

17.05.05**Empfehlungen
der Ausschüsse**Vk - AS - Fz - Inzu **Punkt ...** der 811. Sitzung des Bundesrates am 27. Mai 2005

Verordnung zur Durchführung des Gesetzes über die mit der Einführung des digitalen Kontrollgerätes zur Kontrolle der Lenk- und Ruhezeiten erforderlichen Begleitregelungen

A.

Der **Ausschuss für Arbeit und Sozialpolitik** empfiehlt dem Bundesrat, der Verordnung gemäß Artikel 80 Abs. 2 des Grundgesetzes nach Maßgabe folgender Änderungen zuzustimmen.

1. Zur Präambel

In der Präambel ist die Angabe "Nummer 1 Buchstabe e durch Artikel 1 Nr. 2 des Gesetzes vom 15. Mai 2004 (BGBl. I S. 954) geändert und" durch die Angabe "Nummer 1 Buchstabe e und Nr. 2 Buchstabe e durch Artikel 1b Nr. 1 des Gesetzes vom ... 2005 (BGBl. I S. ... geändert und" zu ersetzen.

Begründung:

Das Fahrpersonalgesetz in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 640) wurde zuletzt geändert durch Artikel 1b der Zweiten Änderung des Straßenverkehrsgesetzes vom ... 2005 (BGBl. I S. ...). Das Gesetz soll in Kürze verkündet werden. Im Rahmen dieser Änderung des Fahrpersonalgesetzes wurde unter Nummer 1 der § 2 Nr. 1 Buchstabe e und Nummer 2 Buchstabe e geändert. Die Verordnung ist entsprechend zu aktualisieren.

...

2. Zu Artikel 1 (§ 1 Abs. 1 FPersV)

In Artikel 1 ist in § 1 Abs. 1 nach den Wörtern "nach Maßgabe der" die Angabe "Artikel 1," einzufügen.

Begründung:

Die Bezugnahme auch auf Artikel 1 der Verordnung (EWG) Nr. 3820/85 entspricht dem Wortlaut der FPersV in der derzeit geltenden Fassung. Sie geht zurück auf die Verordnung zur Änderung der FPersV vom 20. Mai 1998 (BGBl. I S. 1127).

In der entsprechenden BR-Drucksache 182/98 heißt es zur Begründung auf Seite 8: "Die entsprechende Anwendung der Sachregelung der EG (Lenk-, Unterbrechungs- und Ruhezeiten) bedingt auch die Anwendung der Begriffsbestimmungen nach Artikel 1 der Verordnung (EWG) Nr. 3820/85."

Diese Bezugnahme auf Artikel 1 der Verordnung (EWG) Nr. 3820/85 ist auf Grund fehlender Begriffsbestimmungen im Fahrpersonalgesetz und in der FPersV für die Anwendung der Sachregelung der EG (Lenk-, Unterbrechungs- und Ruhezeiten) nach wie vor erforderlich.

In Artikel 1 Nr. 5 wird z. B. der Begriff Ruhezeit definiert. Danach handelt es sich bei der Ruhezeit um ununterbrochene Zeiträume von mindestens einer Stunde, in denen der Fahrer frei über seine Zeit verfügen kann.

Die Anwendung des Artikels 8 der Verordnung (EWG) Nr. 3820/85 über die tägliche und wöchentliche Ruhezeit im Geltungsbereich der FPersV setzt also voraus, dass gleiche Begriffsbestimmungen zur Anwendung kommen. Würde auf eine Bezugnahme auf Artikel 1 der Verordnung (EWG) Nr. 3820/85 verzichtet werden, müssten auch Zeiträume, die kleiner als eine Stunde sind, als Ruhezeit anzuerkennen sein.

Auch hinsichtlich des Verzichts auf eine Begriffsbestimmung zur Woche erwachsen Probleme bei der Anwendung der vorgenannten Sachregelungen.

3. Zu Artikel 1 (§ 1 Abs. 6 Satz 7 FPersV)

In Artikel 1 ist in § 1 Abs. 6 Satz 7 die Angabe "Verordnung (EWG) Nr. 3281/85" durch die Angabe "Verordnung (EWG) Nr. 3821/85" zu ersetzen.

Begründung:

Redaktionelle Änderung

4. Zu Artikel 1 (§ 1 Abs. 6 Sätze 6 und 7 und Abs. 7 Satz 4 FPersV)

In Artikel 1 ist § 1 wie folgt zu ändern:

- a) Absatz 6 ist wie folgt zu ändern:
 - aa) In Satz 6 sind nach dem Wort "Vorwoche" die Wörter ", an dem sie ein nachweispflichtiges Fahrzeug gefahren haben," einzufügen.
 - bb) In Satz 7 ist das Wort "Tag" durch das Wort "Fahrtag" zu ersetzen.
- b) In Absatz 7 Satz 4 ist das Wort "Tag" durch das Wort "Fahrtag" zu ersetzen.

Begründung:

Maßgeblich für die Nachweispflicht sind die Tage, an denen nachweispflichtige Fahrzeuge gefahren wurden. Der letzte Tag der Vorwoche ist jedoch regelmäßig der Sonntag, an dem nur wenige Fahrer nachweispflichtige Fahrzeuge lenken. Das Ziel der Regelung, die Beachtung der Rechtsvorschriften über die Lenkzeiten, Ruhezeiten und Pausen sicherzustellen, kann nur dann erfüllt werden, wenn diese Aufzeichnungen für den letzten Fahrtag der Vorwoche, an dem ein nachweispflichtiges Fahrzeug gelenkt wurde, vorgelegt werden. Mit der Änderung wird eine Angleichung an die entsprechende Regelung nach Artikel 15 Abs. 7 der Verordnung (EWG) Nr. 3821/85 erzielt.

5. Zu Artikel 1 (§ 4 Abs. 1 Satz 5 FPersV)

In Artikel 1 sind in § 4 Abs. 1 Satz 5 nach dem Wort "hat" die Wörter "für Kontrollgerätarten nach Nr. 1" einzufügen.

Begründung:

Für die Ausgabe der Unternehmens- und Werkstattkarten sollte zur Vereinfachung des Verwaltungsablaufs diese Überprüfung nicht zwingend vorgeschrieben werden. Für die Unternehmenskarte ist diese Überprüfung auf Grund der tatsächlich vorzulegenden Unterlagen ohnehin entbehrlich. Bei den Werkstattkarten kann diese Überprüfung durch die ausgebende Stelle einzelfallbezogen erfolgen, z. B. bei Vorlage unleserlicher Kopien oder sofern Zweifel an der Echtheit der Unterlagen bestehen. Eine unrechtmäßige Beschaffung dieser Kontrollgerätarten würde spätestens bei

Betriebskontrollen aufgedeckt werden. Darüber hinaus unterliegen die Werkstätten ohnehin einem strengen Anerkennungs- und Aufsichtsverfahren nach StVZO, das dort ausführlich in den Anlagen XVIIIc und XVIII d festgelegt ist. So haben z. B. die Anerkennungsstellen die fachliche Eignung und Schulung der verantwortlichen Fachkräfte als Voraussetzung für die Anerkennung zu prüfen und mindestens alle drei Jahre erneut zu prüfen, ob die Werkstatt die ihr obliegenden Pflichten erfüllt und z. B. auch die Werkstattkarten ordnungsgemäß handhabt. Vor diesem Hintergrund ist im Fall der Werkstattkarte der Verwaltungsaufwand für die kartenausgebende Stelle nicht zu rechtfertigen.

6. Zu Artikel 1 (§ 7 Abs. 1 FPersV)

In Artikel 1 ist in § 7 Abs. 1 nach den Wörtern "die verantwortliche Fachkraft" das Wort "(Installateur)" einzufügen.

Begründung:

In den §§ 7 und 8 FPersV wird der Begriff "verantwortliche Fachkraft" verwandt, während der Abschnitt 8 "Ordnungswidrigkeiten" FPersV unter Bezugnahme auf § 8 Abs. 1 Nr. 4 FPersG den Begriff "Installateur" verwendet. Beide Begriffe sollen aber nach dem Willen des Ordnungsgebers synonyme Bedeutung erhalten.

Aus Gründen der Klarstellung soll mit dem Klammereinschub verdeutlicht werden, dass im Sinne der FPersV die "verantwortliche Fachkraft" auch der "Installateur" ist.

7. Zu Artikel 1 (§ 7 Abs. 1 FPersV)

In Artikel 1 sind in § 7 Abs. 1 die Wörter "zuverlässig und" zu streichen.

Als Folge

ist Artikel 1 wie folgt zu ändern:

a) § 7 ist wie folgt zu ändern:

aa) In Absatz 2 ist am Ende der Nummer 8 das Komma durch einen Punkt zu ersetzen und die Nummer 9 zu streichen.

bb) Absatz 3 ist zu streichen.

- b) In § 4 Abs. 3 Satz 3 sind die Wörter "und spätestens nach drei Jahren ein polizeiliches Führungszeugnis nach § 7 Abs. 2 Nr. 9" zu streichen.

Begründung:

Nach den EU-Sozialvorschriften haben Werkstätten Kontrollgeräte einzubauen, zu kalibrieren und zu prüfen. Sie haben damit eine besondere Verantwortung für das ordnungsgemäße Funktionieren des Kontrollgerätes. Diese Aufgabe obliegt den Werkstätten sowohl für das herkömmliche analoge als auch für das neue digitale Kontrollgerät. Für das analoge Kontrollgerät war die Zuverlässigkeit bisher kein eigenständiges Prüfkriterium. Es ist daher nicht nachvollziehbar, weshalb bei einem gleichgelagerten Gefahrenpotenzial der Eingriffs- und Manipulationsmöglichkeit die persönliche Zuverlässigkeit zur Voraussetzung für die Erteilung der Werkstattkarte gemacht werden soll. Das EU-Recht verlangt eine solche Zuverlässigkeitsprüfung nicht.

Über dies findet bereits eine entsprechende Zuverlässigkeitsprüfung im Rahmen der Anerkennung von Werkstätten nach § 57b StVZO statt. Nach den Ausführungsbestimmungen zu dieser Vorschrift müssen Werkstätteninhaber und Fachkräfte persönlich zuverlässig sein und ein Führungszeugnis und einen Auszug aus dem Verkehrszentralregister vorlegen. Der nochmalige Nachweis der Zuverlässigkeit bei der Erteilung von Werkstattkarten ist insofern eine nicht notwendige Doppelprüfung.

Zu den Folgeänderungen:

zu Buchstabe a Doppelbuchstabe aa:

Die Streichung von § 7 Abs. 2 Nr. 9 FPersV ist eine Folgeänderung zur Änderung von § 7 Abs. 1 FPersV.

Die Vorlage eines polizeilichen Führungszeugnisses ist als eigenständiges Zuverlässigkeitskriterium nicht erforderlich. Zudem wäre die Vorlage und Prüfung der Zuverlässigkeit anhand des polizeilichen Führungszeugnisses ungeeignet, um Manipulationen zu vermeiden. Antragsteller und Verwaltung werden durch dieses Prüfmerkmal unnötig zusätzlich belastet. Das EU-Recht verlangt eine solche Zuverlässigkeitsprüfung nicht.

zu Buchstabe a Doppelbuchstabe bb:

Folgeänderung zu § 7 Abs. 1 und § 7 Abs. 2 Nr. 9 FPersV.

Eine Feststellung der Unzuverlässigkeit anhand der Prüfung der in dieser Bestimmung aufgeführten Straftatbestände ist außerdem nicht erforderlich, da Manipulationen auf andere Weise, namentlich durch Einziehung bei missbräuchlicher Verwendung von Kontrollgerätkarten, entgegengewirkt werden können. Sie ist überdies rechtsstaatlich bedenklich, da eine bindende Zuverlässigkeitsprüfung auch auf Straftaten zu erweitern ist, die keinen notwendigen Sachbezug zur ausgeübten Prüftätigkeit aufweisen. Zudem besteht keine Möglichkeit, den zurückliegenden Zeitraum, seit dem eine Straftat begangen wurde, bei der Bewertung der Zuverlässigkeit zu

berücksichtigen. Im Ergebnis kann sich dies als dauerhaftes Berufsverbot auswirken.

zu Buchstabe b:

Folgeänderung zu § 7 Abs. 2 Nr. 9 FPersV.

8. Zu Artikel 1 (§ 18 Abs. 1 Nr. 3 FPersV)

In Artikel 1 sind in § 18 Abs. 1 Nr. 3 nach dem Wort "die" die Wörter "in einem Umkreis von 50 Kilometern vom Standort des Fahrzeugs" einzufügen.

Begründung:

Bislang fallen Fahrzeuge, die beseitigungspflichtige Rohmaterialien von den Schlachthöfen zu den Tierkörperbeseitigungsanlagen transportieren, unter diese Ausnahmeregelung unabhängig von der zurückzulegenden Wegstrecke. Da die Entsorgung jedoch mittlerweile europaweit erfolgt und das Fahrpersonal dieser Fahrzeuge vergleichbaren Belastungen wie das Fahrpersonal im allgemeinen Güterverkehr unterliegt, ist eine unbegrenzte Ausnahme für diese Transporte heute nicht mehr zeitgemäß und aus Arbeitsschutzgründen nicht mehr vertretbar. Daher sollte die Ausnahmeregelung auf Fahrzeuge beschränkt werden, die im Umkreis von 50 km vom Standort eingesetzt werden.

9. Zu Artikel 1 (§ 18 Abs. 1 Nr. 7 FPersV)

In Artikel 1 sind in § 18 Abs. 1 Nr. 7 die Wörter "eines Berufes" durch die Wörter "seines Berufes" zu ersetzen.

Begründung:

Redaktionelle Änderung

10. Zu Artikel 1 (§ 18 Abs. 1 Nr. 12 - neu - FPersV)

In Artikel 1 ist in § 18 Abs. 1 am Ende der Nummer 11 der Punkt durch ein Semikolon zu ersetzen und folgende Nummer anzufügen:

"12. Fahrzeuge, die ausschließlich zur privaten, nicht gewerblichen Personenbeförderung dienen und die nach ihrer Bauart und Ausstattung geeignet und dazu bestimmt sind, bis zu 17 Personen - einschließlich des Fahrers - zu befördern."

Begründung:

Omnibusse für bis zu 17 Personen werden in zunehmendem Maße auch von Großfamilien eingesetzt. Bei der privaten Nutzung von Omnibussen für bis zu 17 Personen sind nach unmittelbar geltendem europäischem Recht Einbau und Benutzung eines Kontrollgerätes vorgeschrieben, weil die Bundesrepublik Deutschland von der Abweichungsbefugnis nach Artikel 13 Abs. 1 Buchstabe a der Verordnung (EWG) Nr. 3820/85 keinen Gebrauch gemacht hat. Einzelausnahmebewilligungen durch Behörden sieht das europäische Fahrpersonalrecht nicht vor.

Somit ist auch bei ausschließlich privater Verwendung derartiger Fahrzeuge durch eine Großfamilie oder durch Vereine der Einbau und die Benutzung des Kontrollgerätes unabhängig von der Länge der Fahrtstrecken erforderlich. Schwere Lastkraftwagen, die zur nichtgewerblichen Güterbeförderung für private Zwecke verwendet werden, sind demgegenüber nach Artikel 4 Nr. 12 Verordnung (EWG) 3820/85 von der Pflicht zur Benutzung des Kontrollgerätes ausgenommen.

Die erheblichen Kosten der Kontrollgeräte sowie die zeitaufwändige Benutzung der Geräte belastet Private, insbesondere die Familien, enorm. So ist z. B. bei jeder Fahrt, auch auf Kurzstrecken mit wenigen Personen im Fahrzeug, das Ausfüllen und Einlegen eines Schaublattes erforderlich. Die Einhaltung der Lenkzeiten, Ruhezeiten und Pausen, die durch die Geräte überwacht werden, ist nur beim Fahrpersonal des gewerblichen Verkehrs zum Schutz der Gesundheit und der Sicherheit des Straßenverkehrs erforderlich. Private nutzen die Fahrzeuge jedoch weit überwiegend auf kurzen Fahrtstrecken. Die seltene Nutzung auf längeren Strecken im Urlaub oder an Wochenenden rechtfertigt nicht die Überwachung der privaten Fahrer durch Kontrollgeräte, die den Schutz der Gesundheit des gewerblichen Fahrpersonals sicherstellen sollen. Einbau und Benutzung des Kontrollgerätes bringen bei ausschließlich privater Verwendung der Fahrzeuge keine erkennbaren Vorteile für die Sicherheit des Straßenverkehrs.

Die Änderung hat insbesondere eine familienpolitisch erstrebenswerte Erleichterung für Großfamilien zum Ziel. Auch die mögliche private Nutzung durch Vereine, z. B. an Wochenenden, oder andere private Nutzungen lassen keine Gefährdung des Straßenverkehrs durch Aufhebung der Kontrollgerätepflcht befürchten.

11. Zu Artikel 1 (§ 20 Abs. 1 Satz 1 FPersV)

In Artikel 1 ist § 20 Abs. 1 Satz 1 wie folgt zu ändern:

- a) Die Wörter "in folgenden Fällen" sind zu streichen.

- b) Die Wörter "für diese Tage" sind durch die Wörter "für die Tage der laufenden Woche" zu ersetzen.
- c) Nach dem Wort "vorzulegen" ist der Doppelpunkt durch einen Punkt zu ersetzen und es sind die Nummern 1 und 2 zu streichen.

Begründung:

Die Vorschrift zum Mitführen einer Bescheinigung für den "letzten Tag der Vorwoche" wird weder der Zielsetzung gerecht noch drückt die Formulierung das Gewollte konkret aus; auch ist aus dem EU-Recht für eine derartige Regelung keine rechtliche Grundlage ersichtlich.

Nach Artikel 15 Abs. 7 der Verordnung (EWG) Nr. 3821/85 sind die Schaublätter der laufenden Woche, für den vorausgegangenen Zeitraum jedoch nur das Schaublatt des letzten Tages der vorangegangenen Woche, an dem der Fahrer gefahren ist, vorzulegen (nach dem EuGH-Urteil C-158/90 vom 13. Dezember 1991 kann dieser Tag mehrere Wochen zurückliegen). Abgesehen von Berufseinsteigern muss somit neben den Schaublättern der laufenden Woche immer ein vorausgegangenes Schaublatt vorgelegt werden können, egal wie lange dieser letzte Fahrtag zurückliegt. Da es also immer ein "letztes" Schaublatt gibt, läuft die Forderung nach einer Bescheinigung ins Leere. Im Übrigen ist die Nichtvorlage dieses Schaublattes ohnehin auch bußgeldbewehrt.

Dafür, dass es sich dabei tatsächlich um den letzten Fahrtag handelt, hat auch eine formlose Bescheinigung keinerlei Beweiskraft, zumal sie nur im Straßenverkehr vorgehalten werden muss. War der letzte Fahrtag beispielsweise der Samstag oder der Sonntag der unmittelbar vorausgegangenen Woche, ist eine wirksame Kontrolle der Wochenruhezeit ebenfalls nicht gewährleistet, da diese auch schon zu einem früheren Zeitpunkt eingebracht sein kann. Letztlich ist eine Überprüfung der Wochenruhezeit auch bei Vorlage einer Bescheinigung nur über eine Betriebskontrolle möglich, die in Zweifelsfällen zu veranlassen ist. Unberührt bleibt die freiwillige Mitführung von Bescheinigungen um zusätzliche Betriebskontrollen zu vermeiden.

12. Zu Artikel 1 (§ 21 Abs. 2 Nr. 5 FPersV)

In Artikel 1 ist in § 21 Abs. 2 Nr. 5 die Angabe "§ 1 Abs. 7 Satz 5" durch die Angabe "§ 1 Abs. 7 Satz 4" zu ersetzen.

Begründung:

Die Verpflichtung, Schaublätter mitzuführen und den Kontrollbeamten auf Verlangen zur Prüfung auszuhändigen, ist in § 1 Abs. 7 Satz 4 FPersV geregelt.

13. Zu Artikel 1 (§ 21 Abs. 3 - neu - FPersV)

In Artikel 1 ist in § 21 nach Absatz 2 folgender Absatz anzufügen:

"(3) Ordnungswidrig im Sinne des § 8 Abs. 1 Nr. 4 Buchstabe a des Fahrpersonalgesetzes handelt, wer als Werkstattinhaber oder als verantwortliche Fachkraft (Installateur) vorsätzlich oder fahrlässig

1. entgegen § 8 Abs. 1 Satz 1 erster Halbsatz den Wegfall der Erteilungsvoraussetzungen nicht meldet oder
2. entgegen § 4 Abs. 4 Satz 5 oder § 8 Abs. 1 Satz 1 zweiter Halbsatz, in Verbindung mit Satz 3 oder Satz 5 eine Werkstattkarte nicht oder nicht rechtzeitig zurückgibt."

Begründung:

Durch Artikel 1b der Zweiten Änderung des Straßenverkehrsgesetzes wurde die Nummer 4 in § 8 Abs. 1 FPersG eingefügt. Das Gesetz soll in Kürze verkündet werden. Damit besteht eine Rechtsgrundlage, um die für die Praxis erforderlichen Ordnungswidrigkeitstatbestände für Zuwiderhandlungen von Werkstattinhabern und verantwortlichen Fachkräften (Installateuren) zu definieren.

Die Werkstattkarte stellt angesichts der Möglichkeit eines Missbrauchs eine hochsensible Kontrollgerätkarte dar. Daher müssen Antragsteller für Werkstattkarten besondere Voraussetzungen erfüllen. Bei Wegfall von Erteilungsvoraussetzungen ist die ausgebende Behörde unverzüglich zu informieren und die Werkstattkarte an die zuständige Behörde innerhalb einer von dieser gesetzten Frist zurückzugeben. Zuwiderhandlungen gegen diese Bestimmungen der FPersV fördern den Missbrauch der Werkstattkarte. Diese Zuwiderhandlungen müssen als Ordnungswidrigkeiten im Sinne des Fahrpersonalgesetzes definiert werden, damit die Aufsichtsbehörden entsprechende Verstöße verfolgen und ahnden können.

14. Zu Artikel 1 (§ 25 Abs. 2 Nr. 5 FPersV)

In Artikel 1 sind in § 25 Abs. 2 Nr. 5 nach dem Wort "führt" die Wörter "oder nicht vorlegt" einzufügen.

Begründung:

Das Fahrpersonal ist nach Artikel 10 Abs. 1 Buchstabe d AETR sowohl zum Mitführen als auch zur Vorlage der Schaublätter bei Kontrollen verpflichtet.

Als Ordnungswidrigkeit sind somit sowohl Zuwiderhandlungen gegen die Mitführipflicht als auch gegen die Vorlagepflicht zu ahnden.

15. Zu Artikel 1 (Anlage 2 zu § 3 FPersV)

In Artikel 1 ist in Anlage 2 zu § 3 FPersV die Zertifizierungs-Policy für die Bundesrepublik Deutschland (Version 1.0 in der Fassung vom 21. Januar 2005) durch folgende Zertifizierungs-Policy für die Bundesrepublik Deutschland (Version 1.0 in der Fassung vom 23. Februar 2005) zu ersetzen:

Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0

Digitales Tachographensystem im Straßenverkehr

Zertifizierungs-Policy für die

Bundesrepublik Deutschland

Version 1.0 in der Fassung vom 23.02.2005

1 Einleitung

Dieses Dokument ist die Zertifizierungs-Policy der Zertifizierungsstelle der Bundesrepublik Deutschland, im Folgenden kurz als **die CA-Policy** bezeichnet, für den elektronischen Fahrtenschreiber gemäß VO(EG) 3821/85 und Anlage 11 des Anhangs I (B) der VO(EG) 2135/98 in Verbindung mit 1360/2002 (CSM_008). Die vorgenannte Zertifizierungsstelle wird als **D-CA** bezeichnet.

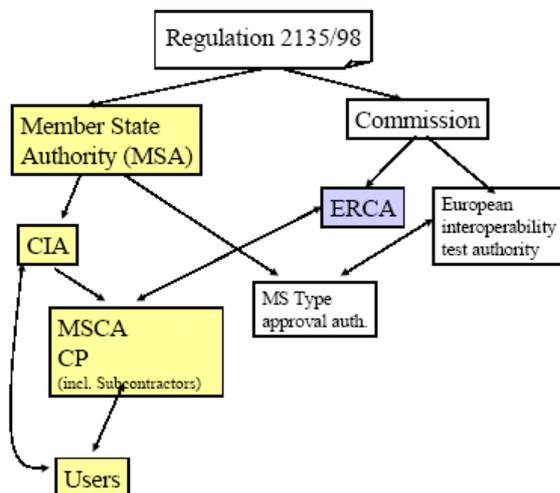
Die CA-Policy befindet sich im Einklang mit der

- Digital Tachograph System - European Root Policy (Version 2.0 Special Publication I.04.131)
- VO(EG) 3821/85
- VO(EG) 2135/98
- VO(EG) 1360/2002
- „Common Security Guideline“

Elektronischer Fahrtenschreiber Deutsche CA-Policy Version 1.0

1.1 Zuständige Organisationen

Das Tachographen-System verfügt über folgende Organisation¹:



Die für die Umsetzung der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 in Deutschland zuständige Stelle wird im Folgenden dem internationalen Sprachgebrauch folgend mit **D-MSA** (Deutschland-Member State Authority) bezeichnet und vom BMVBW wahrgenommen. Offizieller Ansprechpartner ist:

Bundesministerium für Verkehr, Bau- und Wohnungswesen
Referat S35
Robert Schuman-Platz 1
53175 Bonn.

Die D-MSA beauftragt das Kraftfahrt-Bundesamt (KBA) mit der Wahrnehmung der Aufgaben der **D-CA**. Dazu gehört insbesondere die Verantwortung für die Umsetzung der CA-Policy. Die D-CA kann die Erfüllung (von Teilen) ihrer Aufgaben externen Dienstleistern übertragen. Hierdurch wird die Verantwortung der D-CA in keiner Weise eingeschränkt.

Die Wahrnehmung der Aufgaben der **D-CIA** wird von den Bundesländern jeweils individuell bestimmt.

Der **D-CP** wird von der D-MSA bestimmt.

1.2 Genehmigung

Die deutsche CA-Policy wurde von der D-MSA bei der EU-Kommission zur Genehmigung vorgelegt und durch die Europäische Behörde am 09. Februar 2005 genehmigt².

¹ Guideline and Template National CA policy, V 1.0

² Genehmigt wurde die Fassung in englischer Sprache, die bei Zweifelsfragen Vorrang vor der deutschen Fassung hat.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

1.3 Verfügbarkeit und Kontakt-Details

Die nationale CA Policy steht in elektronischer Form auf der Web-Seite <http://www.kba.de> zur Verfügung.

Fragen und Kontakt-Details zu dieser nationalen CA Policy sind zu richten an:

Bundesministerium für Verkehr, Bau- und Wohnungswesen
Referat S35
Robert Schuman-Platz 1
53175 Bonn.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

2 Geltungsbereich

[r2.1]

Die Gültigkeit der CA-Policy erstreckt sich ausschließlich auf die Wahrnehmung der Aufgaben im Rahmen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002.

[r2.2]

D-MSA und D-CA stellen im Rahmen ihrer jeweiligen Zuständigkeiten und der jeweils geltenden Rechtsvorschriften sicher, dass die von der D-CA erstellten Zertifikate und Schlüssel nur für die in der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 definierten Zwecke im Rahmen ihrer individuellen Zuständigkeiten und den relevanten gültigen Regelungen eingesetzt werden.

[r2.3]

Der Geltungsbereich der vorliegenden deutschen Policy ist in folgender Übersicht fett markiert³:

³ Vgl. Digital Tachograph System European Root Policy, V 2.0

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

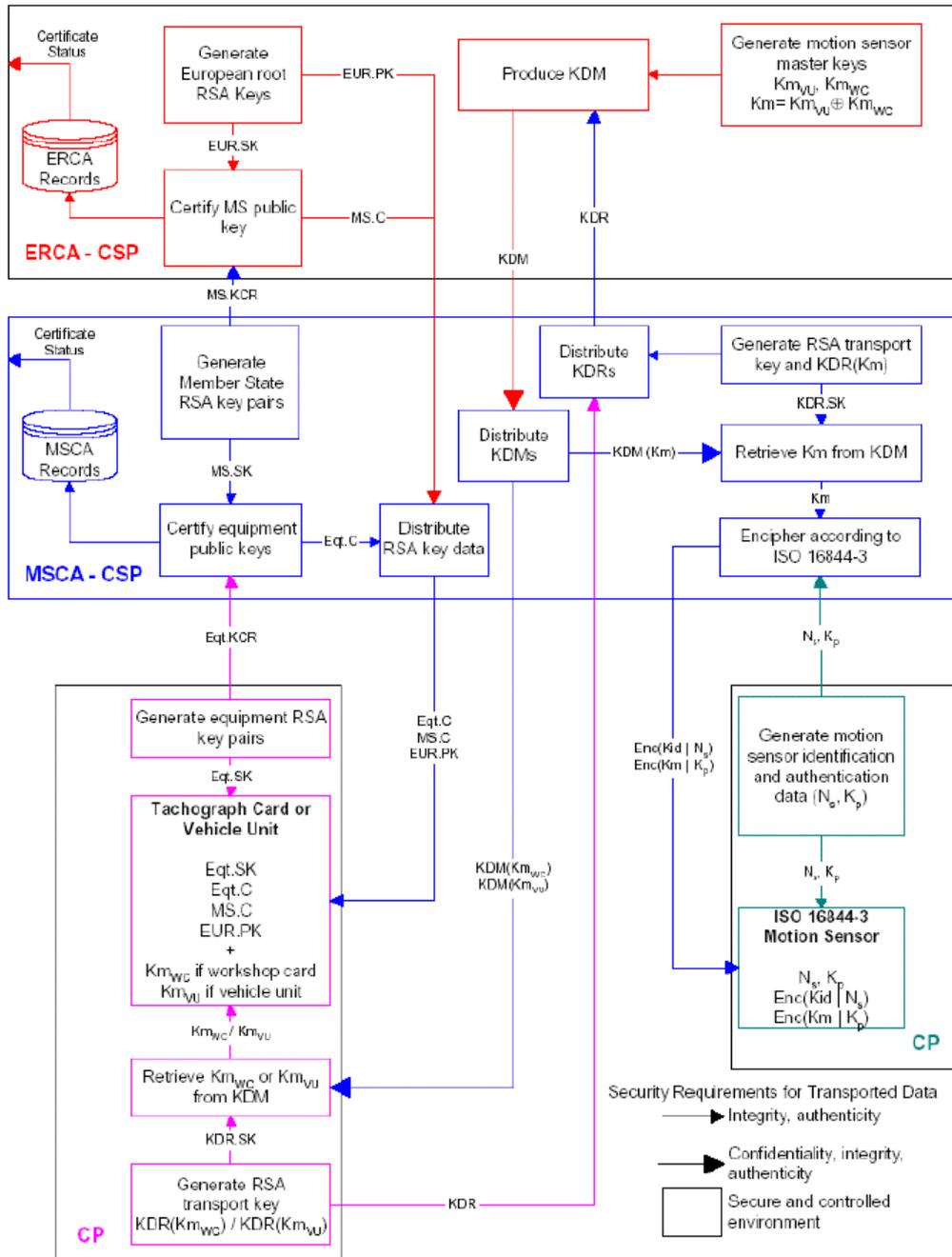


Figure 1 Description of Annex I(B) key management

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

3 Allgemeine Regelungen

3.1 Aufgaben und Verpflichtungen

Dieser Abschnitt beschreibt Aufgaben und Verpflichtungen der an der Umsetzung der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 beteiligten Stellen, soweit diese den Gültigkeitsbereich der CA-Policy betreffen.

[r3.1]

Die **D-MSA**:

- a) nimmt ihre Aufgaben in Abstimmung mit den Ländern wahr.
- b) ist zuständig für die Erstellung und Aktualisierung der CA-Policy und veranlasst deren Genehmigung durch die Kommission,
- c) ernennt die D-CA und gibt diese Ernennung der Generaldirektion für Verkehr und Energie der Europäischen Union (DG TRE) bekannt,
- d) ernennt den D-CP oder lagert diese Aufgabe an einen externen Dienstleister aus,
- e) kann Überprüfungen der D-CA, der D-CP, der D-CIA, der Hersteller und weiterer externer Dienstleister durchführen oder veranlassen, wenn dies erforderlich ist,
- f) stellt sicher oder veranlasst, dass die D-CA alle für ihre Tätigkeit benötigten Informationen in korrekter Weise erhält,
- g) genehmigt das Practice Statement (PS) der D-CA und ggf. das PS weiterer externer Dienstleister,
- h) stellt sicher oder veranlasst, dass die CA-Policy den beteiligten Stellen zur Verfügung gestellt wird,
- i) informiert unverzüglich die ERCA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle bei der Produktion, Personalisierung und beim Einsatz ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate.

[r3.2]

Die **D-CA**:

- a) führt in ihrem Betrieb die Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, aller hierfür relevanten Rechtsvorschriften, der Root-Policy und dieser CA-Policy aus,
- b) erstellt ein PS, in dem mindestens die Art der Umsetzung der CA-Policy, der Root-Policy und der gesetzlichen Regelungen erläutert wird,
- c) hält die zur ordnungsgemäßen Erfüllung ihrer Aufgabe notwendigen personellen und materiellen Ressourcen bereit,
- d) trägt die Verantwortung für die ordnungsgemäße Durchführung ihrer Aufgaben auch dann, wenn sie diese oder Teile davon an externe Dienstleister auslagert. In diesem Fall hat sie sicherzustellen, dass diese in ihrem Betrieb die relevanten Anforderungen der CA-Policy und des PS einhalten,
- e) informiert unverzüglich die D-MSA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle bei der Produktion, Personalisierung und beim Einsatz ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate.

[r3.3]

Die **D-CIA**:

- a) stellt sicher, dass die Antragsdaten korrekt und entsprechend den Anforderungen der D-CA an die D-CA und den D-CP geliefert werden,
- b) informiert in geeigneter Weise alle Nutzer über die Anforderung dieser Policy,
- c) prüft, ob alle Voraussetzungen für die Ausgabe einer Karte gegeben sind,

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

- d) stellt sicher, dass die PIN der Werkstattkarte nur an die Person ausgeliefert wird, für die die Werkstattkarte ausgestellt wurde,
- e) informiert unverzüglich die D-MSA und die D-CA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle.

[r3.4]

Der D-CP

- a) erfüllt in seinem Betrieb die Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, aller hierfür relevanten sonstigen Rechtsvorschriften, der Root-Policy und dieser CA-Policy sowie des PS der D-CA,
- b) schließt – sofern es sich bei diesem um einen externen Dienstleister handelt – einen Vertrag mit der D-MSA ab, in dem er die Erfüllung seiner Verpflichtungen nach a) verbindlich zusagt,
- c) weist der D-MSA gegenüber die konkrete Umsetzung seiner Verpflichtungen im laufenden Betrieb in geeigneter Weise nach,
- d) gestattet der D-MSA oder einer von ihr beauftragten Stelle, die praktische Umsetzung seiner Verpflichtungen zu überprüfen,
- e) informiert unverzüglich die D-CA oder eine ihrer autorisierten Stellen über alle sicherheitsrelevanten Vorfälle bei der Produktion, Personalisierung und beim Einsatz ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate.

[r3.5]

Der Karteninhaber/Antragsteller:

Ist verpflichtet:

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

[r3.6]

Hersteller von Fahrzeugeinheiten und Hersteller von Weg-/Geschwindigkeitsgebern
stellen insbesondere sicher, dass sie

- a) die für sie relevanten Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, aller hierfür relevanten sonstigen Gesetze und Rechtsverordnungen, insbesondere dieser CA-Policy einhalten, nach bestem Wissen und dem jeweils aktuellen Stand der Technik
 - aa) dass die in die von ihnen hergestellten Geräte einzubringenden oder eingebrachten Schlüssel und Zertifikate nur für deren ordnungsgemäße Zwecke im Rahmen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genutzt werden können,
 - ab) Vorkehrungen treffen, die Geheimhaltung der privaten Schlüssel bzw. geheimen Schlüssel während des gesamten Produktionsprozesses und während der gesamten Nutzungsdauer der Geräte zu gewährleisten.
- b) der D-MSA alle ggf. mit der Wahrnehmung von wesentlichen Aufgaben im Zusammenhang mit der Produktion und der Personalisierung ihrer Geräte beauftragten externen Dienstleister nennen und diese zur Einhaltung der entsprechenden Anforderungen ver

Elektronischer Fahrtenschreiber Deutsche CA-Policy Version 1.0

- pflichten. Sofern der Hersteller Aufgaben an Dritte weitergibt, bleiben seine Rechte und Pflichten davon unberührt.
- c) der D-MSA oder einer von ihr autorisierten Stelle unverzüglich alle ihnen bekannt gewordenen sicherheitsrelevanten Vorfälle im Zusammenhang mit der Produktion, Personalisierung und Nutzung ihrer Geräte sowie der in diese eingebrachten Schlüssel und Zertifikate mitteilen.
 - d) der D-MSA oder einer von ihr beauftragten Stelle gestattet, die praktische Umsetzung seiner Verpflichtungen zu überprüfen.
 - e) im Rahmen ihrer Möglichkeiten ausschließen, dass die ihnen zur Verfügung gestellten Schlüssel und Zertifikate in nicht bauartgenehmigte Geräte eingebaut werden
 - f) sich einem Prozess zur Aufrechterhaltung der Vertrauenswürdigkeit der IT-Sicherheitszertifikate nach dem BSI Zertifizierungsschema zu unterziehen. Dies beinhaltet die Überwachung der zertifizierten Produkte auf einer regelmäßigen Basis (1 Jahr) betreffend die Resistenz gegen relevante Bedrohungen in Übereinstimmung mit den Sicherheitszielen. Das BSI unterrichtet die D-MSA über die Ergebnisse.

[r3.7]

Hersteller von Kontrollgerätkarten oder Lieferanten – soweit sie IT-Sicherheitszertifikate erhalten haben – müssen sich für das Composite-Smartcard-Produkt einem Prozess zur Aufrechterhaltung der Vertrauenswürdigkeit der IT-Sicherheitszertifikate nach dem BSI Zertifizierungsschema zu unterziehen. Dies beinhaltet die Überwachung der zertifizierten Composite-Smartcard-Produkte auf einer regelmäßigen Basis (1 Jahr) betreffend die Resistenz gegen relevante Bedrohungen in Übereinstimmung mit den Sicherheitszielen. Das BSI unterrichtet die D-MSA über die Ergebnisse.

3.2 Besondere Rechtsvorschriften

Die D-CA und die gegebenenfalls von ihr beauftragten externen Dienstleister erfüllen ihre Aufgaben im Einklang mit geltendem Recht, insbesondere mit der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 und den zum Zwecke ihrer Umsetzung erlassenen nationalen Rechtsvorschriften.

Die in diesem Abschnitt genannten Rechtsvorschriften erheben *keinen* Anspruch auf Vollständigkeit.

[r3.8] **Datenschutz**

Die D-CA stellt sicher, dass im Rahmen ihres Einflussbereichs die Vorschriften des Bundesdatenschutzgesetzes und entsprechender weiterer datenschutzrechtlicher Vorschriften für den Umgang mit personenbezogenen Daten eingehalten werden.

[r3.9] **Elektronische Signaturen**

Die bei der D-CA produzierten Zertifikate dienen zur Verifizierung von Elektronischen Signaturen im Sinne des Gesetzes über Rahmenbedingungen für Elektronische Signaturen (SigG). Die Zertifikate sind *nicht qualifizierte* Zertifikate im Sinne des SigG. Die D-CA stellt sicher, dass sie und die von ihr beauftragten externen Dienstleister die hieraus resultierenden Anforderungen (§14) des Signaturgesetzes einhalten.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

4 Practice Statement der D-CA

[r4.1]

Die D-CA erstellt und pflegt ein PS, in dem in Form von konkret umzusetzenden Maßnahmen dargestellt wird, wie die Einhaltung dieser CA-Policy, der Root-Policy und der für die Tätigkeit der D-CA relevanten gesetzlichen Regelungen im Betrieb der D-CA gewährleistet ist. Dieses PS enthält eine tabellarische Übersicht, aus der ersichtlich wird, wo die Anforderungen dieser Policy im PS umgesetzt werden.

[r4.2]

Das PS muss alle externen Dienstleister der D-CA und ihre konkreten Aufgaben benennen sowie darlegen, welche der an die D-CA zu stellenden Anforderungen von diesen Dienstleistern einzuhalten sind.

[r4.3]

Das PS muss darlegen, wie die D-CA ihren Informationspflichten nachkommt.

[r4.4]

Im PS muss ein Revisionsprozess beschrieben sein, der sicherstellt, dass das PS stets dem aktuellen Stand der Gesetzgebung, der Technik und den aktuellen Gegebenheiten bei der D-CA und ihren externen Dienstleistern entspricht.

[r4.5]

Die D-CA legt der D-MSA ihr PS zur Genehmigung vor. Wesentliche Änderungen des PS bedürften ebenfalls der Genehmigung der D-MSA. Die D-CA stellt sicher, dass die D-MSA stets über die aktuelle Version des PS verfügt.

[r4.6]

Die öffentlichen Teile des PS können außerhalb des PS in einem Realisierungskonzept (RK) beschrieben werden.

[r4.7]

Das PS enthält eine genaue Auflistung von Ereignissen, die als Verdacht auf Schlüsselkompromittierung angesehen werden. Diese Auflistung ist vertraulich zu behandeln.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

5 Karten- und Gerätemanagement

[r5.1]

Die D-CA stellt nach den Vorgaben der D-MSA und gemeinsam mit dieser innerhalb ihres Einflussbereichs sicher, dass die von ihr produzierten Zertifikate und die von ihr ausgelieferten geheimen Schlüssel entsprechend ihrem Verwendungszweck nur in Kontrollgerätkarten und Kontrollgeräte eingebracht und eingesetzt werden, die den Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genügen.

[r5.2]

Die D-CA verweigert die Auslieferung von Schlüsseln und Zertifikaten, wenn die Gefahr eines Missbrauchs von Schlüsseln und Zertifikaten vorliegt.

[r5.3]

Die D-CIA gewährleistet die Einhaltung des von der D-MSA entsprechend den Vorgaben der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 definierten Antrags- und Auslieferungsverfahrens für Kontrollgerätkarten.

[r5.4]

Die D-CIA stellt innerhalb ihres Einflussbereichs sicher, dass die Ausstellung von Ersatzkarten und die Kartenerneuerung nur unter den in der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genannten Voraussetzungen erfolgt und dass die dafür vorgeschriebenen Fristen eingehalten werden können.

[r5.5]

Der D-CP stellt sicher, dass die Kontrollgerätkarten logisch entsprechend der Vorgaben der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 personalisiert werden. Dabei ist insbesondere die Integrität der aufgebrachten Daten zu wahren.

[r5.6]

Die D-CA, D-CP und Hersteller stellen innerhalb ihres jeweiligen Einflussbereiches sicher, dass private und geheime Schlüssel in einer gesicherten Produktionsumgebung aufbewahrt und eingesetzt werden.

[r5.7]

Die D-CIA stellt dem zentralen Register beim KBA die relevanten Daten zur Verfügung, damit nachvollzogen werden kann, welche Karte welchem Inhaber/Nutzer ausgestellt wurde.

[r5.8]

Die D-CIA stellt sicher, dass personalisierte Karten innerhalb der durch die VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 vorgegebenen Fristen sicher und nachvollziehbar an ihre Inhaber/Nutzer ausgeliefert werden. Voraussetzung für die Ausstellung einer personalisierten Karte an einen Inhaber/Nutzer ist, dass dieser entweder bei Antragstellung und/oder bei Kartenübergabe persönlich identifiziert wurde. Sofern Karten nicht auf eine natürliche Person ausgestellt werden, muss der Antragsteller und der Empfänger der Karten eine ausreichende Legitimation nachweisen können.

[r5.9]

Die D-CP stellt sicher, dass Werkstattkarten mit einer PIN gemäß den Vorgaben der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 ausgestattet werden.

[r5.10]

Die Generierung der PIN erfolgt in einem gegen unautorisierte Zugriffe abgesicherten System. Dieses System verhindert, dass nachträglich eine Zuordnung von PIN und Werkstattkarte erfolgen kann. Die PIN wird nach ihrer Generierung auf einem angeschlossenen Drucker ausgedruckt, in einem Briefumschlag (PIN-Brief) verschlossen und nur an die Person ausgeliefert, für die die Werkstattkarte ausgestellt wurde.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Das zur PIN-Generierung und PIN-Brieferstellung benutzte System muss zumindest die Anforderungen von ITSEC E3 (mittel), Common Criteria EAL 4, oder einem äquivalenten IT-Sicherheitskriterienwerk erfüllen oder nachweislich durch andere Maßnahmen eine gleichwertige Sicherheit gewährleisten.

[r5.11]

Die Versendung der PIN-Briefe muss getrennt von den personalisierten Karten erfolgen. Sie kann auf normalem Postweg erfolgen.

[r5.12]

Die Rekonstruktion einer PIN ist auszuschließen.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

6 Schlüsselmanagement in der D-CA

Dieser Abschnitt enthält Anforderungen für den Umgang der D-CA mit folgendem Schlüsselmaterial (in Klammern die in der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 ggf. hierfür verwendeten Kürzel):

- der öffentliche Schlüssel der Root-CA (EUR.PK),
- das Schlüsselpaar der D-CA (MS.SK, MS.PK),
- symmetrische Schlüssel für Weg-/Geschwindigkeitsgeber (Km, Km_{wc}, Km_{vu}),
- ggf. Transportschlüssel zur Kommunikation mit der Root-CA und
- ggf. eigene Transportschlüssel der D-CA.

Die D-CA stellt die Vertraulichkeit und Integrität aller bei ihr erzeugten, verwendeten und/oder gespeicherten nicht-öffentlicher Schlüssel sicher und verhindert wirksam jeglichen Missbrauch dieser Schlüssel. Hierzu hat sie besonders geeignete technische Systeme einzusetzen, die eine der folgenden Anforderungen erfüllen:

- FIPS 140-2 (oder 140-1); Level 3 oder höher [FIPS],
- CEN Workshop Agreement 14176-2 [CEN],
- Zertifizierung nach EAL 4 oder höher [CC] in Verbindung mit ISO 15408 [CC] oder E3 oder höher [ITSEC] auf der Grundlage eines Schutzprofils oder von Sicherheitsvorgaben („security targets“), die die Anforderungen dieser CA-Policy - basierend auf einer umfassenden Risikoanalyse - auch infrastrukturelle und nicht-technische Sicherheitsmaßnahmen erfasst,
- äquivalente Sicherheitskriterien, die nachweislich eine gleichwertige Sicherheit gewährleisten.

Ebenso ist aufzuzeigen, dass diese Systeme bei der D-CA in einer ausreichend sicheren Betriebsumgebung eingesetzt werden.

6.1 Öffentlicher Schlüssel der Root-CA (EUR.PK)

[r6.1]

Die D-CA stellt sicher, dass in ihrem laufenden Betrieb Integrität und Verfügbarkeit des Schlüssels EUR.PK sichergestellt sind.

[r6.2]

Die D-CP und Hersteller stellen sicher, dass EUR.PK in alle Kontrollgerätkarten und Fahrzeugeinheiten in ihrem Einflussbereich eingebracht werden.

6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK)

[r6.3]

Die D-CA muss verschiedene Mitgliedstaatschlüsselpaare besitzen für die Produktion von öffentlichen Schlüssel-Zertifikaten für Weg-/Geschwindigkeitsgeber (unbegrenzte Gültigkeit) und öffentlichen Schlüssel-Zertifikaten für Fahrzeugeinheiten (begrenzte Gültigkeit).

[r6.4]

Die D-CA stellt sicher, dass MS.SK ausschließlich zur Signierung von Zertifikaten für Kontrollgerätkarten, Fahrzeugeinheiten und für die Produktion der ERCA Schlüsselzertifikate

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

rungsanforderung (KCR) verwendet wird. Dies beinhaltet insbesondere die Geheimhaltung des privaten Schlüssels MS.SK.

[r6.5]

Die Erzeugung des D-CA-Schlüsselpaars darf nur bei aktiver Mitwirkung von mindestens drei unterschiedlichen Personen innerhalb der D-CA erfolgen. Eine dieser Personen muss die Rolle des CA-Administrators einnehmen, die beiden anderen müssen jeweils eine andere der in dieser CA-Policy beschriebenen Rollen wahrnehmen.

[r6.6]

Die D-CA sollte – im Rahmen der Vorgaben der Root-Policy – eine angemessene Anzahl von Ersatz-Schlüsselpaaren mit den zugehörigen Zertifikaten vorhalten, um bei Nicht-Verfügbarkeit des aktuellen Schlüssels einen schnellen Schlüsselwechsel auch ohne aktive Mitwirkung der Root-CA durchführen zu können. Sollten mehrere aktuelle Schlüsselpaare vorliegen, stellt die D-CA sicher, dass stets der richtige Schlüssel verwendet wird.

[r6.7]

Jeder private Schlüssel MS.SK soll höchstens zwei Jahre eingesetzt werden. Nach Ende seiner Verwendungsdauer ist er von der D-CA so zu vernichten, dass ein künftiger Gebrauch oder Missbrauch ausgeschlossen ist.

[r6.8]

Die Gültigkeitsdauer der öffentlichen Mitgliedstaatschlüssel MS.PK ist unbegrenzt.

[r6.9]

Die D-CA hat den privaten Schlüssel und alle Ersatzschlüssel durch technisch-organisatorische Maßnahmen wirksam vor Missbrauch, Veränderung und unbefugter Kenntnisnahme zu schützen.

[r6.10]

Die D-CA verhindert durch technisch-organisatorische Maßnahmen wirkungsvoll, dass ein Zugriff auf MS.SK durch eine einzelne Person allein erfolgen kann („4-Augen-Prinzip“).

[r6.11]

Es findet keine Schlüsselhinterlegung von MS.SK statt, d.h. einschließlich Geräteschlüssel.

[r6.12]

Das PS der D-CA soll eine explizite Vorgehensweise für den Fall enthalten, dass eine Kompromittierung von MS.SK stattgefunden hat oder der begründete Verdacht dazu besteht. Diese Vorgehensweise soll auch Anweisungen an externe Dienstleister und Informationen an Kartenbesitzer und Gerätehersteller enthalten.

Im Falle das die Schlüssel EUR.SK, MS.SK, Km, Km_{WC}, Km_{VU} kompromittiert wurden oder der begründeten Verdacht dazu besteht, sind die D-MSA und die Root-CA unverzüglich zu informieren.

In anderen Fällen von Schlüsselkompromittierung oder des begründeten Verdachts der Schlüsselkompromittierung sind geeignete Maßnahmen zu ergreifen und die betroffenen Institutionen zu informieren.

[r6.13]

Die D-CA stellt in Kooperation mit der Root-CA sicher, dass sie zu jedem Zeitpunkt über ein gültiges Schlüsselpaar (MS.SK, MS.PK) mit zugehörigem Zertifikat verfügt.

[r6.14]

Die D-CA reicht die öffentlichen Mitgliedstaatschlüssel zur Zertifizierung bei der ERCA ein unter Verwendung des Protokolls der Schlüsselzertifizierungsanforderung (KCR), wie in Anhang A der Digital Tachograph System European Root Policy beschrieben.

[r6.15]

Elektronischer Fahrtenschreiber Deutsche CA-Policy Version 1.0

Die D-CA erkennt den öffentlichen ERCA-Schlüssel in dem in Anhang B der Digital Tachograph System European Root Policy beschriebenen Auslieferungsformat an.

[r6.16]

Die D-CA verwendet für den Schlüssel- und Zertifikatetransport die physikalischen Medien, die im Anhang C der Digital Tachograph System European Root Policy beschrieben sind.

6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, Km_{WC}, Km_{VU})

[r6.17]

Die D-CA fordert bei Bedarf von der Root-CA die Weg-/Geschwindigkeitsgeber-Schlüssel Km, Km_{WC}, Km_{VU} an. Für Anforderung und Auslieferung dieser Schlüssel zwischen Root-CA und D-CA sind die Bestimmungen der Root-CA einzuhalten.

[r6.18]

Die D-CA stellt durch geeignete Maßnahmen sicher, dass die Schlüssel Km_{WC} und Km_{VU} nur an die hierfür vorgesehenen Empfänger weitergegeben werden und sichert diese Weitergabe durch geeignete Maßnahmen. Die D-MSA überwacht die Sicherheitsmaßnahmen der D-CA.

Die D-CA stellt sicher, dass der Schlüssel Km nicht weitergegeben wird.

[r6.19]

Im Falle, dass eine Kompromittierung eines der Schlüssel Km_{WC} oder Km_{VU} oder insbesondere von Km stattgefunden hat oder dass der begründete Verdacht hierauf vorliegt, informiert die D-CA unverzüglich die D-MSA und die Root-CA von diesem Sachverhalt.

[r6.20]

Die D-CA fordert die Weg-/Geschwindigkeitsgeber-Schlüssel unter Verwendung des Protokolls der Schlüsselauslieferungsanforderung (KDR), beschrieben in Anhang D der ERCA-Policy, bei der ERCA an.

6.4 Transportschlüssel der Root-CA

[r6.21]

Für den Fall, dass die Root-CA der D-CA zur Absicherung der gegenseitigen Kommunikation kryptographische Schlüssel zur Verfügung stellt, so ist deren Vertraulichkeit und Integrität von der D-CA wirksam zu schützen sowie jeglicher Missbrauch wirksam zu verhindern.

6.5 Eigene Transportschlüssel der D-CA

[r6.22]

Für den Fall, dass die D-CA ihren Kommunikationspartnern (etwa Personalisierer, Gerätehersteller,...) zur Absicherung der gegenseitigen Kommunikation kryptographische Schlüssel zur Verfügung stellt, so ist deren Vertraulichkeit und Integrität von der D-CA wirksam zu schützen sowie jeglicher Missbrauch wirksam zu verhindern.

Die D-CA verpflichtet ihre Kommunikationspartner dazu, in deren Einflussbereich gleichwertige Sicherheitsvorkehrungen zum Schutz der Schlüssel zu treffen.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

7 Schlüsselmanagement asymmetrischer Karten- und Geräteschlüssel

Dieser Abschnitt enthält Anforderungen für die Erzeugung und den Umgang mit asymmetrischen kryptographischen Schlüsseln für Kontrollkarten und Kontrollgeräte und die zugehörigen Zertifikate. Anforderungen für die symmetrischen Schlüssel K_m , $K_{m_{WC}}$, $K_{m_{VU}}$ finden sich in Abschnitt 6.3.

7.1 Allgemeine Anforderungen, Protokollierung

[r7.1]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass Initialisierung, Beschlüsselung und Personalisierung der Karten und Kontrollgeräte in besonders abgesicherten Produktionsumgebungen erfolgen. Der Zutritt zu diesen Bereichen muss wirksam beschränkt und kontrollierbar sein. Die Administration der entsprechenden Systeme muss die Anwesenheit von mindestens zwei gemäß Rollenkonzept verantwortlichen Personen erfordern.

Jeder Zutritt zu den Systemen, jeder Zugriff auf die Systeme sowie alle von den Systemen vorgenommenen Aktionen müssen revisionssicher so protokolliert werden, dass die Verfügbarkeit und Integrität der Protokollierung auch im Falle einer Schlüsselkompromittierung sichergestellt ist.

[r7.2]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass bei der Initialisierung, Beschlüsselung und Personalisierung der Karten und Kontrollgeräte sicherheitskritische Informationen wie private Schlüssel u. ä. entsprechend der Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 und der CA-Policy geschützt werden.

[r7.3]

Die D-MSA verpflichtet etwaige externe Dienstleister dazu, die übernommenen Aufgaben vollständig getrennt von ihren sonstigen Tätigkeiten wahrzunehmen. Dies gilt insbesondere dann, wenn der Dienstleister auch für die CAs anderer Mitgliedsstaaten Aufgaben übernimmt.

Die D-MSA verpflichtet etwaige externe Dienstleister dazu, ihre Tätigkeit gemäß [r7.1] revisionssicher zu protokollieren und der D-MSA auf Anforderung Einblick in die Protokollierung zu gestatten.

[r7.4]

Die bei der Personalisierung von Karten und Kontrollgeräten aufgenommenen Protokollierungen müssen eine Zuordnung der jeweiligen Aktion zur zugehörigen Karten-/Geräte-Nummer und zum zugehörigen Zertifikat erlauben.

7.2 Schlüsselerzeugung

[r7.5]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass die Erzeugung der Schlüssel in einer besonders abgesicherten Produktionsumgebung erfolgt, die insbesondere die Geheimhaltung des jeweiligen privaten Schlüssels gewährleistet. Für die dabei einzusetzenden Geräte gelten die gleichen Anforderungen wie für die zur Erzeugung des Schlüsselpaars der D-CA eingesetzten Geräte.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

[r7.6]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereiches sicher, dass private Schlüssel unmittelbar nach ihrer Einbringung in die jeweiligen Karten oder Geräte dauerhaft aus den Speichern der Schlüsselerzeugungs- und Personalisierungssysteme gelöscht werden, sofern die Schlüsselgenerierung nicht direkt im Chip erfolgt.

[r7.7]

Die D-CA stellt sicher, dass innerhalb ihres Verantwortungsbereiches das Auftreten von Schlüsselduplikaten mit hoher Wahrscheinlichkeit ausgeschlossen ist.

[r7.8]

Die Schlüsselerzeugung kann auf Vorrat erfolgen („Batch-Verfahren“), sofern durch technisch-organisatorische Maßnahmen sichergestellt ist, dass ein Missbrauch der vorgehaltenen Schlüsselpaare wirksam verhindert wird. Der Schlüsselvorrat darf die Produktionsmenge eines Monats nicht überschreiten.

7.3 Schlüsselverwendung

[r7.9]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass die jeweiligen privaten Schlüssel ausschließlich zum Zwecke ihrer Bestimmung gemäß der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 genutzt werden können. Dies schließt insbesondere ein, dass nach Beendigung des Personalisierungsvorgangs keine Kopien dieser Schlüssel außerhalb der gesicherten Umgebungen der Kontrollkarten und Kontrollgeräte existieren.

[r7.10]

Der D-CP stellt innerhalb ihres Einflussbereichs sicher, dass nur solche Karten ausgeliefert werden, bei denen optische und logische Personalisierung jeweils korrekt auf den Karteninhaber verweisen.

[r7.11]

Von den geheimen Mitgliedstaatenschlüssel kann ein Backup gefertigt werden unter Verwendung einer Schlüsselwiederherstellungsprozedur im 4-Augen-Prinzip.

[r7.12]

Die D-MSA, D-CA, D-CP und Hersteller stellen innerhalb ihres Einflussbereichs sicher, dass private Schlüssel nach Ablauf der Nutzungsdauer einer Kontrollkarte oder eines Kontrollgeräts nicht weiter genutzt werden können.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

8 Zertifikatsmanagement

Dieser Abschnitt enthält Anforderungen an die Erstellung und Verwendung der von der D-CA erzeugten Zertifikate während des Lebenszyklus der betreffenden Kontrollgerätkarten und Kontrollgeräte.

8.1 Registrierung

[r8.1]

Die D-CA stellt innerhalb ihres Einflussbereichs sicher, dass vor der Ausstellung eines Zertifikats eine ordnungsgemäße Registrierung in den dafür zuständigen Stellen stattgefunden hat.

[r8.2]

Insbesondere stellt dabei die D-CP sicher, dass die Registrierungsdaten eine eindeutige Zuweisung der „Certificate Holder Reference“ nach Anforderung CSM_017 aus Anlage 11 zu Anhang I (B) der VO(EG) 2135/98 ermöglicht.

[r8.3]

Sofern die Schlüsselgenerierung außerhalb der D-CA stattfindet, erstellt die D-CA das beantragte Zertifikat nur dann, wenn der Antragsteller gemäß einem vorab vereinbarten Verfahren nachgewiesen hat, dass er über den zugehörigen privaten Schlüssel verfügt. Der private Schlüssel soll dabei die gesicherte Umgebung der Schlüsselgenerierung nicht verlassen.

8.2 Zertifikatserteilung

[r8.4]

Die D-CA erstellt Zertifikate nur dann, wenn ein ordnungsgemäßer Zertifikatsantrag einer dafür bevollmächtigten Stelle vorliegt und wenn bei der Antragstellung alle Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 und aller damit zusammenhängender Rechtsvorschriften und Vereinbarungen eingehalten worden sind.

Bei einem automatisierten Verfahren ist eine Zertifikatserstellung durch manuellen Eingriff in das System auszuschließen.

[r8.5]

Die D-CA stellt innerhalb ihres Einflussbereichs sicher, dass die von ihr erstellten Zertifikate nur an den Antragsteller übermittelt werden.

[r8.6]

Die D-CA erstellt Zertifikate nur für solche Geräte und Karten, für die eine Bauartgenehmigung ausgestellt wurde.

[r8.7]

Schlüssel-Zertifikats-Anforderungen, die auf dem Transport von geheimen Schlüsseln beruhen, sind nicht erlaubt.

8.3 Zertifikatgültigkeit

[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,

Elektronischer Fahrtschreiber Deutsche CA-Policy Version 1.0

- Unternehmenskarten nicht länger als 5 Jahre gerechnet vom Zeitpunkt des Beginns der Gültigkeit der jeweiligen Karte. Zertifikate für Fahrzeugeinheiten haben eine unbegrenzte Gültigkeitsdauer.

8.4 Zertifikatinhalte und -formate

[r8.9]

Inhalte und Formate der von der D-CA erstellten Zertifikate entsprechen den Anforderungen der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, insbesondere den in Anlage 11 zum Anhang I (B) genannten Spezifikationen.

Die D-CA signiert alle von ihr erstellten Zertifikate mit ihrem privaten Signaturschlüssel.

Die D-MSA stellt sicher, dass der Key Identifier (KID) und Modulus (n) von Schlüsseln, die der ERCA zur Zertifizierung und für die Anforderung von Weg-/Geschwindigkeitsgeber-Schlüssel vorgelegt werden, einmalig innerhalb des Einflussbereichs der D-CA sind.

8.5 Informationspflichten der D-CA

[r8.10]

Die D-CA übergibt alle Zertifikatsdaten an D-CP und Hersteller, so dass Zertifikate, Geräte bzw. Karten und Karteninhaber miteinander verknüpft werden.

[r8.11]

Sofern bestimmte Stellen ein berechtigtes Interesse an speziellen, nicht öffentlichen Informationen zur Tätigkeit der D-CA oder ihrer externen Auftragnehmer haben, und keine Vorschriften oder keine Sicherheitsbedenken dieser Auskunftserteilung entgegen stehen, stellt die D-CA diese Informationen in Abstimmung mit der D-MSA schnellstmöglich und korrekt zur Verfügung.

[r8.12]

Das Betriebskonzept der D-CA ist vertraulich zu behandeln. Informationen daraus dürfen in Absprache mit der D-MSA Vorort bei der D-CA eingesehen, wenn ein nachgewiesenes, berechtigtes Interesse vorliegt und die Vertraulichkeit der Informationen auch beim Empfänger hinreichend geschützt ist.

[r8.13]

Die D-CA führt die Zertifikatsstatusinformationen und stellt sie zur Verfügung.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

9 Informations-Sicherheit

9.1 Informations-Sicherheitsmanagement (ISMS)

[r9.1]

Die D-CA und alle ggf. von ihr beauftragten Dienstleister etablieren ein geeignetes Informations-Sicherheitsmanagement-System (ISMS), durch das die informationstechnische Sicherheit aller für die Aufgaben der D-CA relevanten Tätigkeiten dauerhaft gewährleistet ist.

Die Vorgehensweisen sollen den Anforderungen von [ISO] 17799 sowie [GSHB] genügen.

[r9.2]

Die D-CA stellt sicher, dass für alle im Zusammenhang mit der D-CA relevanten IT-Systeme und Informationen eine Schutzbedarfsfeststellung nach [GSHB] durchgeführt wird.

[r9.3]

Für die Tätigkeit der D-CA ist ein Sicherheitskonzept zu erstellen. Dieses Konzept ist mit dem Betriebskonzept abzustimmen.

[r9.4]

Erstellung und Aktualisierung des Betriebskonzepts sind Bestandteil des Informations-Sicherheitsmanagements.

9.2 Besondere Anforderungen an das Sicherheitskonzept

Der folgende Abschnitt stellt innerhalb des Sicherheitskonzepts *besonders* zu beachtende Gesichtspunkte zusammen. Er ist *nicht* als abschließende Aufzählung von dessen Inhalten gedacht.

[r9.5]

Die D-CA stellt sicher, dass nur zuverlässiges und ausreichend qualifiziertes Personal mit den erforderlichen Tätigkeiten betraut wird. Dies gilt auch für das Personal bei externen Auftragnehmern.

[r9.6]

Die für die Tätigkeit der D-CA und ggf. externer Dienstleister eingesetzten IT-Systeme müssen so betrieben werden, dass mögliche Schädigungen durch Viren und anderen schadhafte Code weitestgehend verhindert sowie die möglichen Folgen von 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.

[r9.7]

Die Initialisierung von Systemen, die den privaten Signaturschlüssel der D-CA oder die geheimen symmetrischen Schlüssel $K_{m_{VU}}$, $K_{m_{WC}}$ oder K_m enthalten, darf nur in Kooperation von zwei Personen erfolgen, die vom System vorab ausreichend sicher zu authentifizieren sind.

[r9.8]

Die D-CA soll für ihre Aufgaben vertrauenswürdige Systeme und Software einsetzen, die durch geeignete Maßnahmen wirksam gegen unautorisierte Veränderungen geschützt sind. Sofern speziell entwickelte Soft- oder Hardware eingesetzt wird, müssen die relevanten Sicherheitsvorgaben bereits im Entwicklungsprozess nachvollziehbar berücksichtigt werden. Bei allen Veränderungen der eingesetzten Soft- und Hardware müssen dokumentierte Kontrollmechanismen umgesetzt werden.

Elektronischer Fahrtenschreiber Deutsche CA-Policy Version 1.0

[r9.9]

Die innerhalb der D-CA eingesetzten Netzwerke und die dort gespeicherten und verarbeiteten Daten sind durch besondere Schutzmechanismen (wie z. B. Firewalls) gegen externe Zugriffe zu schützen.

[r9.10]

Alle sicherheitsrelevanten Aktionen und Prozesse auf den für die Tätigkeit der D-CA 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.

[r9.11]

Die Protokolle sind gegen Veränderung und unberechtigten Zugriff zu schützen. Sie sollen regelmäßig und anlassbezogen ausgewertet und analysiert werden.

[r9.12]

Die Protokolldaten sollen für mindestens 7 Jahre so aufgehoben werden, dass eine Auswertung während dieser Zeitspanne jederzeit möglich ist.

[r9.13]

Die D-CA erstellt einen Notfallplan, in den das Verhalten bei schwerwiegenden Notfällen wie einer Schlüsselkompromittierung oder beim Verlust oder Ausfall von relevanten Daten und/oder IT-Systemen festgelegt ist.

[r9.14]

Die D-CA gewährleistet einen ausreichenden infrastrukturellen und physischen Schutz ihrer Daten und IT-Systeme. Dieser umfasst insbesondere einen ausreichenden Zutrittsschutz für sicherheitsrelevante Bereiche.

Bereiche, in denen private und geheime Schlüssel erzeugt, aufbewahrt und verarbeitet werden, müssen durch besondere Maßnahmen geschützt werden.

9.3 Rollentrennung

[r9.15]

Durch die Einrichtung von Rollenkonzepten soll verhindert werden, dass einzelne Personen Sicherheitsvorkehrungen der D-CA umgehen. Hierzu werden den einzelnen Rollen jeweils beschränkte Rechte und Pflichten zugewiesen. Die genaue Ausgestaltung hängt von den konkreten Abläufen bei der D-CA ab und bleibt dem Betriebskonzept der D-CA vorbehalten. Folgende Rollen sind aber mindestens vorzusehen:

- D-CA-Verantwortlicher (NR)
- Key-Manager (KM)
- CA-Administrator (CAA)
- 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.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Die Inhaber dieser Rollen sind von den IT-Systemen der D-CA zuverlässig zu authentifizieren.

[r9.16]

Die NR-Rolle umfasst:

- Er ist für den sicheren und störungsfreien Betrieb der D-CA als Organisation zuständig.
- Er vertritt die Organisation nach außen und ist in der D-CA-Organisation weisungsbefugt.
- Er ist nicht direkt an der Realisierung von Geschäftsprozessen beteiligt, sondern neben der Gesamtleitung der D-CA verantwortlich für die Einhaltung und Überwachung von Sicherheitsmaßnahmen.
- Er übernimmt die Verantwortung für das Change-Management.

[r9.17]

Die KM-Rolle umfasst:

- die sichere Durchführung der Key-Management-Prozesse,
- die Erzeugung, Zertifizierung, Verwaltung und Löschung der asymmetrischen Schlüssel der D-CA, sowie der symmetrischen Schlüssel, die zur Verschlüsselung von Daten der Kontrollgeräte bzw. Werkstattkarten dienen.

Die Rolle Key-Manager kann nur im Vier-Augen-Prinzip umgesetzt werden.

[r9.18]

Die CAA-Rolle umfasst:

- Verantwortlich für den reibungslosen Betrieb der technischen Systeme der D-CA.

[r9.19]

Die SysA-Rolle umfasst:

- Er ist verantwortlich für den reibungslosen Betrieb der technischen Netzwerkkomponenten der D-CA. Dies betrifft beispielsweise die FireWall-Komponenten, die VPN-Komponenten und die Verkabelung. Einstellungen auf der FireWall und auf den VPN-Gateway sind nur im Vier-Augen-Prinzip gestattet.

[r9.20]

Die ISSO-Rolle umfasst:

- die Überwachung der Sicherheit aller Geschäftsprozesse im Detail und die Auswertung der Sicherheitsmaßnahmen.
- die Überwachung aller anderen Rollen, die Umsetzung der Security Policy, das Change-Management bzw. die Realisierung der Geschäftsprozesse und Anweisungen innerhalb der D-CA-Organisation.
- die Verantwortung zur Durchführung der Audits, die regelmäßig innerhalb der D-CA-Organisation vorgenommen werden müssen.
- die Verantwortung für die Erstellung und Pflege des Sicherheitskonzeptes.
- die Teilnahme an der Mitgliedstaatenschlüssel-Generierung.

[r9.21]

Sofern die D-CA Teile ihrer Aufgaben an externe Dienstleister überträgt, müssen diese ein ihren Aufgaben entsprechendes Rollenkonzept einrichten.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

10 Beendigung des D-CA-Betriebs

10.1 Verlegung der D-CA Verantwortlichkeit

Die D-MSA entscheidet über eine Verlegung der D-CA-Verantwortlichkeit. Dafür muss die D-MSA eine neue D-CA benennen. Um diese Verlegung durchzuführen, müssen die folgenden Punkte erfüllt werden.

[r10.1]

Die D-MSA stellt sicher, dass die Übertragung der Aufgaben und Pflichten an die neue D-CA in geeigneter Art und Weise zu erfolgen hat.

[r10.2]

Die alte D-CA muss alle vorhandenen D-CA-Schlüssel an die neue D-CA übertragen. Die Art und Weise wird durch die D-MSA bestimmt.

[r10.3]

Kopien von Schlüsseln jeglicher Art, die in Zusammenhang mit der alten D-CA gebracht werden können oder nicht transferiert werden konnten, müssen vernichtet werden.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

11 Überprüfungen des Betriebs

11.1 D-CA

[r11.1]

Die D-MSA stellt die Durchführung von regelmäßigen und anlassbezogenen unabhängigen Überprüfungen des Betriebs der D-CA sicher. Eine entsprechende Überprüfung soll mindestens einmal jährlich erfolgen. Die D-MSA kann externe Dienstleister mit dieser Aufgabe betrauen.

Bei Überprüfungen des D-CA-Betriebs muss insbesondere die Übereinstimmung des laufenden Betriebs mit den relevanten Rechtsvorschriften, mit der D-CA-Policy sowie mit dem aktuellen Betriebskonzept und dem aktuellen IT-Sicherheitskonzept verifiziert werden.

Von der D-CA ggf. beauftragte externe Dienstleister sind in die Überprüfung einzubeziehen.

[r11.2]

Die D-MSA stellt sicher, dass die Sicherheit des Betriebs des D-CA durch die Überprüfungen nicht beeinträchtigt wird. Insbesondere stellt sie sicher, dass die Ergebnisse der Überprüfungen Unbefugten nicht zugänglich gemacht werden.

Sie verpflichtet ggf. externe Dienstleister zur Verschwiegenheit.

[r11.3]

Die D-MSA fasst die Ergebnisse der Überprüfung in einem Bericht zusammen, der die Abhilfemaßnahmen definiert, einschließlich eines Implementierungsplanes, der erforderlich ist, um die Verpflichtungen der D-MSA zu erfüllen. Der Bericht ist in englischer Sprache an die ERCA zu leiten.

[r11.4]

Sofern Überprüfungen der D-CA Schwachstellen oder Abweichungen offengelegt haben, veranlasst die D-MSA die D-CA, diese zu beseitigen. Die D-CA berichtet der D-MSA unverzüglich über Einleitung und Abschluss dieser Maßnahmen. Die D-MSA kann eine unabhängige Überprüfung des Erfolgs dieser Maßnahmen anordnen.

11.2 D-CP und Hersteller

[r11.5]

Die Einhaltung der Sicherheitsvorschriften, insbesondere der deutschen CA-Policy sind nachzuweisen durch

- ein Zertifikat von einem vom BSI oder vergleichbaren EU-Behörden akkreditierten Prüflabor,
- mindestens einmal jährliche Audits.

Die Kosten trägt der Hersteller bzw. der D-CP.

[r11.6]

Anlassbezogene Audits im Zusammenhang mit der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 können jederzeit von der D-MSA und der D-CA verlangt werden. Sollten Unregelmäßigkeiten nachgewiesen werden, trägt der Hersteller bzw. D-CP die Kosten. Andernfalls trägt die veranlassende Aufsichtsstelle die Kosten.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

12 Änderungen und Anpassungen der D-CA-Policy

[r12.1]

Anträge zur Änderung der D-CA-Policy sind an die D-MSA zu richten, welche in angemessener Frist geeignete Maßnahmen zu treffen hat.

[r12.2]

Die einzigen Änderungen in der D-CA-Policy, die ohne Benachrichtigung erfolgen können, sind:

- a) redaktionelle oder Schreibfehlerkorrekturen
- b) Änderungen in der Kontaktadresse

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

13 Übereinstimmung mit der ERCA Policy

Die Anforderungen für die Deutsche CA-Policy sind in der ERCA-Policy in § 5.3 beschrieben. Die nachstehende Tabelle stellt die Verbindung zwischen den in der ERCA Policy formulierten Anforderungen und den Anforderungen der Deutschen CA-Policy dar.

Nr.	Referenz ERCA policy	Anforderung	Referenz D-CA-Policy
1.	§ 5.3.1	The MSA Policy shall identify the entities in charge of operations.	§ 1.1 Zuständige Organisationen
2.	§ 5.3.2	The MSCA key pairs for equipment key certification and for motion sensor key distribution shall be generated and stored within a device which either: <ul style="list-style-type: none"> <input type="checkbox"/> is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [10]; <input type="checkbox"/> is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [11]; <input type="checkbox"/> is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [12]; to level E3 or higher in ITSEC [13]; or equivalent security criteria. These evaluations shall be to a protection profile or security target, <input type="checkbox"/> is demonstrated to provide an equivalent level of security. 	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
3.	§ 5.3.3	Member State Key Pair generation shall take place in a physically secured environment by personnel in trusted roles under, at least dual control.	§ 6 Schlüsselmanagement in der D-CA (Absatz 3) § Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.5] § Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.10] § 7.3 Schlüsselverwendung [r7.9] § 9.2 Besondere Anforderungen an das Sicherheitskonzept [r9.7]
4.	§ 5.3.4	The Member State Key Pairs shall be used for a period of at most two years starting from certification by the ERCA.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.7]
5.	§ 5.3.5	The generation of new Member State Key Pairs shall take into account the one month turn-around time required for certification by the ERCA	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.13]
6.	§ 5.3.6	The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.14]
7.	§ 5.3.7	The MSA shall request motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, KmWC, KmVU) [r6.20]
8.	§ 5.3.8	The MSA shall recognise the ERCA public key in the distribution format described in Annex B.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.15]

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Nr.	Referenz ERCA policy	Anforderung	Referenz D-CA-Policy
9.	§ 5.3.9	The MSA shall use the physical media for key and certificate transport described in Annex C.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.16]
10.	§ 5.3.10	The MSA shall ensure that the Key Identifier (KID) and modulus (<i>n</i>) of keys submitted to the ERCA for certification are unique within the domain of the MSCA.	§ 8.4 Zertifikat Inhalte und -formate [r8.9]
11.	§ 5.3.11	The MSA shall ensure that expired keys are not used for any purpose. The Member State private key shall be either: destroyed so that the private key cannot be recovered or retained in a manner preventing its use.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.7]
12.	§ 5.3.12	The MSA shall ensure that an equipment RSA key is generated, transported, and inserted into the equipment, in such a way as to preserve its confidentiality and integrity. For this purpose, the MSA shall <ul style="list-style-type: none"> • ensure that any relevant prescription mandated by security certification of the equipment is met. • ensure that both generation and insertion (if not onboard) takes place in a physically secured environment; • unless key generation was covered by the security certification of the equipment, ensure that specified and appropriate cryptographic key generation algorithms are used; The last two of these requirements on generation shall be met by generating equipment keys within a device which either: <ol style="list-style-type: none"> a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9]; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10]; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target. d) is demonstrated to provide an equivalent level of security. 	§ 7.1 Allgemeine Anforderungen, Protokollierung [r7.1] § 7.2 Schlüsselerzeugung [r7.5]
13.	§ 5.3.13	The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA Policy.	§ 5 Karten- und Gerätemanagement [r5.6] § 6 Schlüsselmanagement in der D-CA (Absatz 2) § 7.1 Allgemeine Anforderungen, Protokollierung [r7.2]
14.	§ 5.3.14	The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA Policy.	§ 6 Schlüsselmanagement in der D-CA (Absatz 2) § 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.9] § 7.2 Schlüsselerzeugung [r7.8]
15.	§ 5.3.15	The Member State private keys may be backed	§ 7.3 Schlüsselerzeugung

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Nr.	Referenz ERCA policy	Anforderung	Referenz D-CA-Policy
		up using a key recovery procedure requiring at least dual control.	[r7.11]
16.	§ 5.3.16	Key certification requests that rely on transportation of private keys are not allowed.	§ 8.2 Zertifikatserteilung [r8.7]
17.	§ 5.3.17	Key escrow is strictly forbidden	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.11]
18.	§ 5.3.18	The MSA shall prevent unauthorised use of its motion sensor keys.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, KmWC, KmVU) [r6.18]
19.	§ 5.3.19	The MSA shall ensure that the motion sensor master key (Km) is used only to encrypt motion sensor data for the purposes of motion sensor manufacturers. The data to be encrypted is defined in the ISO / IEC 16844-3 standard [7].	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
20.	§ 5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, KmWC, KmVU) [r6.18]
21.	§ 5.3.21	The MSA shall forward the workshop card motion sensor key (Km _{WC}) to the component personaliser (in this case, the card personalisation service), by appropriately secured means, for the sole purpose of insertion into workshop cards.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, KmWC, KmVU) [r6.18]
22.	§ 5.3.22	The MSA shall forward the vehicle unit motion sensor key (Km _{VU}) to the component personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.	§ 6.3 Symmetrische Schlüssel für Werkstattkarten und Weg-/Geschwindigkeitsgeber (Km, KmWC, KmVU) [r6.18]
23.	§ 5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
24.	§ 5.3.24	The MSA shall ensure that its motion sensor key copies are stored within a device which either: a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9]; b) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target.	§ 6 Schlüsselmanagement in der D-CA (Absatz 2)
25.	§ 5.3.25	The MSA shall possess different Member State Key Pairs for the production of vehicle unit and tachograph card equipment public key certificates.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.3] § 7.3 Schlüsselverwendung [r7.9]
26.	§ 5.3.26	The MSA shall ensure availability of its equipment public key certification service.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.6]
27.	§ 5.3.27	The MSA shall only use the Member State Private Keys for: a) the production of Annex I(B) equipment key certificates using the ISO / IEC 9796-2 digital signature algorithm as described in	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.4]

Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0

Nr.	Referenz ERCA policy	Anforderung	Referenz D-CA-Policy
		Annex I(B) Appendix 11 <i>Common Security Mechanisms</i> [6]; b) production of the ERCA key certification request as described in Annex A.. c) issuing Certificate Revocation Lists if this method is used for providing certificate status information (see 5.3.30).	
28.	§ 5.3.28	The MSA shall sign equipment certificates within the same device used to store the Member State Private Keys (see 5.3.2).	§ 6 Schlüsselmanagement in der D-CA (Absatz 4)
29.	§ 5.3.29	Within its domain, the MSA shall ensure that equipment public keys are identified by a unique key identifier which follows the prescriptions of Annex 1(B) [6].	§ 8.4 Zertifikatinhalte und -formate [r8.9]
30.	§ 5.3.30	Unless key generation and certification is performed in the same physically secured Environment, the key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.	§ 8 Zertifikatsmanagement [r8.3]
31.	§ 5.3.31	The MSA shall maintain and make certificate status information available.	§ 8.5 Informationspflichten der D-CA [r8.13]
32.	§ 5.3.32	The validity of a tachograph card certificate shall equal the validity of the tachograph card.	§ 8.3 Zertifikatgültigkeit [r8.8]
33.	§ 5.3.33	The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.	§ 8.3 Zertifikatgültigkeit [r8.8]
34.	§ 5.3.34	The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.	§ 8.3 Zertifikatgültigkeit [r8.8]
35.	§ 5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	§ 5 Karten- und Gerätemanagement [r5.8] § 7.3 Schlüsselverwendung [r7.10]
36.	§ 5.3.36	The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.12]
37.	§ 5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	§ 6.2 Schlüsselpaar der D-CA (MS.SK, MS.PK) [r6.6] § 9 Informations-Sicherheit [r9.13]
38.	§ 5.3.38	The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.	§ 9.1 Informations-Sicherheitsmanagement (ISMS) [r9.1]
39.	§ 5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	§ 9.2 Besondere Anforderungen an das Sicherheitskonzept [r9.5] § 9.3 Rollentrennung [r9.15]
40.	§ 5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	§ 8.4 Zertifikatinhalte und -formate [r8.9] § 9 Informations-Sicherheit [r9.10] [r9.11] [r9.12]
41.	§ 5.3.41	The MSA shall include provisions for MSCA termination in the MSA Policy.	§ 10.1 Verlegung der D-CA Verantwortlichkeit
42.	§ 5.3.42	The MSA Policy shall include change procedures.	§ 12 Änderungen und Anpassungen der D-CA-Policy [r12.1]

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Nr.	Referenz ERCA policy	Anforderung	Referenz D-CA-Policy
43.	§ 5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	§ 11.1 D-CA [r11.1] 2. Paragraph
44.	§ 5.3.44	The MSA shall audit the operations covered by the approved policy at intervals of not more than 12 months.	§ 11.1 D-CA [r11.1] 1. Paragraph
45.	§ 5.3.45	The MSA shall report the results of the audit as mentioned in 5.3.43 and provide the audit report, in English, to the ERCA.	§ 11.1 D-CA [r11.3]
46.	§ 5.3.46	The audit report shall define any corrective actions, including an implementation schedule, required to fulfil the MSA obligations.	§ 11.1 D-CA [r11.3]

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Anhang A Abkürzungen, Definitionen

BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	CA-Administrator ↑ siehe CAA-Rolle S. 4
CA-Policy	Zertifizierungs-Policy für die Bundesrepublik Deutschland für die ↑Zertifizierungsstelle der Bundesrepublik Deutschland für den e- lektronischen Fahrtenschreiber gemäß Anlage 11 des Anhangs I (B) VO(EG) 2135/98
Change Management	Behandlung technischer, organisatorischer und/oder fachlicher Änderungen des Verfahrens
D-CA	Die ↑Zertifizierungsstelle der Bundesrepublik Deutschland für den elektronischen Fahrtenschreiber gemäß der ↑VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002, Kraftfahrt-Bundesamt. Nach internationalem Sprachgebrauch (CA = certification authority) ↑ siehe D-CA, S. 4
D-CIA	Ausgabestelle, ↑ siehe D-CIA, S. 4
D-CP	Kartenpersonalisierer. Stelle, die asymmetrische Schlüsselpaare und die gemäß ↑VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 zugehörigen Zertifikate auf die in der ↑VO(EG) 2135/98 definierten Fahrer-, Werkstatt-, Kontroll- und Unternehmenskarten aufbringt. ↑ siehe D-CP, S. 4
D-MSA	Die für die Umsetzung der ↑EU-Richtlinie in der Bundesrepublik Deutschland verantwortliche Stelle, BMVBW. Nach internationalem Sprachgebrauch (MSA = Member State Authority) ↑ siehe D-MSA, S. 4
Digitale Signatur	Verfahren zur Sicherung der Unverfälschtheit (Integrität) und zum Herkunftsnachweis (Authentizität) eines elektronischen Dokuments mittels Anwendung der asymmetrischen Kryptographie.
ERCA	Europäische Route Zertifizierungsstelle
FE	Fahrzeugeinheiten nach Definition der ↑ VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002
ISMS	Informations-Sicherheitsmanagement-System
ISSO	Der Sicherheitsbeauftragte Nach internationalem Sprachgebrauch (ISSO = Information System Security Officer) ↑ siehe ISSO-Rolle S. 4
Kartenpersonalisierer	Siehe D-CP
KDR	Key Distribution Request (Schlüssel-Auslieferungsantrag für den Hauptschlüssel des Weg-/Geschwindigkeitsgebers)
KM	Der Key-Manager ↑ siehe KM-Rolle , S. 4
NR	Der D-CA-Verantwortliche

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Nach internationalem Sprachgebrauch (NR = D-CA-Responsible)
↑ siehe NR-Rolle , S. 4

Öffentlicher Schlüssel	In der asymmetrischen Kryptographie der öffentliche Teil eines Schlüsselpaars. Dieser dient meistens zur Verifizierung einer ↑digitalen Signatur oder zur Verschlüsselung einer Nachricht. (s. auch ↑Privater Schlüssel)
Personalisierung	Auch: logische P. Einbringung von privaten/geheimen Schlüsseln und den zugehörigen Zertifikaten in Kontrollgerätkarten und Kontrollgeräte. Diese ist zu unterscheiden von der optischen P. einer Karte, bei der Namen, Fotos u. ä. auf den Kartenkörper aufgebracht werden.
Privater Schlüssel	In der asymmetrischen Kryptographie der private (geheime) Teil eines Schlüsselpaars. Dieser dient meistens zur Erzeugung einer ↑digitalen Signatur oder zur Entschlüsselung einer Nachricht. (s. auch ↑Öffentlicher Schlüssel)
PS	Das Practice Statement der D-CA, wie es in Kapitel 4 der CA-Policy definiert ist. Im internationalen Kontext ist dafür die Bezeichnung „ <i>Certification Practice Statement (CPS)</i> “ gebräuchlich.
Root-CA	Die europäische ↑Zertifizierungsstelle für den elektronischen Fahrtenschreiber gemäß der ↑ VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002.
Root-Policy	„Digital Tachograph System – European Root Policy“ erstellt vom JRC in Ispra
RSA	Spezielles Verfahren der asymmetrischen Kryptographie. Gemäß Anlage 11 des Anhangs I (B) der VO(EG) 2135/98 wird im elektronischen Fahrtenschreiber das RSA-Verfahren zur Erstellung ↑digitaler Signaturen eingesetzt.
SysA	Der Systemadministrator ↑ siehe SysA-Rolle , S. 4
VPN	Virtual Private Network ↑ siehe SysA-Rolle , S. 4
Zertifikat	In der asymmetrischen Kryptographie wird durch ein Z. die Bindung eines ↑öffentlichen Schlüssels an eine im Z. bezeichnete Identität (Person, Organisation, Maschine,...), die sich im Besitz des zugehörigen ↑privaten Schlüssels befindet, bestätigt. Im Kontext der ↑CA-Policy werden hierunter insbesondere die in Anlage 11 zum Anhang I (B) der ↑VO(EG) 2135/98 definierten Zertifikate verstanden.
Zertifizierungsstelle	Stelle, die ein ↑Zertifikat ausstellt. Im Kontext der VO(EG) 3821/85, VO(EG) 2135/98 und VO(EG) 1360/2002 existieren die Europäische Zertifizierungsstelle (↑Root-CA) und die Zertifizierungsstellen der Mitgliedsstaaten (für Deutschland ↑D-CA), die die für ihre Tätigkeit benötigten Zertifikate von der ↑Root-CA erhalten.

**Elektronischer Fahrtenschreiber
Deutsche CA-Policy Version 1.0**

Anhang B Referenzdokumente

- [CC] Common Criteria. ISO/IEC 15408 (1999)
- [CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP...
- [FIPS] FIPS PUB 140-2. NIST
- [GSHB] BSI-IT-Grundschutzhandbuch
- [ISO] ISO 17799

Begründung:

Die englische Fassung vom 21. Januar 2005 wurde am 9. Februar 2005 von der ERCA¹ genehmigt. Im Anschluss daran wurde die deutsche Übersetzung "(Version 1.0 in der Fassung vom 23. Februar 2005)" erstellt, in der gleichzeitig bestimmte redaktionelle Änderungen (redaktionelle Änderungen müssen nicht von der ERCA genehmigt werden) eingearbeitet wurden. Durchgängig handelt es sich dabei um eine

Anpassung der Schlüssel an die technische Nomenklatur:²

- K_m ersetzen durch Km
- km ersetzen durch Km

- K_{WC} ersetzen durch Km_{WC}
- KWC ersetzen durch Km_{WC}
- k_{VC} ersetzen durch Km_{WC}

- K_{VU} ersetzen durch Km_{VU}
- KVU ersetzen durch Km_{VU}
- k_{VU} ersetzen durch Km_{VU}

Zu Nr. 1.2 Genehmigung

In der Nr. 1.2 wird die Angabe "16. November 2004" durch "9. Februar 2005" ersetzt.

Nicht korrekte Kapitelstruktur³

Bedingt durch die fehlende Setzung des Kapitels 3 (Allgemeine Regelungen) in der Bundesratsdrucksache haben sich in der Kapitelstruktur Verschiebungen ergeben, die dazu führen, dass nahezu alle Querverweise fehlerhaft sind.

1 Die Europäische Zertifizierungsstelle untersteht der Europäischen Kommission.

2 Beispiel (BR-Drucksache): In der Nr. 5, drittes Aufzählungszeichen sind die Angaben "(K_m, K_{WC}, K_{VU})" durch die Angaben "(Km, Km_{WC}, Km_{VU})" zu ersetzen.

3 Beispiel (BR-Drucksache): Nach der Nr. 2 ist die Überschrift "Allgemeine Regelungen" durch die Überschrift "3 Allgemeine Regelungen" zu ersetzen.
Die Überschrift "2.1 Aufgaben und Verpflichtungen" wird ersetzt durch die Überschrift "3.1 Aufgaben und Verpflichtungen".

16. Zu Artikel 1 (§ 7 Abs. 2 Nr. 5 FPersV)
Artikel 2 Nr. 3 (§ 57b Abs. 3 Satz 1 StVZO)

- a) In Artikel 1 sind in § 7 Abs. 2 Nr. 5 nach dem Wort "Anerkennung" die Wörter "oder Beauftragung" einzufügen.
- b) In Artikel 2 Nr. 3 sind in § 57b Abs. 3 Satz 1 nach den Wörtern "amtlich anerkannten Fahrtschreiber- oder Kontrollgerätehersteller" die Wörter "oder durch von diesen beauftragte Kraftfahrzeugwerkstätten" einzufügen.

Begründung:

Prüfungen der Fahrtschreiber und Kontrollgeräte können von anerkannten Werkstätten (Anlage XVIII d zu § 57b Abs. 3 und 4 StVZO) oder von Werkstätten, die von Geräteherstellern beauftragt werden (Anlage XVIII c zu § 57b Abs. 3 und 4 StVZO), vorgenommen werden.

Die Möglichkeit, dass von Geräteherstellern beauftragte Werkstätten Prüfungen vornehmen und zu diesem Zwecke auch Werkstattkarten beantragen können, ist in § 7 Abs. 2 Nr. 5 FPersV und § 57b Abs. 3 StVZO nicht vorgesehen.

Deshalb ist eine Ergänzung in diesen Vorschriften notwendig.

B.

17. Der **federführende Verkehrsausschuss**,
der **Ausschuss für Innere Angelegenheiten** und
der **Finanzausschuss**

empfehlen dem Bundesrat, der Verordnung gemäß Artikel 80 Abs. 2 des Grundgesetzes zuzustimmen.