentyp EquipmentType).“

ii) Absatz CSM_165 erhält folgende Fassung:

„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.PKeph) 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.PKeph). Nach einem erfolgreichen Befehl GENERAL AUTHENTICATE setzt die Karte Comp(VU.PKeph) zurück.“

p) Abschnitt 10.3 wird wie folgt geändert:

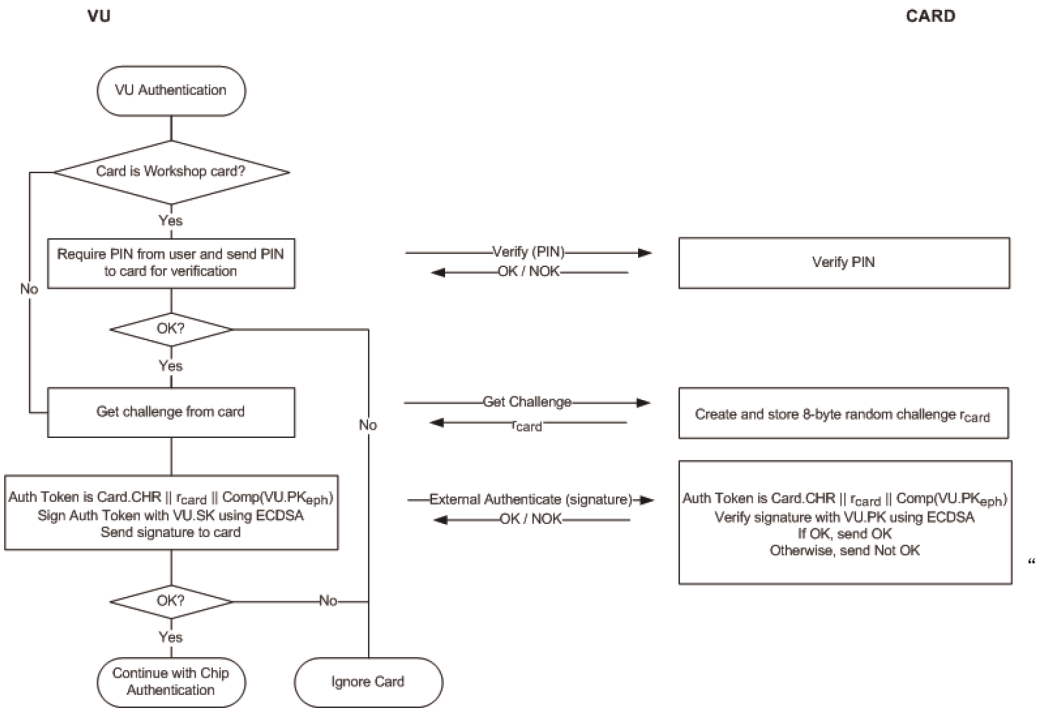
i) Absatz CSM_170 Unterabsatz 1 erhält folgende Fassung:

„Neben der Zufallszahl enthält die Signatur der VU die dem Kartenzertifikat entnommene Kennung des Zertifikatinhabers.“

ii) Abschnitt CSM_171 Abbildung 6 erhält folgende Fassung:

„Abbildung 6

VU-Authentisierungsprotokoll



“

iii) Absatz CSM_174 erhält folgende Fassung:

„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}), miteinander verkettet;

— sie überprüft die Signatur der VU unter Verwendung des ECDSA-Algorithmus und des Hash-Algorithmus, der an die Schlüsselgröße des VU_MA-Schlüsselpaars der VU gebunden ist (siehe CSM_50), in Kombination mit VU.PK und dem berechneten Authentisierungstoken.“

q) Abschnitt 10.4 Absatz CSM_176 wird wie folgt geändert:

i) Nummer 2 erhält folgende Fassung:

„2. Die VU sendet den öffentlichen Punkt VU.PK_{eph} ihres flüchtigen Schlüsselpaars an die Karte. Der öffentliche Punkt ist gemäß TR-03111 in einen Oktettstring umzuwandeln. Dabei ist das unkomprimierte Verschlüsselungsformat zu verwenden. 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.“

ii) Nummer 6 erhält folgende Fassung:

„6. Mithilfe von K_{MAC} berechnet die Karte anhand der Kennung des flüchtigen öffentlichen Punkts der VU einen Authentisierungstoken: T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph}). Der öffentliche Punkt muss das von der VU verwendete Format haben (siehe Nummer 2 oben). Die Karte übermittelt N_{PICC} und T_{PICC} an die Fahrzeugeinheit.“

r) Abschnitt 10.5.2 Absatz CSM_191 erhält folgende Fassung:

„CSM_191 Sämtliche zu verschlüsselnde Datenobjekte sind gemäß ISO 7816-4 mithilfe von Padding Indicator ‚01' aufzufüllen. Zur Berechnung des MAC müssen Datenobjekte im APDU 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) ohne Verschlüsselung: DO '81' || DO '99' || DO '8E' || SW1SW2

Fall 2 oder 4 (gerades INS-Byte) mit 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 1/Fall 3, 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

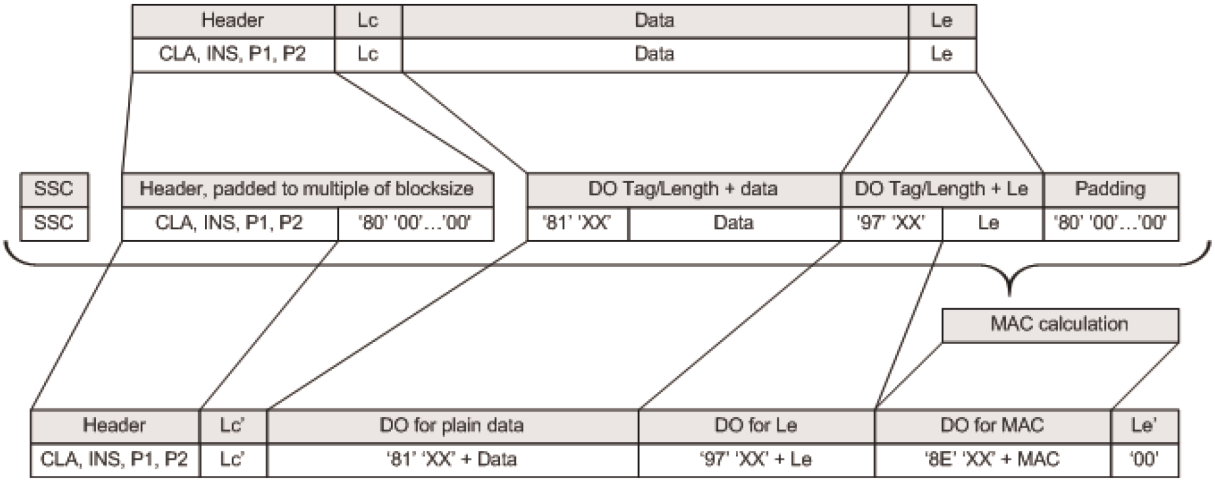


Abbildung 9

Transformation einer authentisierten Antwort-APDU für Fall 1/Fall 3

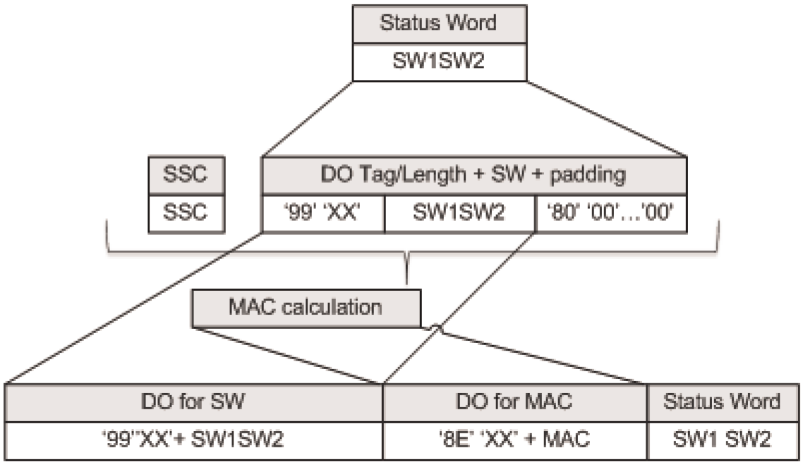
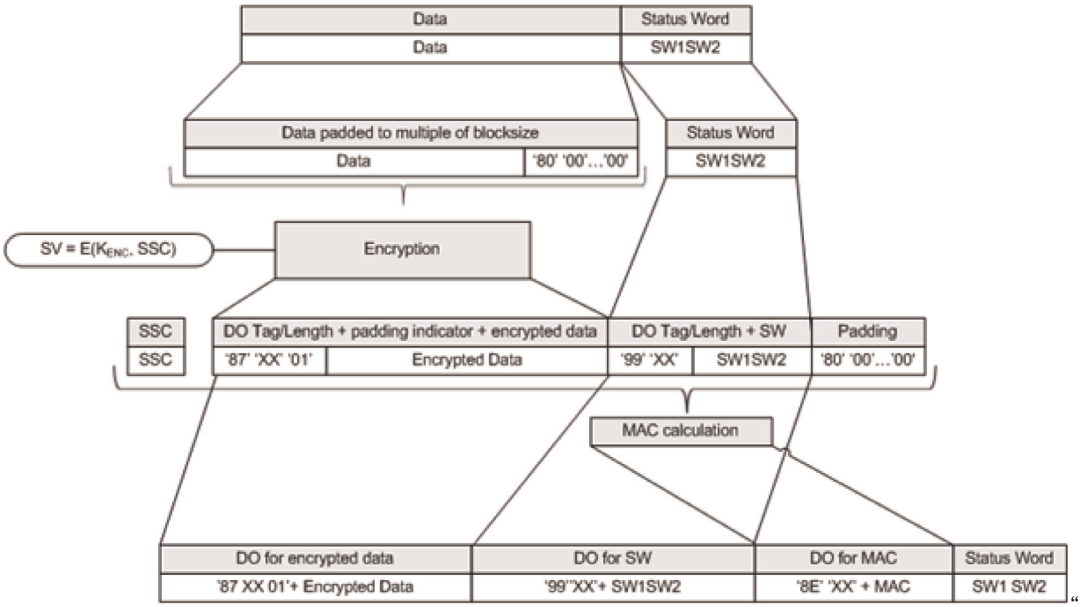


Abbildung 10

Transformation einer verschlüsselten und authentisierten



“

s) Abschnitt 10.5.3 Absatz CSM_193 erhält folgende Fassung:

„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 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.“

t) Abschnitt 11.3.2 wird wie folgt geändert:

i) Absatz CSM_208 Unterabsatz 1 erhält folgende Fassung:

„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."

ii) Absatz CSM_210 erhält folgende Fassung:

„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."

u) Abschnitt 11.3.3 Absatz CSM_211 Unterabsatz 1 erhält folgende Fassung:

„Im Normalbetrieb verwenden Fahrzeugeinheit und EGF das in Abbildung 11 dargestellte Protokoll, um die temporäre Gültigkeit des gespeicherten EGF_MA-Zertifikats zu überprüfen und um den öffentlichen VU_MA-Schlüssel zur anschließenden VU-Authentisierung festzulegen. Im Normalbetrieb findet keine weitere gegenseitige Verifizierung der Zertifikatketten statt."

v) Nummer 12.3 Tabelle 6 erhält folgende Fassung:

„*Tabelle 6*

Anzahl der Klartext- und verschlüsselten Datenbytes 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
11	Antwort	Authentisierungsdaten + Inhalte der Datei	16 oder 32, je nach Datei	16 oder 32, je nach Datei	32/48	32/48	32/48
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"

w) In Abschnitt 13.1 Unterabsatz CSM_224 erhält die Anforderung an die VU-Seriennummer folgende Fassung:

„**VU serial number** die Seriennummer der VU oder die Kennung für den Zertifikatsantrag (Datentyp VuSerialNumber oder CertificateRequestID) — siehe CSM_123"

x) Abschnitt 13.3 Absatz CSM_228 Nummer 2 erhält folgende Fassung:

„2. Die Kontrollkarte verwendet den angegebenen DSRC-Hauptschlüssel in Kombination mit der VU-Seriennummer oder der Kennung für den Zertifikatsantrag in den DSRC-Sicherheitsdaten, um daraus die VU-spezifischen DSRC-Schlüssel K_VU_{DSRC}_ENC und K_VU_{DSRC}_MAC abzuleiten (siehe CSM_124).“

y) Abschnitt 14.3 wird wie folgt geändert:

i) In Absatz CSM_234 erhält der Text vor den Hinweisen zu Abbildung 13 folgende Fassung:

„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. Die Kontrollkarte überprüft die temporäre Gültigkeit eines vom IDE vorgelegten Zertifikats mithilfe ihrer internen aktuellen Uhrzeit (siehe CSM_167). Die Kontrollkarte darf dann ihre aktuelle Uhrzeit aktualisieren, wenn das Effective Date eines authentischen Zertifikats einer ‚gültigen Zeitquelle‘ jünger ist als die aktuelle Uhrzeit der Karte. Die Karte darf nur die folgenden Zertifikate als gültige Zeitquelle akzeptieren:

— ERCA-Linkzertifikate der 2. Generation

— MSCA-Zertifikate der 2. Generation

— VU_Sign- oder Card_Sign-Zertifikate der 2. Generation, die vom selben Land ausgestellt sind wie das bzw. die Kartenzertifikat(e) der Kontrollkarte selbst.

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 der Daten gemäß dem in DSS definierten Signatursystem überprüfen. In beiden Fällen ist es erforderlich, bei jedem aus der Datei ausgelesenem Zertifikat die Richtigkeit des Feldes Certificate Holder Authorisation (CHA) zu überprüfen:

— Im Feld CHA des EQT-Zertifikats muss ein VU-Zertifikat bzw. ein Kartenzertifikat zur Signierung angegeben sein (siehe Anlage 1, Datentyp EquipmentType).

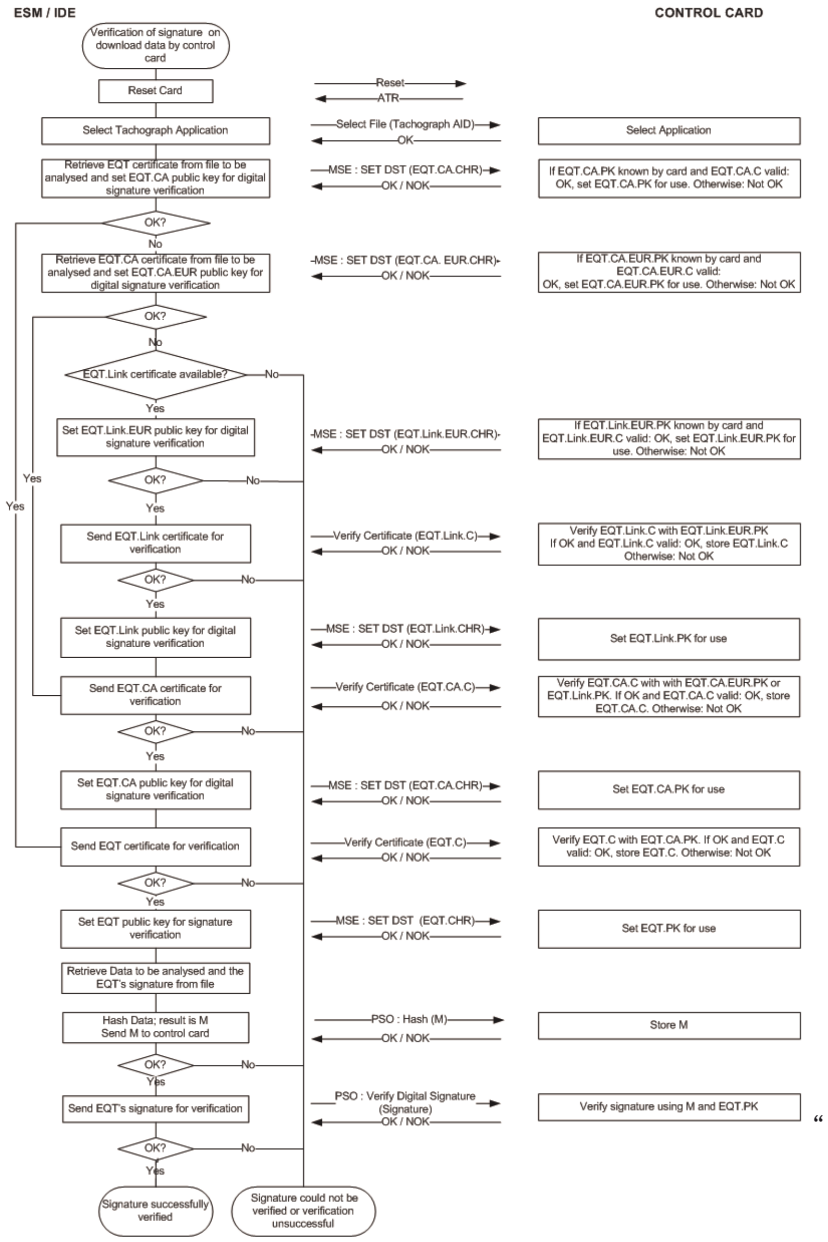
— In der CHA des EQT.CA-Zertifikats muss eine MSCA angegeben sein.

— In der CHA des EQT.Link-Zertifikats muss die ERCA angegeben sein.“

ii) Abbildung 13 erhält folgende Fassung:

„Abbildung 13

Protokoll für die Verifizierung der Signatur mithilfe einer heruntergeladenen Datei



“

37. Anlage 12 wird wie folgt geändert:

a) Abschnitt 3 wird wie folgt geändert:

i) In Absatz GNS_4 erhält der zweite Unterabsatz nach Abbildung 2 folgende Fassung:

„Die Auflösung der Position basiert auf dem oben beschriebenen RMC-Datensatzformat. Der erste Teil der Felder 3) und 5) wird verwendet, um die Gradwerte darzustellen. Der Rest dient dazu, die Minuten mit drei Dezimalzahlen darzustellen. Die Auflösung ist also 1/1 000 Minute oder 1/60 000 Grad (da eine Minute 1/60 Grad ist).“

ii) Absatz GNS_5 erhält folgende Fassung:

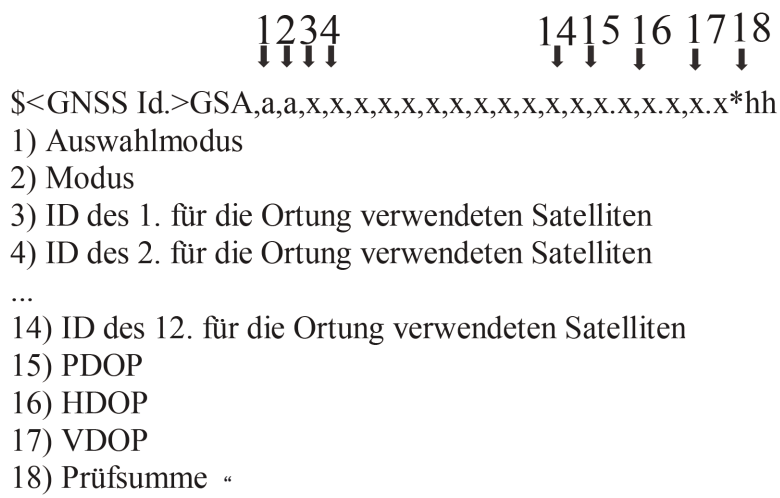
„GNS_5 Die Fahrzeugeinheit muss die Positionsinformation zur Breite und Länge mit einer Auflösung von 1/10 Minute oder 1/600 Grad in der VU-Datenbank speichern, wie in Anlage 1 für GeoCoordinates beschrieben.

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 gibt für jede GNSS-Konstellation und satellitengestützte Ergänzungssysteme (Satellite-Based Augmentation System, SBAS) die entsprechende NMEA-ID an.

Abbildung 3

Struktur des GSA-Datensatzes



iii) Absatz GNS_6 erhält folgende Fassung:

„GNS_6 Der *GSA*-Datensatz muss unter der Datensatznummer ‘02’ bis ‘06’ gespeichert werden.“

b) Abschnitt 4.2.1 wird wie folgt geändert:

i) Absatz GNS_16 erhält folgende Fassung:

„GNS_16 Im Kommunikationsprotokoll müssen erweiterte Längenfelder nicht unterstützt werden.“

ii) Absatz GNS_18 erhält folgende Fassung:

„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 (Dedicated 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."

iii) Absatz GNS_20 erhält folgende Fassung:

„GNS_20 Der GNSS Secure Transceiver muss für die Speicherung der Daten einen Speicher verwenden und mindestens 20 Millionen Schreib/Lese-Zyklen durchführen können. 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 fünf GSA-Datensätze für die GNSS-Konstellationen und satellitengestützte Ergänzungssysteme (Satellite-Based Augmentation System, SBAS) gibt."

c) Abschnitt 4.2.2 Absatz GNS_23 Nummer 5 erhält folgende Fassung:

„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 Mindestwert für das verfügbare Satellitensystem (z. B. wenn die Ortung verfügbar ist)."

d) Abschnitt 4.4.1 Absatz GNS_28 erhält folgende Fassung:

„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 Enum '0E'H Communication error with the external GNSS facility (Kommunikationsfehler mit der externen GNSS-Ausrüstung) 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."

e) Abschnitt 4.4.2 Absatz GNS_29 erhält folgende Fassung:

„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 '19'H Tamper detection of GNSS (Manipulationserkennung beim GNSS). Alternativ kann die externe GNSS-Ausrüstung auch auf keine externen Anfragen mehr antworten."

f) Abschnitt 4.4.3 Absatz GNS_30 erhält folgende Fassung:

„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 '0D'H Absence of position information from GNSS receiver (Fehlende Positionsdaten des GNSS-Empfängers) 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."

g) In Abschnitt 4.4.4 Absatz GNS_31 erhält der Text bis Abbildung 4 folgende Fassung:

„Wenn die VU erkennt, dass das EGF-Zertifikat zur gegenseitigen Authentisierung nicht mehr gültig ist, muss die VU ein Kontrollgerät-Ereignis des Typs EventFaultType Enum '1B'H *External GNSS facility certificate expired* (Abgelaufenes Zertifikat der externen GNSS-Ausrüstung) mit einem Zeitstempel des aktuellen Zeitwerts generieren und aufzeichnen. Die VU verwendet weiterhin die erhaltenen GNSS-Positionsdaten."

h) Abschnitt 5.2.1 Absatz GNS_34 erhält folgende Fassung:

„GNS_34 Erhält die VU mehr als 3 Stunden durchgehend keine Daten vom GNSS-Empfänger, so muss die VU ein Ereignis des Typs EventFaultType Enum '0D'H Absence of position information from GNSS receiver (Fehlende Positionsdaten des GNSS-Empfängers) mit 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."

i) Abschnitt 6 erhält folgende Fassung:

„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. Wenn ein Zeitkonflikt-Ereignis ausgelöst wurde, prüft die VU die Zeitabweichung in den nächsten 12 Stunden nicht. Das Ereignis wird nicht ausgelöst, wenn der GNSS-Empfänger innerhalb der letzten 30 Tage kein gültiges GNSS-Signal empfangen konnte."

38. Anlage 13 wird wie folgt geändert:

a) In Abschnitt 2 erhält der vierte Absatz folgende Fassung:

„Folgendes wird in dieser Anlage 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 11 Gemeinsame Sicherheitsmechanismen]).

— Die Bluetooth®-Protokolle, die durch die ITS-Schnittstelle genutzt werden."

b) In Abschnitt 4.2 erhält der dritte Absatz folgende Fassung:

„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. Zusätzliche Verschlüsselungsmechanismen, die über die Funktionen von Bluetooth® hinausgehen, sind nicht vorgesehen. Sollten allerdings zusätzliche Sicherheitsmaßnahmen erforderlich sein, so müssen diese Anlage 11 Gemeinsame Sicherheitsmechanismen entsprechen."

c) Abschnitt 4.3 wird wie folgt geändert:

i) Der erste Absatz erhält folgende Fassung:

„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 der korrekte PIN-Code angegeben werden, bevor es Daten empfängt."

ii) Der dritte Absatz nach Tabelle 1 erhält folgende Fassung:

„Der Hersteller kann es optional ermöglichen, den PIN-Code direkt über die VU zu ändern, der PUC-Code jedoch muss unabänderlich sein. Besteht die Möglichkeit zur Änderung des PIN-Codes, so muss der aktuelle PIN-Code direkt in der VU eingegeben werden."

d) In Abschnitt 4.4 erhält der zweite Absatz nach der Überschrift „Datenfeld" folgende Fassung:

„Falls mehr Daten zu verarbeiten sind als Raum in einer Einzelnachricht zur Verfügung steht, werden sie in mehrere Teilnachrichten aufgeteilt. 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."

e) Anhang 1 wird wie folgt geändert:

i) Die Überschrift erhält folgende Fassung:

„1) LISTE DER ÜBER DIE ITS-SCHNITTSTELLE VERFÜGBAREN DATEN"

ii) In der Tabelle in Abschnitt 3 wird nach „Fehlende Positionsdaten des GNSS-Empfängers" folgender Punkt eingefügt:

„Kommunikationsfehler mit der externen GNSS-Ausrüstung	— 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."

iii) In Nummer 5 wird folgender Gedankenstrich angefügt:

„— Störung der ITS-Schnittstelle (falls zutreffend)".

f) Die ASN.1-Spezifikationen in Anhang 3 werden wie folgt geändert:

i) Nach Zeile 206 werden folgende Zeilen 206a bis 206e eingefügt:

```
“206a
206b       DriverID ::= SEQUENCE{
206c       issuingMemberState OCTET STRING (SIZE(3)),
206d       cardNumber OCTET STRING (SIZE(16))
206e }“;
```

ii) Die Zeilen 262 bis 264 erhalten folgende Fassung:

```
„262    driveRecognize BIT STRING ('00'B UNION '01'B),
263     driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264     driverCardDriver2 BIT STRING ('00'B UNION '01'B), “;
```

iii) Zeile 275 erhält folgende Fassung:

```
„275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),„;
```

iv) Die Zeilen 288 bis 310 erhalten folgende Fassung:

```
„288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289     '011'B UNION '100'B UNION '101'B …),
290     driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291     '011'B UNION '100'B UNION '101'B …),
292
293     driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296     UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299     driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302     UNION '1011'B UNION '1100'B UNION '1101'B …),
303
304
305
306     overSpeed BIT STRING ('00 'B UNION '01 'B),
307     driver1Identification DriverID,
308     driver2Identification DriverID,
309
310“
```

v) Die Zeilen 362 und 363 erhalten folgende Fassung:

```
„362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),“;
```

vi) Nach Zeile 410 werden folgende Zeilen 410a und 410b eingefügt:

```
„410a   comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,“;
```

vii) Nach Zeile 539 werden folgende Zeilen 539a bis 539j eingefügt:

```
„539a     CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b      beginDate GeneralizedTime,
539c      endDate GeneralizedTime,
539d      cardsType SEQUENCE OF UTF8String,
539e      cardsNumber SEQUENCE OF INTEGER,
539f      issuingMemberState SEQUENCE OF NationAlpha,
539g      cardsGeneration SEQUENCE OF INTEGER,
539h      numberOfSimilarEvent INTEGER
539i            }
539j“;
```

39. Anlage 14 wird wie folgt geändert:

a) Nummer 5.5 im Inhaltsverzeichnis erhält folgende Fassung:

„5.5 Unterstützung für Richtlinie (EU) 2015/719 ..... 490“

b) Abschnitt 2 Absatz 3 erhält folgende Fassung:

„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 (z. B. höchstzulässige Gewichte und Abmessungen von Nutzfahrzeugen gemäß der Richtlinie (EU) 2015/719) eingesetzt werden; diese Maßnahmen können im Ermessen der zuständigen Kontrollbehörden getrennt oder aufeinanderfolgend durchgeführt werden.“

c) Abschnitt 5.1 wird wie folgt geändert:

i) Absatz DSC_19 zwölfter Gedankenstrich erhält folgende Fassung:

„— 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, wenn das Lesegerät 15 Meter vor dem Fahrzeug und in 2 Meter Höhe installiert und auf die horizontale und vertikale Mitte der Windschutzscheibe gerichtet ist. Bei leichten Fahrzeugen ist eine Anbringung im oberen Teil der Windschutzscheibe geeignet. Bei allen anderen Fahrzeugen muss die DSRC-Antenne entweder nahe dem unteren Teil oder nahe dem oberen Teil der Windschutzscheibe eingebaut sein.“

ii) Absatz DSC_22 Unterabsatz 1 erhält folgende Fassung:

„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 befestigt werden und muss den in 4.1.2 und 4.1.3 beschriebenen Anwendungsfällen effizient gerecht werden.“

d) Abschnitt 5.4.3 Sequenz 7 erhält folgende Fassung:

„7 REDCR > DSRC-VU Sendet GET.request für Daten anderer Attribute (falls zutreffend)“

e) In Abschnitt 5.4.4 Absatz DCS_40 wird die Definition des ASN.1-Moduls wie folgt geändert:

i) Die erste Zeile der Sequenz `TachographPayload` erhält folgende Fassung:

„`tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509`[1]“

ii) Folgende Fußnote 1 wird hinzugefügt:

„1. Wenn ein LPN einen AlphabetIndicator ‚LatinAlphabetNo2‘ oder ‚latinCyrillicAlphabet‘ enthält, werden die Sonderzeichen von der Fernabfrageeinrichtung unter Anwendung besonderer Regeln gemäß ISO/DIS 14 906,2 neu abgebildet.“

iii) In der Zeile, in der „Timestamp of current record“ definiert ist, wird die hochgestellte „2“ gestrichen.

iv) Die Definition des ASN.1-Moduls für `RtmTransferAck` erhält folgende Fassung:

„
```
RtmTransferAck ::= INTEGER {
                   Ok (1),
                   NoK (2)
                   } (1..255)
```
“;

f) In Abschnitt 5.4.5 Tabelle 14.3 erhält der Eintrag RTM12 folgende Fassung:

„**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 des Typs „35"H Sensorstörung aufgezeichnet worden ist, — 2 wenn in den letzten 10 Tagen ein Ereignis des Typs GNSS-Empfängerstörung (intern oder extern Enum „36"H oder „37"H) aufgezeichnet worden ist, — 3 wenn in den letzten 10 Tagen ein Ereignis des Typs „0E"H Kommunikationsfehler mit der externen GNSS-Ausrüstung aufgezeichnet worden ist, — 4 wenn in den letzten 10 Tagen sowohl Sensorstörungen als auch GNSS-Empfängerstörungen aufgezeichnet worden sind, — 5 wenn in den letzten 10 Tagen sowohl Sensorstörungen als auch Kommunikationsfehler mit der externen GNSS-Ausrüstung aufgezeichnet worden sind, — 6 wenn in den letzten 10 Tagen sowohl GNSS-Empfängerstörungen als auch Kommunikationsfehler mit der externen GNSS-Ausrüstung aufgezeichnet worden sind, — 7 wenn in den letzten 10 Tagen alle drei Arten von Sensorstörungen aufgezeichnet worden sind; wenn in den letzten 10 Tagen keine Ereignisse aufgezeichnet worden sind, ist der Wert 0 zuzuweisen.	–Sensorstörung ein Oktett gemäß Datenglossar	`sensorFault INTEGER (0..255),;` "

g) Abschnitt 5.4.6 Absatz DSC_43 erhält folgende Fassung:

„DSC_43 Bei jedem DSRC-Austausch werden die Daten mit PER (Packed Encoding Rules) UNALIGNED verschlüsselt, mit Ausnahme von `TachographPayload` und `OwsPayload`;, die mit OER (Octet Encoding Rules) gemäß ISO/IEC 8825-7, Rec. ITU-T X.696 verschlüsselt werden."

h) In Abschnitt 5.4.7 Tabelle 14.9 Spalte 4 erhält die Beschreibung des Felds `Rtm-ContextMark`; folgende Fassung:

„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."

i) Die Abschnitte 5.5 und 5.5.1 erhalten folgende Fassung:

„5.5 **Unterstützung für Richtlinie (EU) 2015/719**

5.5.1 *Überblick*

DSC_59 Um die Richtlinie (EU) 2015/719 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 auf die Norm ISO 15638 (TARV) Teil 20 (WOB/OWS) verweist."

j) Abschnitt 5.6.1 Absatz DSC_68 Buchstabe a erhält folgende Fassung:

„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 nicht VU-interner DSRC-VU nach einem offenen Standard erfolgen. Die VU wird auf eine der folgenden Arten mit der DSRC-VU verbunden:"

k) Abschnitt 5.7.1 Absatz DSC_77 erhält folgende Fassung:

„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-Wert ‚0C'H für das Ereignis ‚Kommunikationsfehler mit der Fernkommunikationsausrüstung' zusammen mit dem Zeitstempel erfolgen."

40. Anlage 15 wird wie folgt geändert:

a) Abschnitt 2.2 Absatz 1 erhält folgende Fassung:

„Fahrtenschreiberkarten der 1. Generation sind interoperabel mit Fahrzeugeinheiten der 1. Generation (gemäß Anhang IB der Verordnung (EWG) Nr. 3821/85); Fahrtenschreiberkarten der 2. Generation wiederum sind interoperabel mit Fahrzeugeinheiten der 2. Generation (gemäß Anhang IC dieser Verordnung). Zusätzlich gelten die nachfolgenden Bestimmungen."

b) Abschnitt 2.4.1 Absatz MIG_11 wird wie folgt geändert:

i) Der erste Gedankenstrich erhält folgende Fassung:

„— nicht signierte EF ic und icc (optional),"

ii) Der dritte Gedankenstrich erhält folgende Fassung:

„— sonstige Anwendungsdaten-EF (innerhalb der DF Tachograph), 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.

Die entsprechenden Downloads dürfen keine Anwendungsdaten-EF umfassen, die nur in Fahrer- (und Werkstatt-)Karten der 2. Generation vorhanden sind (Anwendungsdaten-EF innerhalb der DF Tachograph_G2)."

c) Abschnitt 2.4.3 Absätze MIG_014 und MIG_015 erhalten folgende Fassung:

„MIG_014 Außerhalb des Rahmens von Fahrerkontrollen durch eine Nicht-EU-Kontrollbehörde werden für den Datendownload von Fahrzeugeinheiten der 2. Generation 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 können, ist es optional möglich, Daten von Fahrzeugeinheiten der 2. Generation unter Verwendung der Sicherheitsmechanismen der 1. Generation herunterzuladen. Die heruntergeladenen Daten müssen in dem Fall das gleiche Format aufweisen wie Daten, die von einer Fahrzeugeinheit der 1. Generation heruntergeladen werden. Diese Funktion kann durch entsprechende Menübefehle ausgewählt werden."

ANHANG II

Anhang II der Verordnung (EU) 2016/799 wird wie folgt geändert:

1. Kapitel I Abschnitt 1 Buchstabe b erhält folgende Fassung:

„b) aus einer Typgenehmigungsnummer, die der Nummer des für das Muster des Kontrollgeräts oder des Schaublatts oder der Fahrtenschreiberkarte ausgestellten Typgenehmigungsbogens entspricht und an einer beliebigen Stelle in der Nähe des Rechtecks anzubringen ist."

2. Kapitel III Abschnitt 5 erhält folgende Fassung:

„5. Zur Typgenehmigung vorgelegt am ....."

3. Kapitel IV Abschnitt 5 erhält folgende Fassung:

„5. Zur Typgenehmigung vorgelegt am ....."