

D-CP Practice Statement

Version 1.0

Stand: 14.07.2010



Historie

Version	Datum	Autor(en)	Qualitätssicherung	Bemerkung
1.0	14.07.2010	Frau Fröhling	Herr Brockstedt, Herr Hansen	

Tabelle 1: Historie Dokument



INHALTSVERZEICHNIS

HISTORIE	2
ABBILDUNGSVERZEICHNIS	7
TABELLENVERZEICHNIS	8
1 EINFÜHRUNG	8
1.1 Verantwortliche Organisation	8
1.2 Genehmigung	8
1.3 Veröffentlichung und Kontakt.....	9
1.4 Überblick.....	9
1.4.1 Organisatorische Struktur.....	9
1.4.2 Zertifizierungsinfrastruktur	10
1.4.3 Funktionen des D-CP.....	11
1.5 Geltungsbereich.....	12
2 ALLGEMEINE BESTIMMUNGEN	13
2.1 Pflichten des D-CP	13
2.2 Pflichten externer Organisationen	13
2.2.1 Pflichten der DC-A	13
2.2.2 Pflichten der Ausgabestellen (CIAs)	14
2.2.3 Pflichten der Hersteller von Fahrzeugeinheiten.....	14
2.2.4 Pflichten der Hersteller von Weg-/Geschwindigkeitsgebern	15
2.2.5 Pflichten von Karteninhabern/Antragsteller	16
2.2.6 Pflichten der Hersteller von Kontrollgerätkarten	16
Pflichten der Inhaber von RA-Zertifikaten	16
2.3 Haftung.....	17
3 KARTEN- UND GERÄTEMANAGEMENT	18
3.1 Übersicht.....	18
3.2 Kartenpersonalisierer	18
3.2.1 Berechtigung zur Antragstellung	18



3.2.2	Zertifikatsanträge für Karten	18
4	SCHLÜSSELMANAGEMENT	19
4.1	Überblick.....	19
4.1.1	Pflichten des Kartenpersonalisierers.....	19
4.2	Schlüsselpaare der D-CA	19
4.2.1	Verwendungszweck	19
5	SCHLÜSSEL FÜR KARTEN	20
5.1	ALLGEMEINES	20
5.2	Schlüsselerzeugung	20
5.3	Dauer der Verwendung von Schlüsseln	20
5.4	Archivierung der öffentlichen Schlüssel	20
6	ZERTIFIKATSMANAGEMENT FÜR DIE KARTEN	20
6.1	Anträge und Antragsdaten.....	20
6.2	Gültigkeitsdauer der ausgestellten Zertifikate	21
7	SICHERUNG DER KOMMUNIKATION ZWISCHEN DEM D-CP UND SEINEN VERTRAGSPARTNERN	21
7.1	Allgemeines	21
8	SICHERHEITSMANAGEMENT	21
8.1	Allgemeines	21
8.2	Risikomanagement	22
8.3	Personelle Sicherheitsmaßnahmen	22
8.3.1	Rollen mit besonderem Vertrauen.....	22
8.3.2	Rollentrennung.....	25
8.3.3	Identifizierung und Authentisierung	25
8.3.4	Anforderungen an das Personal.....	26
8.3.5	Schulungen.....	26
8.4	Technische Sicherheitsmaßnahmen.....	27



8.4.1	Allgemeine technische Maßnahmen	27
8.5	Protokollierung sicherheitsrelevanter Ereignisse	28
8.5.1	Protokollierte Ereignisse.....	28
8.5.2	Häufigkeit der Überprüfung von Protokolldaten	29
8.5.3	Aufbewahrungszeitraum für Protokolldaten	29
8.5.4	Schutz der Protokolldaten.....	29
8.5.5	Sicherung der Protokolldaten.....	29
8.5.6	Protokollierungssystem	29
8.6	Archivierung	30
8.6.1	Archivierte Daten	30
8.6.2	Aufbewahrungsfristen für Archive	30
8.6.3	Zugang zu Archivdaten und Prüfung von Archivdaten	30
8.7	Notfallplanung	31
8.7.1	Korruption von Hardware, Software und Daten	31
8.7.2	Totaler Verlust bzw. erhebliche Einschränkung der Betriebsstätte des D-CP	31
8.7.3	Notfallvorsorge.....	31
8.8	Infrastrukturelle Sicherheit	32
8.8.1	Zutrittskontrolle, Einbruchmeldeanlage und Videoüberwachung.....	32
8.8.2	Stromversorgung	32
8.8.3	Klimaanlage	32
8.8.4	Schutz gegen Wasserschäden	32
8.8.5	Schutz gegen Feuer	33
8.8.6	Safes.....	33
9	EINSTELLEN DES BETRIEBES DES D-CP.....	33
9.1	Endgültige Einstellung des Betriebs einer D-CP in Deutschland.....	33
9.2	Übergabe des Betriebs an eine andere Organisation.....	33
10	AUDIT	33
10.1	Externe Audits.....	33
10.1.1	Gegenstand des externen Audits	33
10.1.2	Person des externen Auditors	34
10.1.3	Handlungen nach unzureichendem Ergebnis	34
10.1.4	Bekanntgabe von Ergebnissen.....	34
10.2	Interne Audits	34
10.2.1	Gegenstand des Audits	34
10.2.2	Person des internen Auditors.....	34
10.2.3	Handlungen nach unzureichendem Ergebnis	34
10.2.4	Bekanntgabe von Ergebnissen.....	34



11 ÄNDERUNGSPROZEDUREN..... 35

11.1 Änderungen ohne gesonderte Mitteilungen..... 35

11.2 Änderungen mit gesonderter Mitteilung..... 35

11.3 Einholen der Genehmigung 35

12 ÜBEREINSTIMMUNG MIT DER D-MSA-POLICY 36

12 GLOSSAR 39



Abbildungsverzeichnis

Abbildung 1: Gesamtübersicht 10
Abbildung 2: Zertifizierungsinfrastruktur nach der EU-Verordnung 11



Tabellenverzeichnis

Tabelle 1: Historie Dokument	2
Tabelle 2: Die Organisationen gemäß D-MSA-Policy in der Bundesrepublik Deutschland	10
Tabelle 3: Funktionen des D-CP	12
Tabelle 4: Rollentrennung	25
Tabelle 5: Übereinstimmung mit der D-MSA-Policy	38
Tabelle 6: Glossar	40

1 Einführung

Dieses Dokument ist das Practice Statement der Personalisierungsstelle für das Kontrollgerätsystem der Bundesrepublik Deutschland. Es stellt in Verbindung mit den referenzierten, nicht öffentlichen Dokumenten (u. a. Betriebs- und Sicherheitskonzept) das Practice Statement, wie in der D-MSA-Policy gefordert dar.

Dieses Practice Statement berücksichtigt nicht die Gegebenheiten der DC-A. Diese sind den Practice Statements der betreffenden Stelle zu entnehmen.

Dieses PS befindet sich in Übereinstimmung mit

- der Verordnung der EU-Kommission für das Kontrollgerätsystem (2135/98)¹,
- der EU-Verordnung zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr (561/2006)
- der Verordnung der EU-Kommission 1360/2002,
- der Nationalen Policy der MSA der Bundesrepublik Deutschland, Version 1.3, 24.11.2008

1.1 Verantwortliche Organisation

Für dieses PS ist der D-CP im Kraftfahrt-Bundesamt verantwortlich.

1.2 Genehmigung

Dieses PS Version 1.0 des D-CP ist durch die MSA (Bundesministerium für Verkehr, Bau- und Stadtentwicklung) am 13.07.2010 genehmigt worden.

¹ Im Folgenden nur kurz als EU-Verordnung bezeichnet.



1.3 Veröffentlichung und Kontakt

Dieses PS ist öffentlich unter www.kba.de abrufbar.

Fragen zu diesem PS des D-CP sind zu richten an:

Kraftfahrt-Bundesamt
Björn Hansen, Leiter des D-CP
Fördestr. 16
24932 Flensburg
Tel.: 0461-316-1240
Fax: 0461-316-1822
bjoern.hansen@kba.de

1.4 Überblick

1.4.1 Organisatorische Struktur

Die ERCA wurde eingerichtet, um die EU-Verordnung technisch und organisatorisch umzusetzen. Sie steht an der Spitze eines hierarchischen Systems, dem die MSA der einzelnen Mitgliedsstaaten angeschlossen sind. Dabei wird das Ziel verfolgt ein konsistentes und sicheres System zu etablieren. Der D-CP ist die Personalisierungsstelle der Bundesrepublik Deutschland.

In jedem Mitgliedsstaat wird eine MSA entsprechend der EU-Verordnung eingerichtet. Von ihr werden die Wahrnehmung der Aufgaben im Rahmen der EU-Verordnung in ihrem jeweiligen Mitgliedstaat verantwortet, also die Ausgabe der Karten für das Kontrollgerätsystem und die Ausgabe der Zertifikate und Schlüssel für die Geräte des Kontrollgerätsystems. Diese Aufgaben werden in der Bundesrepublik Deutschland durch die D-MSA in Übereinstimmung mit der Policy wahrgenommen.

Die MSA ernennt die CIA, die MS-CA und den MS-CP in ihrem jeweiligen Mitgliedsstaat. Die CIA übernimmt dabei die Gesamtverantwortung für die Ausgabe der Karten, die MSCA das Zertifikats- und Schlüsselmanagement, und der MS-CP die Personalisierung der Karten. Karteninhaber sind dabei Fahrer, Werkstätten, Transportunternehmen und Kontrollorgane. In Abbildung 1 ist der Gesamtüberblick über das Kontrollgerätsystem dargestellt.

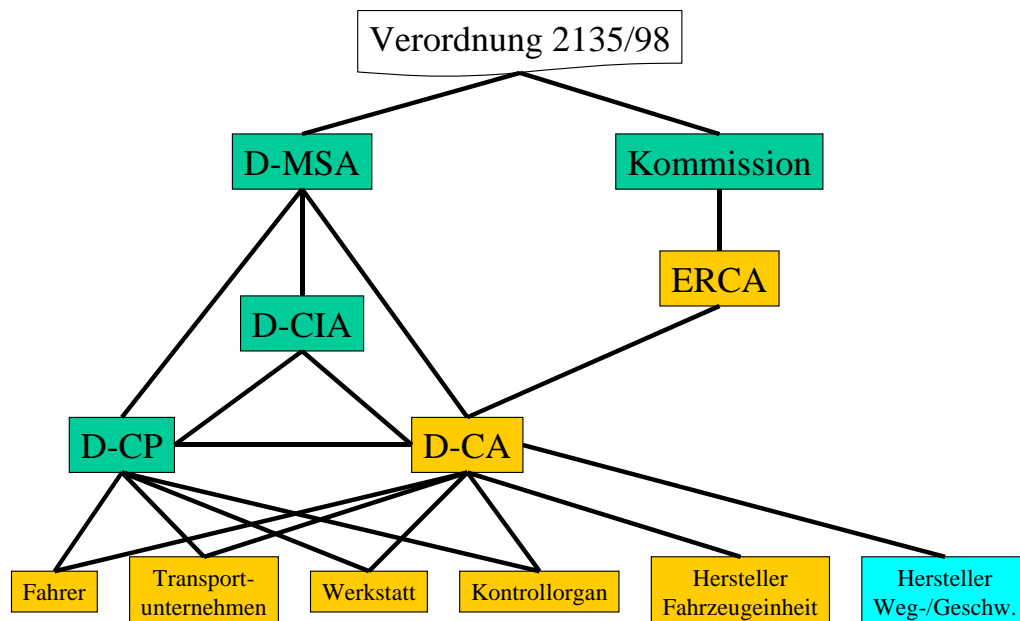


Abbildung 1: Gesamtübersicht

In der Bundesrepublik Deutschland werden diese Rollen von folgenden Organisationen wahrgenommen:

Rolle	Organisation
MSA	D-MSA
CIA	D-CIA [Register beim KBA, Führerscheinstellen]
MSCA	D-CA beim Kraftfahrt-Bundesamt
CP	D-CP beim Kraftfahrt-Bundesamt
NCA	Dieses Organisationsmodell wird nicht gewählt.

Tabelle 2: Die Organisationen gemäß D-MSA-Policy in der Bundesrepublik Deutschland

Der D-CP ist verantwortlich für

- die Personalisierung von Kontrollgerätkarten,

Diese Aufgabe nimmt der D-CP selbst wahr, d. h. eine nach der EU-Verordnung mögliche Unterbeauftragung an Dienstleister erfolgt nicht.

1.4.2 Zertifizierungsinfrastruktur

Die ERCA erzeugt ein asymmetrisches kryptografisches Schlüsselpaar, das aus einem geheimen und einem öffentlichen Schlüssel besteht. Die D-CA erzeugt ihrerseits die Mitgliedsstaatschlüssel (Schlüsselpaare der D-CA). Öffentliche Schlüssel der D-CA werden durch die ERCA

beglaubigt, indem öffentliche Schlüssel der D-CA unter Verwendung des geheimen Schlüssels der ERCA digital signiert werden. Das so erstellte Zertifikat kann mittels des öffentlichen Schlüssels der ERCA überprüft werden.

Die D-CA stellt ihrerseits durch Verwendung eines ihrer geheimen Schlüssel Zertifikate für Karten und für Geräte des Kontrollgerätsystems aus. Zertifikatsinhaber sind Fahrer, Werkstätten, Transportunternehmen, Kontrollorgane und Fahrzeugeinheiten. Die Zertifizierungsinfrastruktur nach der EU-Verordnung weist die Besonderheit auf, dass nur die Kontrollorgane auf die Korrektheit der Zertifikate vertrauen. Diese können anhand des von der ERCA für die D-CA ausgestellten Zertifikats überprüft werden. Die Abbildung 2 stellt die Zertifizierungshierarchie dar.

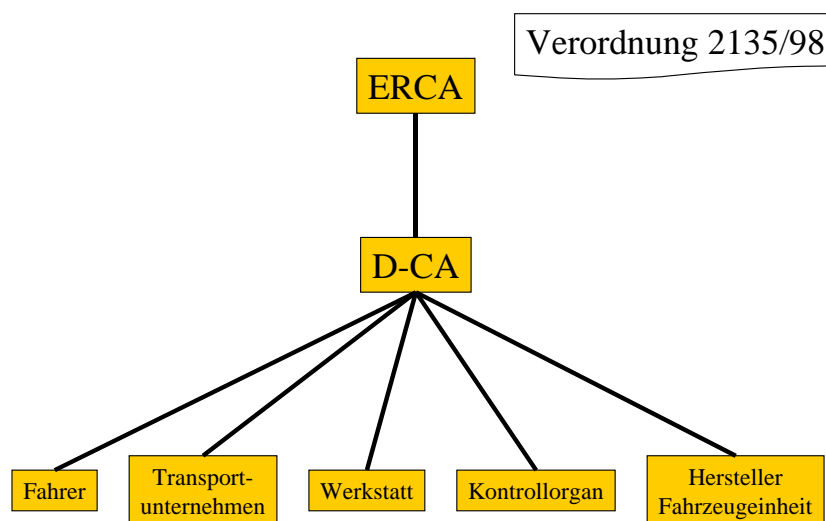


Abbildung 2: Zertifizierungsinfrastruktur nach der EU-Verordnung

Die so aufgebaute Zertifizierungshierarchie wird als zweistufig bezeichnet und erlaubt unter Kenntnis des öffentlichen Schlüssels der ERCA eine Überprüfung aller Zertifikate, die durch eine MSCA ausgestellt worden. Dabei ist zu beachten, dass kein sogenanntes selbstsigniertes Wurzelzertifikat von der ERCA erzeugt wird.

1.4.3 Funktionen des D-CP

Die folgende Tabelle enthält die möglichen Funktionen einer MSCA nach der EU-Verordnung und welche davon von dem D-CP wahrgenommen werden:

Funktion	Verantwortliche Organisation in der Bundesrepublik Deutschland
Bestellabwicklung der Kontrollgerätkarten	D-CP
Personalisierung von Kontrollgerätkarten	D-CP
Sicheres Einbringen der Schlüssel für die Karten	D-CP
Versand von Kontrollgerätkarten	D-CP



Tabelle 3: Funktionen des D-CP

1.5 Geltungsbereich

Dieses PS ist ausschließlich für die Wahrnehmung von Aufgaben des D-CP nach der EU-Verordnung verbindlich. Die in diesem Rahmen vom D-CP hergestellten Kontrollgerätkarten dürfen ausschließlich im Rahmen des Kontrollgerätsystems verwendet werden.



2 Allgemeine Bestimmungen

2.1 Pflichten des D-CP

Der D-CP übernimmt folgende Pflichten:

- in Übereinstimmung mit der Policy der D-MSA und mit diesem PS zu handeln,
- dieses PS von der D-MSA genehmigen zu lassen und zu veröffentlichen,
- das Haftungsrisiko im Zusammenhang mit dem Betrieb des D-CP zu beschränken,
- die in der Policy der D-MSA aufgeführten Anforderungen zu erfüllen,
- sicherzustellen, dass dieses PS des D-CP ordnungsgemäß implementiert wird,
- mindestens ein jährliches Audit durchzuführen,
- beabsichtigte Änderungen dieses PS im Vorfeld bekannt zu geben und nach Zustimmung der D-MSA die revidierte Fassung zur Verfügung zu stellen,
- die Beziehungen zur DC-A, zu den Ausgabestellen und den Kartenlieferanten zu regeln.

2.2 Pflichten externer Organisationen

In diesem Abschnitt werden die Pflichten der DC-A, der Ausgabestellen und der Kartenlieferanten in Übereinstimmung mit der CA-Policy der D-MSA und diesem PS und den darin festgelegten Prozessen dargestellt.

2.2.1 Pflichten der DC-A

Die D-CA übernimmt folgende Pflichten:

- in Übereinstimmung mit der CA-Policy der D-MSA und den ihn betreffenden Teilen dieses PS zu handeln.
- beabsichtigte Änderungen seines PS bekannt zugeben und nach Zustimmung der D-MSA die revidierte Fassung zur Verfügung zu stellen.

Mit den in diesem PS beschriebenen Abläufen muss die DC-A folgende besondere Verpflichtungen erfüllen:

- Die D-CA muss ein sicheres Erzeugen und Verwalten der Signaturschlüssel der MS-CA gewährleisten.



- Die D-CA muss die Zertifikate an den Kartenpersonalisierer und die Hersteller von Fahrzeugeinheiten verteilen.
- Die D-CA muss sicherstellen, dass die digitale Kommunikation mit dem D-CP über das vorgeschriebene VPN erfolgt.
- Die D-CA muss ein sicheres Management und eine sichere Verteilung der Schlüssel für die Weg-/Geschwindigkeitsgeber, die Werkstattkarten und die Fahrzeugeinheiten gewährleisten.
- Die DC-A muss die Daten für die Weg-/Geschwindigkeitsgeber verschlüsseln

2.2.2 Pflichten der Ausgabestellen (CIAs)

Die CIA's übernehmen folgende Pflichten:

- in Übereinstimmung mit der D-MSA-Policy und den ihn betreffenden Teilen dieses PS zu handeln.

Mit den in diesem PS beschriebenen Abläufen müssen die CIA's folgende besonderer Verpflichtung erfüllen:

- in Übereinstimmung mit der D-MSA Policy und den sie betreffenden Teilen dieses PS zu handeln.

2.2.3 Pflichten der Hersteller von Fahrzeugeinheiten

Der Hersteller von Fahrzeugeinheiten übernimmt folgende Pflichten:

- in Übereinstimmung mit der CA-Policy der D-MSA und den ihn betreffenden Teilen dieses PS zu handeln.

Mit den in diesem PS beschriebenen Abläufen muss der Hersteller von Fahrzeugeinheiten folgende besondere Verpflichtungen erfüllen:

- Der Hersteller von Fahrzeugeinheiten muss sicherstellen, dass das Personal, welches die Zertifikatsanträge in seinem Namen an die D-CA übermittelt, über gültige RA-Zertifikate der RA-CA verfügt. Diese Zertifikate werden nur für natürliche Personen von der RA-CA ausgestellt. Die D-CA muss darüber informiert werden, wenn der Mitarbeiter ausscheidet oder wenn er nicht mehr berechtigt ist, digitale Signaturen im Auftrag des Herstellers im Rahmen dieses PS zu erzeugen.
- Der Hersteller von Fahrzeugeinheiten muss sicherstellen, dass die digitale Kommunikation mit der D-CA über das von der D-CA vorgeschriebene VPN erfolgt.



- Der Hersteller von Fahrzeugeinheiten muss den öffentlichen Schlüssel der ERCA, das D-CA-Zertifikat und die ausgestellten Zertifikate unmittelbar nach Erhalt bzw. Abholung auf Integrität und Authentizität prüfen.
- Der Hersteller von Fahrzeugeinheiten ist verpflichtet, das von der D-CA ausgestellte Zertifikat nur in die zugehörige Fahrzeugeinheit des Kontrollgerätsystems nach EU-Verordnung einzubringen, welche in der Bundesrepublik Deutschland eine gültige Bauartgenehmigung besitzt.
- Der Hersteller von Fahrzeugeinheiten muss die D-CA davon unterrichten, wenn RA-Zertifikatsinhaber seine Organisation verlassen oder wenn diese Personen nicht mehr länger berechtigt sind, Anträge im Namen des Kartenpersonalisierers zu stellen.

2.2.4 Pflichten der Hersteller von Weg-/Geschwindigkeitsgebern

Der Hersteller von Weg-/Geschwindigkeitsgebern übernimmt folgende Pflichten:

- in Übereinstimmung mit der CA-Policy der D-MSA und den ihn betreffenden Teil dieses PS zu handeln.

Mit den in diesem PS beschriebenen Abläufen muss der Hersteller von Weg-/Geschwindigkeitsgebern folgende besondere Verpflichtungen erfüllen:

- Der Hersteller von Weg-/Geschwindigkeitsgebern muss sicherstellen, dass das Personal, welches die Verschlüsselungsanträge in seinem Namen an die D-CA übermittelt, über gültige RA-Zertifikate der RA-CA verfügt. Diese Zertifikate werden nur für natürliche Personen von der RA-CA ausgestellt. Die D-CA muss darüber informiert werden, wenn der Mitarbeiter ausscheidet oder wenn er nicht mehr berechtigt ist, digitale Signaturen im Auftrag des Herstellers im Rahmen dieses PS zu erzeugen.
- Der Hersteller von Weg-/Geschwindigkeitsgebern muss sicherstellen, dass die digitale Kommunikation mit der D-CA über das von der D-CA vorgeschriebene VPN erfolgt.
- Der Hersteller von Weg-/Geschwindigkeitsgebern muss nach Erhalt bzw. Abholung der Daten, diese auf Integrität und Authentizität prüfen.
- Hersteller von Weg-/Geschwindigkeitsgebern sind verpflichtet, die von der D-CA verschlüsselten Daten nur in den zugehörigen Weg-/Geschwindigkeitsgeber des Kontrollgerätsystems nach EU-Verordnung einzubringen, welches in der Bundesrepublik Deutschland eine gültige Bauartgenehmigung besitzt.
- Der Hersteller von Weg-/Geschwindigkeitsgebern muss die D-CA davon unterrichten, wenn RA-Zertifikatsinhaber seine Organisation verlassen oder wenn diese Personen nicht mehr länger berechtigt sind, Anträge im Namen des Kartenpersonalisierers zu stellen.



2.2.5 Pflichten von Karteninhabern/Antragsteller

Der Karteninhaber übernimmt folgende Pflichten:

- wahrheitsgemäße Angaben über die Antragsdaten zu machen
- wahrheitsgemäße Angaben über vorhandene Karten und Kartenarten zu machen
- auf geeignete Weise sicherzustellen, dass seine Karte nur für den vorgesehenen Zweck benutzt wird und Missbrauch, insbesondere durch Dritte verhindert wird,
- sicherzustellen, dass er nur in Besitz einer einzigen, gültigen Fahrerkarte ist,
- beschädigte und abgelaufene Karten nicht zu verwenden,
- Verlust, Diebstahl, Beschädigung oder Missbrauch bzw. des jeweiligen Schlüssels oder den Verdacht darauf der jeweilig zuständigen Stelle zu melden.

2.2.6 Pflichten der Hersteller von Kontrollgerätkarten

Der Hersteller von Kontrollgerätkarten übernimmt folgende Pflichten:

- Herstellen von Rohlingen für die Produktion von Kontrollgerätkarten nach Anhang Ib der Verordnung (EWG)3821/85
- Initialisierung des Chip in die Karten mit den Schlüsseln KPers, M.SM und M.Aut
- geschützter Versand der Rohlingen an den D-CP.

Pflichten der Inhaber von RA-Zertifikaten

Die Inhaber von RA-Zertifikaten des Kartenpersonalisierers verpflichten sich

- in Übereinstimmung mit der CA-Policy der MSA und diesem PS zu handeln,
- richtige Angaben bei der Registrierung zu machen und bei der Identifizierung und Authentifizierung mitzuwirken,
- nur die von der D-CA zur Verfügung gestellte RA-Chipkarte zur Speicherung seines geheimen Schlüssels zu verwenden,
- die RA-Chipkarte vor Verlust, Diebstahl und Zerstörung zu schützen,
- die zur RA-Chipkarte zugehörige PIN geheim zu halten,
- die RA-Chipkarte nicht an Dritte (insbesondere auch nicht an andere Mitarbeiter) weiterzugeben,
- die D-CA umgehend davon zu informieren:



- wenn der geheime Schlüssel kompromittiert worden ist oder der begründete Verdacht dazu besteht,
- wenn die RA-Chipkarte verloren, gestohlen oder zerstört wurde,
- die zur RA-Chipkarte zugehörige PIN Dritten (vermutlich) bekannt geworden ist,
- wenn er nicht mehr Mitarbeiter des im Zertifikat angegebenen Organisation ist, oder
- wenn er nicht mehr berechtigt ist, Daten im Auftrag seiner Organisation im Rahmen dieser CP digital zu signieren.

2.3 Haftung

Das KBA haftet für sich und das Verschulden seiner Mitarbeiter bei eigenem Verschulden nur bei Vorsatz und grober Fahrlässigkeit. Eine Haftung des D-CP kann nur gegenüber der MSA entstehen.

Der D-CP haftet nach der EU-Verordnung und den einschlägigen gesetzlichen Bestimmungen, die Anwendung auf sein Aufgabengebiet finden. Eine darüber hinausgehende Haftung wird ausgeschlossen. Insbesondere ist jegliche Haftung ausgeschlossen, wenn die Kontrollgerätkarten nicht im Rahmen der EU-Verordnung und der Policy angegebenen Zweck verwendet werden.



3 Karten- und Gerätemanagement

3.1 Übersicht

Die Personalisierung und Verteilung der Karten übernimmt der Kartenpersonalisierer.

3.2 Kartenpersonalisierer

3.2.1 Berechtigung zur Antragstellung

Beantragt werden die Kontrollgerätkarten von Ausgabestellen, die von den Ländern bzw. für das BAG und den BGS von den zuständigen Ministerien benannt werden. Diese Stellen prüfen die rechtliche Voraussetzung für die Antragstellung anhand der vorzulegenden Unterlagen. Die Kommunikation erfolgt über eine browserorientierte Dialogoberfläche oder über eine Schnittstelle für den Programm zu Programm Dialog.

Die RA-Zertifikate werden nur auf schriftlichem Antrag und unter den im Vertrag mit dem Kartenpersonalisierer vereinbarten Bedingungen ausgestellt.

Der Kartenpersonalisierer verpflichtet sich, nur für das Kontrollgerätsystem nach EU-Verordnung zugelassene Karten zu personalisieren. Die Beauftragten der Hersteller können für jeden Missbrauch verantwortlich gemacht werden.

Die Auftragseinlastung in der Personalisierungsstelle geschieht über den KBA internen Bestellservers. Nach der Übernahme der Daten vom Bestellservers kann die weitere Datengenerierung automatisch ablaufen.

3.2.2 Zertifikatsanträge für Karten

Der Kartenpersonalisierer bestätigt mit seiner digitalen Signatur unter dem Antrag/Sammelantrag für Kartenzertifikate, dass der jeweilige Antragsteller nach den Regelungen der MSA einen gültigen Antrag gestellt hat.

Die D-CA prüft den Antrag/Sammelantrag auf Integrität, Korrektheit und Vollständigkeit. Insbesondere wird anhand der digitalen Signatur geprüft, ob der Unterzeichnende berechtigt ist, diese Anträge an die D-CA weiterzuleiten. Die Berechtigungsprüfung erfolgt anhand einer Positivliste. Die Prüfungen erfolgen auf dem Zertifizierungssystem.

Nicht integere, unkorrekte, unvollständige und unberechtigte Anträge/Sammelanträge und solche, deren Signatur fehlt oder nicht gültig ist, werden von der D-CA zurückgewiesen. Dieser Vorgang wird protokolliert und dem ISSO gemeldet.



Bei positiver Prüfung werden die einzelnen Anträge bearbeitet und bei korrektem Datensatz die entsprechenden Zertifikate ausgestellt. Die Zertifikate, die zugeordneten Anträge und die Seriennummern der Karten werden in einer Datenbank gespeichert.

4 Schlüsselmanagement

4.1 Überblick

Dieses Kapitel beinhaltet das Schlüsselmanagement von folgenden Schlüsseln:

- Der öffentliche Schlüssel der ERCA wird zur Überprüfung des Zertifikats von MS-CAs benötigt.
- Das asymmetrische Schlüsselpaar der D-CA wird zum Ausstellen und Prüfen von Karten- und Gerätezertifikaten verwendet.
- Symmetrische Schlüssel werden für die gegenseitige Authentisierung zwischen den Fahrzeugeinheiten und Weg-/Geschwindigkeitsgeber verwendet und in Werkstattkarten eingebracht.
- Symmetrische Transportschlüssel werden für die sichere Kommunikation zwischen der ERCA und D-CA benötigt.

4.1.1 Pflichten des Kartenpersonalisierers

Der Kartenpersonalisierer muss den öffentlichen Schlüssel der ERCA in jede ausgestellte Karte einbringen.

4.2 Schlüsselpaare der D-CA

4.2.1 Verwendungszweck

Die Schlüssel der D-CA sind diejenigen Schlüssel der D-CA, die für die Zertifizierung im Rahmen der EU-Verordnung verwendet werden. Der geheime Schlüssel der D-CA darf ausschließlich für das Ausstellen von Zertifikaten für Karten und Geräte im Rahmen der EU-Verordnung verwendet werden.

Davon zu unterscheiden sind die asymmetrischen Signaturschlüssel der RA-CA, die ausschließlich zur Absicherung der Kommunikation zwischen den beteiligten Parteien verwendet werden. Diese Schlüssel werden in diesem Abschnitt nicht betrachtet.



5 Schlüssel für Karten

5.1 Allgemeines

Die Initialisierung, das Einbringen der Schlüssel und die Personalisierung der Karten findet ausschließlich beim Kartenpersonalisierer statt.

Die D-CA erzeugt und/oder speichert keine geheimen Schlüssel von Karten oder Fahrzeugeinheiten. Dies trifft auch auf eventuell notwendige Aktivierungsdaten (PINs) von Karten zu.

Der D-CP ist vertraglich verpflichtet nur solche Zertifikatsanträge zu stellen, die in Übereinstimmung mit der EU-Verordnung, der CA-Policy und diesem PS stehen (insbesondere Zuständigkeitsbereich).

Technische Vorkehrungen der D-CA stellen sicher, dass Zertifikatsanträge, für die die D-CA nicht zuständig ist, zuverlässig abgewiesen werden.

5.2 Schlüsselerzeugung

Die Schlüssel für Karten werden ausschließlich vom Kartenpersonalisierer erzeugt.

5.3 Dauer der Verwendung von Schlüsseln

Karten dürfen nicht über den Ablaufzeitpunkt des zugehörigen Zertifikats hinaus verwendet werden.

5.4 Archivierung der öffentlichen Schlüssel

Die D-CA archiviert regelmäßig alle ausgestellten Zertifikate und damit auch die öffentlichen Schlüssel der Karten und Fahrzeugeinheiten.

6 Zertifikatsmanagement für die Karten

Dieses Kapitel beschreibt das Zertifikatsmanagement für die Karten.

6.1 Anträge und Antragsdaten

Der D-CP bearbeitet die Kartenanträge der zugelassenen Ausgabestellen. Die Zertifikatsanträge für Tachografenkarten werden ausnahmslos über den Kartenpersonalisierer von der D-CA entgegengenommen.

Indem der Kartenpersonalisierer die Zertifikats(sammel)anträge mit einem seiner RA-Schlüssel digital signiert, versichert er, dass er die Karten mit den dazugehörigen Zertifikaten nur an End-



benutzer und Ausgabestellen weiterleitet, die einen erfolgreichen Antrag auf eine dem beantragten Zertifikatstyp entsprechende Karte gestellt haben.

Der Kartenpersonalisierer erstellt einen Zertifikatsantrag, der u. a. die CHR und den zu zertifizierenden öffentlichen Schlüssel enthält und mit dem zugehörigen geheimen Schlüssel unterschrieben wird (PKCS#10-Format). Die D-CA prüft diese digitale Signatur, um sicher zu stellen, dass der Kartenpersonalisierer auch den zugehörigen geheimen Schlüssel erzeugt hat. Der geheime Schlüssel selbst wird dabei nicht übertragen. Ist diese Signatur nicht korrekt, wird der Zertifikatsantrag abgelehnt.

6.2 Gültigkeitsdauer der ausgestellten Zertifikate

Die Zertifikate werden in der Regel mit folgender Gültigkeitsdauer ausgestellt:

- Fahrerzertifikate 5 Jahre und sechs Monate,
- Werkstattzertifikate 1 Jahr und sechs Monate,
- Kontrollzertifikate 5 Jahre und sechs Monate,
- Unternehmenszertifikate 5 Jahre und sechs Monate.

Die Zertifikate für Ersatzkarten werden mit einer Gültigkeit ausgestellt, die die ursprüngliche Gültigkeit der zu ersetzenden Karte nicht übersteigt. Diese Gültigkeit schließt der Kartenpersonalisierer in seinen Zertifikatsantrag ein. Die D-CA überprüft diese Angaben anhand ihrer Datenbank. Wäre das Zertifikat für die Ersatzkarte weniger als 6 Monate gültig, stellt die D-CA ein Zertifikat mit der oben angegebenen Gültigkeit aus.

7 Sicherung der Kommunikation zwischen dem D-CP und seinen Vertragspartnern

7.1 Allgemeines

Als Vertragspartner des D-CP werden im Folgenden diejenigen (juristischen) Personen verstanden, die von ihm regelmäßig Dienstleistungen beanspruchen. Dazu gehören die Ausgabestellen der Länder und die D-CA.

8 Sicherheitsmanagement

8.1 Allgemeines

Der D-CP etabliert seine Aufgaben angemessene Abläufe und Prozesse, entsprechend anerkannter Standards. Diese werden in einem Sicherheitskonzept nach [BS] und im Betriebshandbuch dokumentiert. Beide Dokumente sind vertraulich und werden im Gegensatz zu diesem PS nicht veröffentlicht.



Der D-CP trägt die Verantwortung für alle in diesem PS beschriebenen Abläufe und Prozesse. Dieses PS regelt weiterhin die Verpflichtungen von Vertragspartnern des D-CP wie die D-CA und die Ausgabestellen.

Die Sicherheitsinfrastruktur und das Sicherheitsmanagement des D-CP ist Teil der Infrastruktur und des Managements des KBA. Zusätzliche Maßnahmen werden in diesem PS und dem Sicherheitskonzept nach den Vorgaben der Policy festgelegt. Alle Änderungen des PS werden der MSA mitgeteilt. Die Sicherheitsinfrastruktur und das Sicherheitsmanagement des D-CP wird ständig gepflegt und weiterentwickelt, falls es Anpassungen an eine neue Bedrohungslage oder an geänderte gesetzliche oder vertragliche Rahmenbedingungen dies erfordern.

8.2 Risikomanagement

Der D-CP klassifiziert die Informationen in seinem Bereich hinsichtlich der Vertraulichkeit, der Integrität und der Verfügbarkeit. Die Nachvollziehbarkeit aller Prozesse und Abläufe wird dabei besonders berücksichtigt. Dazu werden Sicherheitsanforderungen für die einzelnen Systeme des D-CP festgelegt und im Sicherheitskonzept dokumentiert.

Der D-CP stellt sicher, dass bedrohte Objekte und Informationen angemessen nach den Vorgaben der Policy geschützt werden. Der D-CP führt dazu eine Risikoanalyse durch, um die Geschäftsrisiken zu bewerten und geeignete Sicherheitsmaßnahmen und Betriebsabläufe festzulegen, die im Sicherheitskonzept bzw. Betriebshandbuch dokumentiert werden.

8.3 Personelle Sicherheitsmaßnahmen

8.3.1 Rollen mit besonderem Vertrauen

Die folgenden besonders vertrauenswürdigen Rollen werden für den Betrieb des D-CP eingerichtet:

- Verantwortlicher des D-CP
- ISSO (Sicherheitsbeauftragter)
- Sicherheitsadministrator
- Key-Manager
- Qualitätsmanager
- RA-Karteninhaber
- Systemadministrator



Jeder Rolle wird jeweils eine Person mit mindestens einem Stellvertreter zugeordnet. Für diese Personen werden Berechtigungen auf den Systemen des D-CP eingerichtet, die auf jene eingeschränkt sind, die diese Personen gemäß ihrer Rolle benötigen.

Die Rolle des **D-CP-Verantwortlichen** umfasst u.a. folgende Aufgaben und Verantwortlichkeiten:

- Leitung der Personalisierungsstelle
- Qualitäts-, Sicherheits-, Personal-, Gebäude- und Zutrittsmanagement, Weisungsbefugnis
- Gewährleistung des sicheren und störungsfreien Betriebs der Personalisierungsstelle
- Überwachung der Produktion (auch zuständig bei nicht produzierbaren Karten) und der anderen Rollen innerhalb des D-CP
- Feststellung von Schulungsbedarf und Veranlassen von Schulungen
- Planung und Überwachung des Change-Managements
- Durchführung der Rechnungsstellung
- Ausgabe der PIN-Briefe an Mitarbeiter.

Die Rolle des **ISSO-CP** (Sicherheitsbeauftragten) umfasst u.a. folgende Aufgaben und Verantwortlichkeiten:

- die Überwachung und Kontrolle der Sicherheit der Geschäftsprozesse sowie die Einhaltung und Wirksamkeit der Sicherheitsmaßnahmen des D-CP durch interne Audits,
- Fortschreibung des Sicherheitskonzeptes
- Erstellung von Sicherheitsleitlinien.
- Veranlassung und Durchführung von Sicherheitsaudits und Penetrationstests.
- Initiierung von Schulungen und Sensibilisierungsmaßnahmen.

Die Rolle des **Sicherheitsadministrators-CP** umfasst u.a. folgende Aufgaben und Verantwortlichkeiten:

- Umsetzung und Überwachung der Beteiligung bei Sicherheitsmaßnahmen,
- Überwachung der ordnungsgemäßen Ausführung der einzelnen sicherheitsrelevanten Tätigkeiten,
- Konfiguration und Betrieb der Authentisierungs- und Autorisierungsmechanismen (inklusive der Vergabe von Passwörtern) auf Basis des Berechtigungskonzeptes,



- Überprüfung der Vertrauenswürdigkeit, Zuverlässigkeit und Sicherheit der eingesetzten Systeme,
- Festlegung von Zutritts-, Zugangs- und Systemberechtigungen,
- Regelmäßige Auswertung (mindestens wöchentlich) von Protokolldaten, um Verletzungen der Sicherheitsvorgaben zu erkennen,
- Überwachung der Schlüsselerzeugung,
- Erstellung von Statusreports zur Sicherheit.

•

Die Rolle des **Key-Managers-CP** umfasst u.a. folgende Aufgaben und Verantwortlichkeiten:

- Schlüsselerzeugung für den D-CP,
- Freischalten/Starten des Schlüsselmanagementsystems (zum Generieren, Importieren und Exportieren von Schlüsseln) zusammen mit ISSO-CP und RA-Karten,
- Produktion der Systemkarten zusammen mit SAD-CP und gemeinsame Protokollierung,
- Ausgabe der Systemkarte an die Mitarbeiter.

Das Sicherheitskonzept und das Betriebshandbuch legen weitere Aufgaben und Verantwortlichkeiten fest bzw. verfeinern hier aufgeführte Punkte. Viele der angeführten Aufgaben dürfen nur im Vier-Augen-Prinzip durchgeführt werden und werden vom Sicherheitsbeauftragten überwacht.

Die Rolle des **Qualitätsmanager** umfasst u.a. folgende Aufgaben und Verantwortlichkeiten:

- Planung und Dokumentation von qualitätssichernden Maßnahmen,
- Überwachung, Koordination und Durchführung von Qualitätskontrollen,
- Veranlassung von Nachproduktionen von Kontrollgerätkarten und PIN-Briefen.

Die Rolle des **RA-Karteninhabers** umfasst u.a. folgende Aufgaben und Verantwortlichkeiten:

- Beantragung, Abholung der RA-Chipkarte, des PIN-Briefs und des Datenträgers mit einem Schlüssel Km_{WC} bei der DCA,
- Generieren, Importieren und Exportieren von Schlüsseln,
- Einbringung und Bereitstellung des RA-CA-Zertifikats in bzw. für das Schlüsselssystem.

Die Rolle des **Systemadministrator** umfasst u.a folgende Aufgaben und Verantwortlichkeiten:

- Verantwortlich für den reibungslosen Betrieb der Netzwerkkomponenten und der IT-Systeme,



- Administration und Wartung der Systeme der Personalisierung bei sicherheitsrelevanten Aufgaben,
- Auswertung von System- und Event-Protokollen,
- Unterstützung beim Wiederherstellen von Systemen und Einspielen von Datensicherungen.

Die dezidierten Rollenbeschreibungen sind im nicht-öffentlichen Rollenkonzept von D-CA und D-CP enthalten.

8.3.2 Rollentrennung

Rollen werden nicht von ein und derselben Person wahrgenommen, wenn in der folgenden Tabelle ein Kreuz eingetragen ist:

	DCP Verantwortlicher	ISSO	Sicherheitsadministrator	Key-Manager	Qualitätsmanager	RA-Karteneinhaber	Schlüsselmanager	Systemadministrator
D-CP-Verantwortlicher	-	x	x	x	x	x	x	x
ISSO	x	-	x	x	x	x	x	x
Sicherheitsadministrator	x	x	-	x	x	x	x	x
Key-Manager	x	x	x	-	x	x	x	x
Qualitätsmanager	x	x	x	-	-	-	x	x
RA-Karteneinhaber	x	x	x	x	-	-	x	x
Systemadministrator	x	x	-	x	x	x	x	x

Tabelle 4: Rollentrennung

Diese Unvereinbarkeit von Rollen wird auch bei Wechsel von Rollen innerhalb des D-CP beachtet.

8.3.3 Identifizierung und Authentisierung

Gegenüber Hard- und Software erfolgt die Authentisierung mittels spezifischer Systemkarten mit persönlicher PIN.



Die Systeme des D-CP befinden sich in besonders Zutrittskontrollierten Bereichen des KBA. Beim Zutritt zu diesen Bereichen werden die Personen durch Besitz eines Zugangsmoduls authentisiert.

8.3.4 Anforderungen an das Personal

Die besonders vertrauenswürdigen Rollen werden nur durch Personen besetzt,

- bei denen es keine Zweifel hinsichtlich ihrer Vertrauenswürdigkeit, Integrität und Loyalität gibt,
- die Sicherheitsbewusstsein in ihren bisherigen Aufgaben demonstriert haben,
- bei denen es keine Konflikte ihrer Rolle innerhalb des D-CP mit ihren übrigen Aufgaben und Verantwortlichkeiten gibt,
- von denen bisher nicht bekannt ist, dass sie in früheren Anstellungen oder Dienstverhältnissen fahrlässig oder nachlässig gehandelt haben,
- die entsprechend ihrer Aufgaben ausreichend geschult worden sind,
- die deutsche Staatsbürger sind.

Der Verantwortliche für den D-CP legt in der Stellenbeschreibung für die zu besetzenden Rollen des D-CP, die notwendige Qualifikation fest, die zur Übernahme der Aufgaben und Verantwortlichkeiten notwendig sind.

8.3.5 Schulungen

Bevor das Personal seine Tätigkeit aufnehmen kann, wird es entsprechend seiner einzunehmenden Rolle geschult. Die Schulungen in Sicherheitsbelangen (z. B. Brandschutz) werden mindestens einmal im Jahr durchgeführt. Bevor Änderungen an den Systemen in den Produktivbetrieb übergehen, wird das von den Änderungen betroffene Personal auf den neuen Systemen geschult. Nach Sicherheitsvorfällen werden anlassbezogene Schulungen durchgeführt, die dazu beitragen, solche Vorfälle in Zukunft zu vermeiden.

Nach Veränderungen der gesetzlichen bzw. vertraglichen Rahmenbedingungen wird das Personal des D-CP themenbezogen geschult. Insbesondere wird das Personal von Änderungen der D-MSA-Policy, dieser PS, des Sicherheitskonzepts und des Betriebshandbuchs unterrichtet und gegebenenfalls geschult.



8.4 Technische Sicherheitsmaßnahmen

8.4.1 Allgemeine technische Maßnahmen

Es wird gewährleistet, dass der Betrieb des D-CP sicher, korrekt und störungsfrei erfolgt. Insbesondere wird die Integrität der Systeme und Informationen gegen Viren, schädigende und nicht autorisierte Software geschützt. Sicherheitsrelevante Ereignisse werden dem Sicherheitsbeauftragten (ISSO) und dem Verantwortlichen des D-CP vom Personal mitgeteilt und nach den im Sicherheitskonzept und dem Betriebshandbuch beschriebenen Prozess verfahren.

Das Personalisierungssystem für die Kontrollgerätkarten wird so konfiguriert, dass eine zuverlässige in der D-MSA-Policy und diesem PS beschriebene Rollentrennung sichergestellt wird. Näheres ist hierzu im Rollenkonzept der jeweils aktuellen Version festgelegt.

Die Hardware-Sicherheits-Module, in denen die geheimen Schlüssel des D-CP angewendet werden, können nur im Vier- bzw. Sechs-Augen-Prinzip initialisiert werden.

Die Operatoren werden durch die Zutrittskontroll-Anlage über Besitz zuverlässig authentifiziert. Es werden zuverlässige und sichere Systeme zum Betrieb des D-CP eingesetzt. Darüber hinaus werden Hardware-Sicherheitsmodule eingesetzt, die formale Zertifizierungen besitzen.

Der D-CP setzt vertrauenswürdige Systeme ein, die die installierte Software regelmäßig auf Manipulationen untersucht. Sicherheitssensitive Hardware wird gegen unbemerkte Manipulationen durch geeignet angebrachte Siegel geschützt. Die Ausgabe und Anbringung der Siegel wird protokolliert. Die Unversehrtheit der Siegel wird regelmäßig durch den Sicherheitsadministrator überprüft.

Die geplanten Veränderungen an den Systemen des D-CP werden zunächst bei der Firma Giesecke & Devrient getestet, dokumentiert, und dem Verantwortlichen des D-CP und dem Sicherheitsbeauftragten zur Genehmigung vorgelegt. Jegliche Änderungen an operativen Systemen einschließlich der Änderungen im Notfall werden sorgfältig dokumentiert.

Die definierten Rollen werden auf sämtlichen Systemen durch personenbezogene Benutzerkonten umgesetzt, wobei die Rechte entsprechend der Rolle auf den einzelnen Systemen eingeschränkt sind. Das Berechtigungskonzept und jede Änderung daran wird dokumentiert. Der Sicherheitsbeauftragte genehmigt das Berechtigungskonzept bzw. die Änderungen, bevor diese wirksam werden.

Der Kartenpersonalisierer verfügt über eine Standleitung zur D-CA. Diese Verbindung wird durch eine sichere VPN-Lösung geschützt. Das Netzwerk des KBA wird durch eine Firewall geschützt. Das Netzwerk des D-CP wird durch eine Firewall gegenüber dem KBA-Netz geschützt. Innerhalb des Netzwerks des D-CP gibt es eine weitere Firewall, die das Zertifizierungssystem schützt. Für alle Netzwerksicherheitskomponenten werden Sicherheitsleitlinien aufgestellt. Der Sicherheitsbeauftragte wird vor jeder Änderung der Sicherheitskonfiguration informiert.

Zusätzlich werden sämtliche an den D-CP übermittelten Anträge mit dem geheimen RA-Schlüssel der RA-Zertifikatsinhaber digital signiert. Die Webserver des D-CP unterstützen SSL-



Serverauthentisierung und besitzen Webserver-Zertifikate des Zertifizierungsdienstleisters Telesec.

8.5 Protokollierung sicherheitsrelevanter Ereignisse

8.5.1 Protokollierte Ereignisse

Sicherheitsrelevante Ereignisse werden mit der Angabe von Datum, Uhrzeit und gegebenenfalls dem Namen des Verantwortlichen protokolliert. Dies betrifft:

- Einrichten und Schließen von Benutzerkonten,
- jegliche Transaktion auf den Systemen mit zusätzlicher Angabe von Transaktionstyp und Informationen darüber, ob die Transaktion abgeschlossen wurde bzw. warum sie abgebrochen worden ist,
- Installation und Deinstallation von Software und Software-Updates,
- alle Datensicherungen,
- Starten und Herunterfahren von Systemen,
- Änderungen der Hard- und Softwarekonfiguration,
- Erstellen von Listen mit Protokolldaten,
- Erstellen von Listen mit archivierten Transaktionen.

Folgende Transaktionstypen werden insbesondere aufgezeichnet:

- Anträge der CIAs auf die Erzeugung einer Kontrollgerätkarte,
- Erzeugen von Schlüsseln nach EU-Verordnung.

Die spezifischen Prozesse des D-CP erfordern zusätzlich die Protokollierung folgender Ereignisse:

- Bestätigung des Erhalts der symmetrischen Schlüssel nach EU-Verordnung,
- Bestätigung des Erhalts der RA-Chipkarten und zugehöriger PIN,
- Änderung der Betriebsdokumente (Konzepte, Anweisungen) des D-CP.



8.5.2 Häufigkeit der Überprüfung von Protokolldaten

Die Protokolle des laufenden Betriebs des D-CP werden wöchentlich auf verdächtige Vorkommnisse vom Systemadministrator und dem Sicherheitsadministrator untersucht.

Sicherheitsrelevante Protokolle, die sich aus den Ablaufprozessen des D-CP ergeben, werden im Zuge der Revision auf verdächtige Vorkommnisse und Manipulationen untersucht.

8.5.3 Aufbewahrungszeitraum für Protokolldaten

Die Protokolldaten werden mindestens 7 Jahre aufbewahrt. Sicherheitsrelevante Protokolldateien werden mindestens 10 Jahre aufbewahrt. Dies betrifft insbesondere das Schlüsselmanagement der Signaturschlüssel des D-CP und die Herausgabe der symmetrischen Schlüssel nach der EU-Verordnung.

8.5.4 Schutz der Protokolldaten

Die Einträge in den Protokolldateien enthalten die Systemzeit. Protokolldateien werden auf den Systemen erstellt und elektronisch aufbewahrt. Nur der Systemadministrator und der Sicherheitsadministrator können auf Protokolldaten zugreifen. Die Protokolldateien werden digital signiert, sodass sie vor Modifikation geschützt sind.

Die Protokolldateien werden monatlich vom Systemadministrator und dem Sicherheitsadministrator überprüft und konsolidiert.

8.5.5 Sicherung der Protokolldaten

Die konsolidierten Protokolldaten werden in der Betriebsstätte des D-CP elektronisch gespeichert. Eine Kopie wird im Sicherheitsbereich außerhalb des Betriebsortes archiviert.

Die Protokolldaten werden so verwahrt, dass sie während ihrer Aufbewahrungsfrist von Berechtigten eingesehen werden können. Das bedeutet insbesondere, dass entsprechende Lesegeräte und Auswertungstools zur Verfügung stehen. Die zur Nachprüfung der digitalen Signaturen erforderlichen Zertifikate werden mit den Protokolldaten aufbewahrt.

Die Protokolldaten werden vor nicht autorisiertem Zugang geschützt. Die Anwesenheit des Archivars ist beim Zugriff auf die Protokolldaten erforderlich.

8.5.6 Protokollierungssystem

Die Protokolldateien werden auf den jeweiligen Systemen an ihrem Standort erzeugt.



8.6 Archivierung

8.6.1 Archivierte Daten

Es werden alle für die Nachvollziehbarkeit der Herstellung von Kontrollgerätkarten benötigten Daten archiviert. Dazu gehören insbesondere die Protokolldaten, Revisionsberichte und alle derzeit und in der Vergangenheit implementierten D-MSA Policies und PS's.

8.6.2 Aufbewahrungsfristen für Archive

Archivierte Daten werden für mindestens sieben Jahre aufbewahrt.

Die Sicherungskopien von Systemen werden mindestens so lange aufbewahrt, wie sie für die Wiederherstellung ausgefallener Systemkomponenten im Anwendungszeitraum benötigt werden. Die Verfügbarkeit der Datensicherung ist in der Anlage 1 des internen Betriebskonzeptes beschrieben.

Die Protokolldaten werden sechs Jahre aufbewahrt.

8.6.3 Zugang zu Archivdaten und Prüfung von Archivdaten

Die Archivdaten werden im Safe des Sicherheitsbereiches außerhalb des Betriebsortes verwahrt, wobei der Zugriff nur dazu Berechtigten gestattet ist. Die Zugangs- und Zugriffskontrollen gestatten nur zwei Berechtigten gleichzeitig den Zutritt zum Archiv, wobei immer ein Archivar anwesend sein muss.

Einzelne Transaktionsdaten werden nur an Berechtigte auf Antrag herausgegeben. Der Antragsteller stellt dazu einen schriftlichen Antrag mit der Angabe von Gründen.

Die Berechtigung wird überprüft, wobei neben der EU-Verordnung auch die Datenschutzbestimmungen hinzugezogen werden. Handelt der Antragsteller nicht im eigenen Namen wird zusätzlich die Vollmacht des Berechtigten geprüft. Mindestens muss der Antragsteller bzw. derjenige, den er vertritt, in die Transaktion involviert sein, deren archivierte Daten er einsehen möchte.

Die notwendige Dokumentation, dass der D-CP in Übereinstimmung mit diesem PS steht, wird auf Antrag zur Verfügung gestellt.

Vor technischen Veränderungen sind die Archive auf Lesbarkeit auf dem neuen System zu überprüfen. Ist eine Lesbarkeit mit dem neuen System /der neuen Software nicht gegeben, werden die Archivdaten migriert. Nach der Übertragung der Daten werden diese erneut digital signiert. Ist sichergestellt, dass alle Daten eines bestimmten Archivs in neue Formate bzw. auf neue Systeme übertragen worden sind, werden die ursprünglichen Archive gelöscht.

Bei einer kurzzeitigen Unterbrechung des Betriebs bzw. Suspendierung des D-CP werden die Archive durch das KBA weitergeführt. Bei Einstellung des Betriebs oder länger anhaltenden Betriebsstille bzw. Suspendierung des D-CP werden die Archive an die D-MSA oder einen von



der D-MSA autorisierten Betreiber übergeben. Davon werden die Vertragspartner des DCP unterrichtet.

8.7 Notfallplanung

Der D-CP erstellt ein Notfallkonzept, indem folgende Ereignisse berücksichtigt werden:

- Totaler Verlust bzw. erhebliche Einschränkung der Betriebsstätte des D-CP.

8.7.1 Korruption von Hardware, Software und Daten

Werden Fehler oder Manipulationen an Hardware, Software oder Daten entdeckt, die Auswirkungen auf die Sicherheit des Zertifizierungssystems haben könnten, so werden die betroffenen Komponenten umgehend aus dem Betrieb genommen. Der Sicherheitsbeauftragte und der Verantwortliche des D-CP werden informiert. Zusammen mit dem zuständigen Personal werden die entsprechenden Komponenten ersetzt bzw. Maßnahmen ergriffen, um den zuletzt als sicher eingeschätzten Zustand wieder zu erreichen (z. B. Einspielen von Datensicherungen). Die so wiederhergestellten Systeme werden einer Sicherheitsüberprüfung unterzogen und gegebenenfalls getestet.

Wurden fehlerhafte oder falsche Zertifikate ausgestellt, wird die D-MSA bzw. die D-CIA zeitnah unterrichtet. Betroffene Vertragspartner des D-CP werden umgehend informiert.

Sobald die festgestellten Mängel beseitigt sind, wird der Betrieb des D-CP wieder aufgenommen.

8.7.2 Totaler Verlust bzw. erhebliche Einschränkung der Betriebsstätte des D-CP

Ist die Sicherheit der Betriebsstätte des D-CP erheblich gefährdet, so werden umgehend Maßnahmen zum Schutze ergriffen. Diese Entscheidungen trifft der Verantwortliche des D-CP mit dem Sicherheitsbeauftragten im Katastrophenfall.

Wird die Betriebsstätte des D-CP total oder erheblich zerstört, wird im Rahmen des Notfallkonzepts des KBA der Betrieb in einem Ausweichrechenzentrum aufgenommen. In diesem Fall werden die Systeme entsprechend der an einem sicheren Ort verwahrten Dokumentation wieder aufgebaut und die Systeme mit Hilfe der entsprechenden Sicherheitskopien wiederhergestellt.

8.7.3 Notfallvorsorge

Die Notfallvorsorge des D-CP umfasst die sichere Aufbewahrung folgender Informationen an einem sicheren Ort, der in ausreichender Entfernung von der Betriebsstätte des D-CP liegt:

- Sicherungskopien von digitalen Schlüsseln (Signaturschlüssel und symmetrische Schlüssel nach EU-Verordnung, Signaturschlüssel der RA-CA) in einem Safe,
- Sicherungskopien der aktuellen Systemdokumentation,
- Sicherungskopien zur Wiederherstellung der Systeme,



- Hardware, die nicht zeitnah wiederbeschafft werden kann.

8.8 Infrastrukturelle Sicherheit

Der Zugang zu den Räumen und technischen Komponenten des D-CP (Hardware, Software, Hardware-Sicherheitsmodule, Safes, Datenträgerschränke) wird an die entsprechenden Berechtigungen geknüpft, welche die einzelnen Personen im Rahmen ihrer Rolle wahrnehmen müssen. Diese Berechtigungen werden auf Antrag vom Leiter des D-CP vergeben. Der Zutritt zu den Sicherheitsbereichen wird protokolliert.

8.8.1 Zutrittskontrolle, Einbruchmeldeanlage und Videoüberwachung

Die Zutrittskontrollen sind dem angestrebtem Sicherheitsniveau für einzelne Bereiche (Schalenmodell) angepasst. Die Zutritte werden protokolliert und sind somit jederzeit nachvollziehbar. Besucher werden in ein Besucherbuch eingetragen. Zusätzlich wurden Einbruchmeldeanlagen und Videoüberwachungsanlagen installiert.

Die übrigen Bereiche des D-CP sind gegen unbefugten Zutritt geschützt. Hier erhalten nur solche Personen eine Zutrittsberechtigung, die zur Wahrnehmung ihrer jeweiligen Aufgaben diese Bereiche betreten müssen. Personal, das nur gelegentlich Aufgaben in diesem Bereich wahrnimmt, wird aus diesem Anlass von einem Mitarbeiter ständig begleitet und bei Ausführung seiner Tätigkeiten überwacht.

8.8.2 Stromversorgung

Der D-CP ist an die USV-Komponenten des KBA angeschlossen. Diese sind angemessen dimensioniert. Insbesondere wird die Versorgung der Zutrittskontrollanlage, der Einbruchmeldeanlage und der Videoaufzeichnungsanlage sichergestellt.

8.8.3 Klimaanlage

Der D-CP nutzt die Klimaanlage im Sicherheitsbereich des KBA. Für eine ausreichende Abführung der Wärme der IT-Systeme wird gesorgt. Ein Eindringen unberechtigter Personen über die Lüftungsrohre der Klimaanlage wird ausgeschlossen.

8.8.4 Schutz gegen Wasserschäden

Das Eindringen von Wasser in die IT-Systeme des D-CP wird weitgehend ausgeschlossen. Im Hochsicherheitsbereich wird sich im Bodenbereich ansammelndes Wasser durch Detektoren an die Störungsmeldeanlage übermittelt. Die IT-Systeme sind so aufgestellt, dass sie über ausreichend Bodenfreiheit verfügen. Die Hausmeisterei stellt Mittel bereit, um eingedrungenes Wasser abzuleiten.



8.8.5 Schutz gegen Feuer

Alle Räumlichkeiten des D-CP verfügen über eine geeignete Brandmeldeanlage (Detektoren und Melder), die im Brandfall Polizei und Feuerwehr alarmieren. Es stehen ausreichend geeignete Feuerlöscher zur Verfügung. Der Hochsicherheitsbereich der D-CA verfügt über eine Löschanlage.

8.8.6 Safes

Der Ort an dem die zweiten Sicherungskopien ausgelagert werden, verfügt über ausreichend sichere Safes, die jeweils in gesicherten Räumen aufgestellt sind. Die Safes enthalten Schließfächer, die eine dedizierte Vergabe der Zugriffsberechtigungen gestatten. Die Safes sind zur Aufbewahrung kryptografischer Hardware-Sicherheitsmodule und von Datensicherungen besonders geeignet.

9 Einstellen des Betriebes des D-CP

9.1 Endgültige Einstellung des Betriebs einer D-CP in Deutschland

Die endgültige Einstellung des Betriebs des D-CP in der Bundesrepublik Deutschland erfolgt unter der Verantwortung der D-MSA, die dazu die Anweisung erteilt.

Der D-CP informiert alle ihre Vertragspartner 3 Monate vor dem Einstellen des Betriebs, soweit sie von der Einstellung betroffen sind. Durch die D-MSA wird eine entsprechende Mitteilung im Bundesanzeiger veröffentlicht.

9.2 Übergabe des Betriebs an eine andere Organisation

Die Übergabe des Betriebs des D-CP an einen neuen Betreiber wird im Bundesanzeiger veröffentlicht. Die Vertragspartner des D-CP werden 3 Monate vor dem Wechsel des Betreibers von des D-CP informiert, insofern sie von der Änderung betroffen sind.

10 Audit

10.1 Externe Audits

Sie finden mindestens einmal jährlich statt, um zu prüfen, ob der D-CP in Übereinstimmung mit der D-MSA-Policy und diesem PS betrieben wird. Die Verantwortung liegt beim Leiter des D-CP.

10.1.1 Gegenstand des externen Audits

Prüfgegenstand ist das Feststellen des Grades der Übereinstimmung des Betriebes des D-CP mit der D-MSA-Policy und diesem PS.



10.1.2 Person des externen Auditors

Die D-MSA hat den Leiter der Zertifizierungsstelle für QM-Systeme des KBA (ZSQ) am 24.08.2004 mit der Durchführung regelmäßiger Sicherheitsüberprüfungen beauftragt.

10.1.3 Handlungen nach unzureichendem Ergebnis

Nach unzureichendem Ergebnis eines Audits wird nach den Vorgaben der D-MSA ein Plan erarbeitet, wie der D-CP den Betrieb wieder in Übereinstimmung mit der D-MSA Policy und diesem PS führt. Der Sicherheitsbeauftragte erarbeitet konkrete Maßnahmen und stimmt diese mit der D-MSA ab. Mit der Umsetzung der Maßnahmen wird unmittelbar nach der Zustimmung durch den Verantwortlichen des D-CP begonnen. Sind die festgestellten Mängel behoben, so wird die D-MSA unmittelbar darüber informiert.

10.1.4 Bekanntgabe von Ergebnissen

Ergebnisse von Audits werden durch den D-CP an Dritte nicht bekannt gegeben. Entsprechende Begehren werden an die D-MSA verwiesen. Gemäß den Bestimmungen der ERCA-Policy wird das Gesamtergebnis des Audits der ERCA durch die D-MSA übermittelt.

10.2 Interne Audits

Interne Audits finden mehrmals jährlich statt, um einzelne Arbeitsabläufe zu prüfen.

10.2.1 Gegenstand des Audits

Prüfgegenstand ist das Feststellen der Einhaltung der Vorgaben der D-MSA-Policy, dieses PS, des Betriebshandbuchs, des Sicherheitskonzeptes des D-CP und des Rollenkonzeptes.

10.2.2 Person des internen Auditors

Vom externen Auditor wurde der ISSO als interner Auditor bestimmt.

10.2.3 Handlungen nach unzureichendem Ergebnis

Nach unzureichendem Ergebnis eines internen Audits werden in Abstimmung mit dem Leiter des D-CP Lösungen zur Behebung der festgestellten Mängel erarbeitet.

10.2.4 Bekanntgabe von Ergebnissen

Ergebnisse von internen Audits werden nur dem D-CP und dem externen Auditor übermittelt.



11 Änderungsprozeduren

11.1 Änderungen ohne gesonderte Mitteilungen

Editorische und typografische Änderungen sowie notwendige Aktualisierungen von Ansprechpartnern und Adressdaten werden ohne gesonderte Mitteilung vorgenommen.

11.2 Änderungen mit gesonderter Mitteilung

Beabsichtigte Änderungen dieser PS werden der D-MSA und den betroffenen Parteien mindestens 90 Tage vor Wirksamwerden nachvollziehbar mitgeteilt. Sind die Auswirkungen für die beteiligten Parteien nur vom geringen Ausmaß, so werden die D-MSA und die betroffenen Parteien mindestens 30 Tage vor Wirksamwerden über die beabsichtigten Änderungen nachvollziehbar informiert.

Die betroffenen Parteien werden aufgefordert sich innerhalb von 15 Tagen nach Eingang der Mitteilung zu äußern.

Geht umgekehrt bei der D-CP eine Änderungsmitteilung hinsichtlich der CA Policy oder der PS der D-CA ein, wird der Sicherheitsbeauftragte sich zeitnah mit den Auswirkungen der Änderungen auf den Betrieb des D-CP befassen. Nach Abstimmung mit dem Verantwortlichen des D-CP wird ein schriftlicher Kommentar rechtzeitig formuliert und versendet, sodass die Frist von 15 Tagen eingehalten wird. Insbesondere wird untersucht, ob Änderungen an diesem PS vorgenommen werden müssen.

Werden beabsichtigte Änderungen nach Kommentaren revidiert, so werden die endgültigen Änderungen 30 Tage vor Wirksamwerden der D-MSA und den betroffenen Parteien mitgeteilt.

11.3 Einholen der Genehmigung

Der Verantwortliche des D-CP holt die Genehmigung der D-MSA ein, wenn diese zur Änderung dieses PS notwendig ist.



12 Übereinstimmung mit der D-MSA-Policy

Die Anforderungen für das D-CP-Practice-Statement sind in der D-MSA-Policy in Abschnitt 4 beschrieben. Die nachstehende Tabelle stellt die Verbindung zwischen den in der D-MSA-Policy formulierten Anforderungen und den Anforderungen des D-CP-Practice-Statement dar.

Nr.	Referenz D-MSA Policy	Anforderung	Referenz D-CP-PS
	3 [r3.1]	Aufgaben und Verpflichtungen	1.4.1 Organisatorische Struktur
	3.1 [r3.4]	Aufgaben und Verpflichtungen des D-CP	2.1 Pflichten des DC-P
	3.1 [r3.2]	Aufgaben und Verpflichtungen der D-CA	2.2.1 Pflichten der DC-A
	3.1 [r3.5]	Aufgaben und Verpflichtungen der Karteninhaber/Antragsteller	2.2.5 Pflichten von Karteninhabern
	3.1 [r3.6]	Aufgaben und Verpflichtungen der Hersteller von Fahrzeugeinheiten	2.2.3 Pflichten der Hersteller von Fahrzeugeinheiten
	3.1 [r3.6]	Aufgaben und Verpflichtungen der Hersteller von Weg-/Geschwindigkeitsgebern	2.2.4 Pflichten der Hersteller von Weg-/Geschwindigkeitsgebern
	7.3 [r7.9]	Der D-CP stellt innerhalb ihres Einflussbereichs sicher, dass die jeweiligen privaten Schlüssel ausschließlich zum Zwecke ihrer Bestimmung gemäß der VO(EG) 2135/98 genutzt werden können.	3.2.1 Berechtigung zur Antragstellung
	4 [r4.3]	Das PS muss darlegen, wie die D-CP ihren Informationspflichten nachkommt.	2.1 Pflichten des DC-P 4.1.1 Pflichten des Kartenpersonalisierer 5 Schlüssel für Karten 8 Sicherheitsmanagement 8.2 Risikomanagement 8.3 Personelle Sicherheitsmaßnahmen 8.3.2 Rollentrennung 8.4 Technische Maßnahmen 8.5 Protokollierung sicherheitsrelevanter Ereignisse 10. Audit 11.2 Änderungen mit gesonderten Mitteilungen
	4 [r4.4]	Im PS muss ein Audit beschrieben sein, welches sicherstellt, dass das PS stets dem aktuellen Stand der Gesetzgebung, der Technik und den aktuellen Gegebenheiten bei dem D-CP und ihren externen Dienstleistern entspricht.	2.1 Pflichten des DC-P 10 Audit
	4 [r4.5]	Die D-CP legt der D-MSA ihr PS zur Genehmigung vor.	2.1 Pflichten des DC-P 11.3 Einholen der Genehmigung
	8.3 [r8.8]	Die Gültigkeitsdauer der von der D-CA ausgestellten Zertifikate soll die maximale Verwendungsdauer der zugehörigen Karten bzw. Geräte nicht überschreiten. Zertifikate für: Fahrerkarten sollen nicht länger als 5 Jahre, Werkstattkarten nicht länger als 1 Jahr, Kontrollkarten nicht länger als 5 Jahre, Unternehmenskarten nicht länger als 5 Jahre gerechnet vom Zeitpunkt des Beginns der Gültigkeit der jeweiligen Karte.	6.2 Gültigkeitsdauer der ausgestellten Zertifikate
	9.2 [r9.5]	Die D-CP stellt sicher, dass nur zuverlässiges und ausreichend qualifiziertes Personal mit den erforderlichen Tätigkeiten betraut wird. Dies gilt auch für das Personal bei externen Auftragnehmern.	8.3.4 Anforderungen an das Personal
	9.2 [r9.6]	Die für die Tätigkeit des D-CP eingesetzten IT-Systeme müssen so betrieben werden, dass mögliche Schädigungen durch Viren und anderen schadhafte Code weitestgehend verhindert sowie die möglichen Folgen von	8.3.3 Identifizierung und Authentisierung 8.4.1 Allgemeine technische Maßnahmen 8.8.1 Zutrittskontrolle, Einbruchmeldeanlage und Videoüberwachung



Nr.	Referenz D-MSA Policy	Anforderung	Referenz D-CP-PS
		Schäden und Störungen minimiert werden. Die Systeme müssen über wirksame Zugangskontrollen verfügen und insbesondere die in dieser Policy und den zugehörigen Sicherheits- und Betriebskonzepten beschriebenen Rollenkonzepte wirksam implementieren.	
	9.2 [r9.10]	Alle sicherheitsrelevanten Aktionen und Prozesse auf den für die Tätigkeit des D-CP relevanten IT-Systemen sind so zu protokollieren, dass sich der zugehörige Zeitpunkt und die entsprechenden Personen mit hinreichender Sicherheit nachvollziehen lässt. Dazu gehören zumindest: das Einrichten von Benutzerbereichen (Accounts), alle Transaktions-Anforderungen (Account des Anfordernden, Typ, Status (erfolgreich/nicht erfolgreich), Gründe für das Fehlschlagen, ...), Software-Installationen und -Updates, Hardware-Modifikationen, Herunterfahren und Neustarts des Systems, Zugriff auf Audits und Archive.	8.5.1 Protokolierte Ereignisse
	9.2 [r9.11]	Die Protokolle sind gegen Veränderung und unberechtigten Zugriff zu schützen. Sie sollen regelmäßig und anlassbezogen ausgewertet und analysiert werden.	8.5.2 Häufigkeit der Überprüfung von Protokolldaten 8.5.4 Schutz der Protokolldaten 8.5.5 Sicherung der Protokolldaten 8.6.1 Archivierte Daten
	9.2 [r9.12]	Die Protokolldaten sollen für mindestens 7 Jahre so aufgehoben werden, dass eine Auswertung während dieser Zeitspanne jederzeit möglich ist.	8.6.2 Aufbewahrungsfristen für Archive
	9.2 [r9.13]	Die D-CP erstellt einen Notfallplan, in den das Verhalten bei schwerwiegenden Notfällen festgelegt ist.	8.7 Notfallplanung
	9.2 [r9.14]	Die D-CP gewährleistet einen ausreichenden infrastrukturellen und physischen Schutz ihrer Daten und IT-Systeme. Dieser umfasst insbesondere einen ausreichenden Zutrittsschutz für sicherheitsrelevante Bereiche.	8.6.3 Zugang zu Archivdaten und Prüfung von Archivdaten
	9.3 [r9.15] bis [r9.21]	Durch die Einrichtung von Rollenkonzepten soll verhindert werden, dass einzelne Personen Sicherheitsvorkehrungen des D-CP umgehen. Hierzu werden den einzelnen Rollen jeweils beschränkte Rechte und Pflichten zugewiesen. Die genaue Ausgestaltung hängt von den konkreten Abläufen bei dem D-CP ab und bleibt dem Betriebskonzept des D-CP vorbehalten. Folgende Rollen sind aber mindestens vorzusehen: D-CP-Verantwortlicher Key-Manager (KM) Qualitätsmanager RA-Karteninhaber Sicherheitsadministrator System-Administrator (SysA) IT-Sicherheitsbeauftragter (ISSO) Jede dieser Rollen ist mit mindestens einer Person zu besetzen; mindestens ein Vertreter ist zu benennen. Keine Person darf gleichzeitig mehr als eine dieser Rollen wahrnehmen. Die Inhaber dieser Rollen sind von den IT-Systemen des D-CP zuverlässig zu authentifizieren.	8.3.1 Rollen mit besonderem Vertrauen

Nr.	Referenz D-MSA Policy	Anforderung	Referenz D-CP-PS
	10.1 [r10.1]	Die D-MSA entscheidet über eine Verlegung der D-CP-Verantwortlichkeit. Dafür muss die D-MSA eine neue D-CP benennen.	9.2 Übergabe des Betriebes an eine andere Organisation

Tabelle 5: Übereinstimmung mit der D-MSA-Policy

12 Glossar

Abkürzung	Erklärung
CP-Policy	Policy für das Digitale Tachographensystem der Bundesrepublik Deutschland
D-CA	Die ↑Zertifizierungsstelle der Bundesrepublik Deutschland für das digitale Kontrollgerät gemäß der ↑EU-Verordnung.
D-CIA	Ausgabestellen für Tachografenkarten, Register beim KBA
Digitale Signatur	Verfahren zur Sicherung der Unverfälschtheit (Integrität) und zum Herkunftsnachweis (Authentizität) eines elektronischen Dokuments mittels Anwendung der asymmetrischen Kryptographie.
D-MSA	Die für die Umsetzung der ↑EU-Richtlinie in der Bundesrepublik Deutschland verantwortliche Stelle (Bundesministerium für Verkehr, Bau- und Stadtentwicklung). Nach internationalem Sprachgebrauch (MSA = member state authority)
ERCA	Die europäische ↑Zertifizierungsstelle für den elektronischen Kontrollgerät gemäß der ↑EU-Verordnung.
EU-Verordnung	Verordnung (EU) 2135/98
Fingerabdruck, digitaler	In der asymmetrischen Kryptographie der geheime Teil eines Schlüsselpaars. Dieser dient hier zur Erzeugung einer ↑digitalen Signatur. (s. auch ↑Öffentlicher Schlüssel)
ISSO	Information System Security Officer (Sicherheitsbeauftragter)
Kartenpersonalisierer	Stelle, die asymmetrische Schlüsselpaare und die gemäß ↑EU-Verordnung zugehörigen Zertifikate auf die in der ↑EU-Verordnung definierten Fahrer-, Werkstatt-, Kontroll- und Unternehmenskarten aufbringt.
Kartenpersonalisierer D-CP	Stelle, die in der Bundesrepublik Deutschland, Karten für das Kontrollgerätsystem nach EU-Verordnung personalisiert.
Personalisierung	Auch: logische P. Einbringung von geheimen Schlüsseln und den zugehörigen Zertifikaten in Kontrollgerätekarten und Fahrzeugeinheiten. Diese ist zu unterscheiden von der optischen P. einer Karte, bei der Namen, Fotos u. ä. auf den Kartenkörper aufgebracht wird.
PS	Practice Statement
RA	Registration Authority ist eine Registrierungsstelle, die Zertifikatsanträge und hier auch Anträge auf Verschlüsselung von Daten für Weg-/Geschwindigkeitsgeber an die Zertifizierungsstelle stellt.
Root-Policy (ERCA-Policy)	„Digital Tachograph System - European Root Policy“ Version 2.0 erstellt vom JRC in Ispra

RSA	Spezielles Verfahren der asymmetrischen Kryptographie. Gemäß Anlage 11 des Anhangs I (B) der EU-Verordnung wird im elektronischen Kontrollgerät das RSA-Verfahren zur Erstellung ↑digitaler Signaturen eingesetzt.
SSL	Secure Socket Layer (SSL) ist ein Verfahren, mit denen TCP/IP-Verbindungen verschlüsselt werden können. Zusätzlich ist die Authentisierung der Kommunikationspartner möglich. System zur Kommunikation der D-CA mit ihren Vertragspartnern
Zertifizierungsstelle	Stelle, die ein ↑Zertifikat ausstellt. Im Kontext der EU-Verordnung existieren die Europäische Zertifizierungsstelle (↑ERCA) und die Zertifizierungsstellen der Mitgliedsstaaten, die die für ihre Tätigkeit benötigten Zertifikate von der ↑ERCA erhalten.
Zertifizierungssystem	Kernsystem der D-CA, auf dem Zertifikate erzeugt und Daten für Weg-/Geschwindigkeitsgeber verschlüsselt werden.

Tabelle 6: Glossar