

I

(Veröffentlichungsbedürftige Rechtsakte)

VERORDNUNG (EG) Nr. 1360/2002 DER KOMMISSION

vom 13. Juni 2002

zur siebten Anpassung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr an den technischen Fortschritt

(Text von Bedeutung für den EWR)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Verordnung (EWG) Nr. 3821/85 des Rates vom 20. Dezember 1985 über das Kontrollgerät im Straßenverkehr ⁽¹⁾, zuletzt geändert durch die Verordnung (EG) Nr. 2135/98 ⁽²⁾, insbesondere auf Artikel 17 und 18,

in Erwägung nachstehender Gründe:

- (1) Die technischen Spezifikationen von Anhang I B der Verordnung (EWG) Nr. 3821/85 sollen an den technischen Fortschritt angepasst werden, wobei der Gesamtsicherheit des Systems und der Interoperabilität zwischen dem Kontrollgerät und den Fahrerkarten besondere Aufmerksamkeit zukommt.
- (2) Im Zusammenhang mit der Anpassung des Geräts sind auch in Anhang II der Verordnung (EWG) Nr. 3821/85, der die Prüfzeichen und Bauartgenehmigungsbogen enthält, Änderungen erforderlich.
- (3) Der durch Artikel 18 der Verordnung (EWG) Nr. 3821/85 eingesetzte Ausschuss gab keine Stellungnahme zu den vorgeschlagenen Maßnahmen ab, und die Kommission unterbreitete daher dem Rat einen diesbezüglichen Vorschlag.
- (4) Da der Rat bis zum Ablauf der in Artikel 18 Absatz 6 Buchstabe b) der Verordnung (EWG) Nr. 3821/85 festgesetzten Frist keinen Beschluss gefasst hat, obliegt es nun der Kommission, diese Maßnahmen zu erlassen —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Der Anhang der Verordnung (EG) Nr. 2135/98 wird durch den Anhang dieser Verordnung ersetzt.

Artikel 2

Anhang II der Verordnung (EWG) Nr. 3821/85 wird wie folgt geändert:

1. Kapitel I Punkt 1 Unterabsatz 1 wird wie folgt geändert:
 - das Symbol für Griechenland „GR“ wird durch „23“ ersetzt;
 - das Symbol für Irland „IRL“ wird durch „24“ ersetzt;
 - das Symbol „12“ für Österreich wird hinzugefügt;
 - das Symbol „17“ für Finnland wird hinzugefügt;
 - das Symbol „5“ für Schweden wird hinzugefügt.
2. Kapitel I Punkt 1 Unterabsatz 2 wird wie folgt ergänzt:
 - Nach dem Wort „Schaublatts“ wird die Formulierung „oder einer Kontrollgerätkarte(n)“ eingefügt.
3. Kapitel I Punkt 2 wird wie folgt geändert:
 - Nach dem Wort „Schaublat“ wird die Formulierung „und auf jeder Kontrollgerätkarte(n)“ eingefügt.
4. In Kapitel II wird dem Titel die Formulierung „FÜR PRODUKTE, DIE DIE ANFORDERUNGEN VON ANHANG I ERFÜLLEN“ angefügt.

⁽¹⁾ ABl. L 370 vom 31.12.1985, S. 8.

⁽²⁾ ABl. L 274 vom 9.10.1998, S. 1.

5. Das folgende Kapitel III wird hinzugefügt:

„III. BAUARTGENEHMIGUNGSBOGEN FÜR PRODUKTE, DIE DIE ANFORDERUNGEN VON ANHANG I B ERFÜLLEN

Der Mitgliedstaat, der eine Bauartgenehmigung erteilt hat, stellt dem Antragsteller einen Bauartgenehmigungsbogen nach dem im Folgenden dargestellten Muster aus. Für die Unterrichtung der anderen Mitgliedstaaten über erteilte Bauartgenehmigungen bzw. deren etwaigen Entzug verwendet der jeweilige Mitgliedstaat Kopien dieses Dokuments.

BAUARTGENEHMIGUNGSBOGEN FÜR PRODUKTE, DIE DIE ANFORDERUNGEN VON ANHANG I B ERFÜLLEN

Name der zuständigen Behörde

Mitteilung betreffend (*):

- ☐ die Bauartgenehmigung für
- ☐ den Entzug der Bauartgenehmigung für
- ☐ das Muster eines Kontrollgeräts
- ☐ die Kontrollgerätkomponente (**)
- ☐ eine Fahrerkarte
- ☐ eine Werkstattkarte
- ☐ eine Unternehmenskarte
- ☐ eine Kontrollkarte

Bauartgenehmigung Nr.

1. Hersteller- oder Handelsmarke
2. Modellbezeichnung
3. Name des Herstellers
4. Anschrift des Herstellers
5. Vorgelegt zur Bauartgenehmigung für
6. Prüfstelle(n)
7. Datum und Nr. der Prüfung(en)
8. Datum der Bauartgenehmigung
9. Datum des Entzugs der Bauartgenehmigung
10. Muster der Kontrollgerätkomponente(n), für die die Komponente bestimmt ist
11. Ort
12. Datum
13. Anlagen (Beschreibungen usw.)

14. Bemerkungen (gegebenenfalls Position von Siegeln)

.....
(Unterschrift)

(*) Zutreffendes ankreuzen.

(**) Komponente angeben, auf die sich die Mitteilung bezieht.“

Artikel 3

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

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

Geschehen zu Brüssel am 13. Juni 2002

Für die Kommission

Loyola DE PALACIO

Vizepräsident

ANHANG

„ANHANG I B

VORSCHRIFTEN FÜR BAU, PRÜFUNG, EINBAU UND NACHPRÜFUNG

Im Interesse der Erhaltung der Interoperabilität der Softwareprogramme der in diesem Anhang definierten Geräte wurden bestimmte Programmierungszeichen, -begriffe und -ausdrücke in der Sprache, in der der Text ursprünglich verfasst worden ist, d. h. im Englischen, belassen. Um die Verständlichkeit zu verbessern, ist hinter bestimmten Ausdrücken in Klammern eine wörtliche Übersetzung beigelegt.

INHALTSVERZEICHNIS

I.	BEGRIFFSBESTIMMUNGEN	8
II.	ALLGEMEINE FUNKTIONSMERKMALE DES KONTROLLGERÄTS	12
	1. Allgemeine Merkmale	12
	2. Funktionen	12
	3. Betriebsarten	13
	4. Sicherheit	14
III.	BAUART- UND FUNKTIONSMERKMALE DES KONTROLLGERÄTS	14
	1. Überwachung des Einsteckens und Entnehmens der Karten	14
	2. Geschwindigkeits- und Wegstreckenmessung	14
	2.1. Messung der zurückgelegten Wegstrecke	15
	2.2. Geschwindigkeitsmessung	15
	3. Zeitmessung	15
	4. Überwachung der Fahrttätigkeiten	16
	5. Überwachung des Status der Fahrzeugführung	16
	6. Manuelle Eingaben durch die Fahrer	16
	6.1. Eingaben des Orts des Beginns und/oder des Endes des Arbeitstages	16
	6.2. Manuelle Eingabe der Fahrttätigkeiten	16
	6.3. Eingabe spezifischer Bedingungen	18
	7. Unternehmenssperrern	18
	8. Überwachung von Kontrollaktivitäten	18
	9. Feststellung von Ereignissen und/oder Störungen:	18
	9.1. Ereignis ‚Einstecken einer ungültigen Karte‘	18
	9.2. Ereignis ‚Kartenkonflikt‘	19
	9.3. Ereignis ‚Zeitüberlappung‘	19
	9.4. Ereignis ‚Lenken ohne geeignete Karte‘	19
	9.5. Ereignis ‚Einstecken der Karte während des Lenkens‘	19
	9.6. Ereignis ‚Letzter Vorgang nicht korrekt abgeschlossen‘	19
	9.7. Ereignis ‚Geschwindigkeitsüberschreitung‘	19

9.8.	Ereignis ‚Unterbrechung der Stromversorgung‘	20
9.9.	Ereignis ‚Datenfehler Weg und Geschwindigkeit‘	20
9.10.	Ereignis ‚Versuch Sicherheitsverletzung‘	20
9.11.	Störung ‚Kartenfehlfunktion‘	20
9.12.	Störung ‚Kontrollgerät‘	20
10.	Integrierte Tests und Selbsttests	20
11.	Auslesen von Daten aus dem Massenspeicher	21
12.	Aufzeichnung und Speicherung von Daten im Massenspeicher	21
12.1.	Gerätekenndaten	21
12.1.1.	Kenndaten der Fahrzeugeinheit	21
12.1.2.	Kenndaten des Weg- und/oder Geschwindigkeitsgebers	22
12.2.	Sicherheitselemente	22
12.3.	Einsteck- und Entnahmedaten der Fahrerkarte	22
12.4.	Fahrtfähigkeitsdaten	23
12.5.	Ort des Beginns und/oder des Endes des Arbeitstages	23
12.6.	Kilometerstandsdaten	23
12.7.	Detaillierte Geschwindkeitsdaten	23
12.8.	Ereignisdaten	23
12.9.	Störungsdaten	25
12.10.	Kalibrierungsdaten	26
12.11.	Zeiteinstellungsdaten	26
12.12.	Kontrolldaten	26
12.13.	Unternehmenssperrdaten	27
12.14.	Erfassen des Herunterladens	27
12.15.	Daten zu spezifischen Bedingungen	27
13.	Auslesen von Daten aus Kontrollgerätkarten	27
14.	Aufzeichnung und Speicherung von Daten auf Kontrollgerätkarten	27
15.	Anzeige	28
15.1.	Standardanzeige	28
15.2.	Warnanzeige	29
15.3.	Menübedienung	29
15.4.	Sonstige Anzeigen	29
16.	Drucken	29
17.	Warnungen	30
18.	Herunterladen von Daten auf externe Datenträger	31
19.	Datenausgabe an externe Zusatzgeräte	31
20.	Kalibrierung	32
21.	Zeiteinstellung	32

22.	Leistungsmerkmale	32
23.	Werkstoffe	32
24.	Markierungen	33
IV.	BAUART- UND KONSTRUKTIONSMERKMALE DER KONTROLLGERÄTKARTEN	33
1.	Sichtbare Daten	33
2.	Sicherheit	36
3.	Normen	36
4.	Spezifikationen für Umgebung und Elektrizität	36
5.	Datenspeicherung	36
5.1.	Kenn- und Sicherheitsdaten der Karte	37
5.1.1.	Anwendungskennung	37
5.1.2.	Chipkennung	37
5.1.3.	IS-Kartenkennung	37
5.1.4.	Sicherheits Elemente	37
5.2.	Fahrerkarte	37
5.2.1.	Kartenkennung	37
5.2.2.	Karteninhaberkennung	38
5.2.3.	Führerscheininformationen	38
5.2.4.	Daten zu gefahrenen Fahrzeugen	38
5.2.5.	Fahrtfähigkeitsdaten	38
5.2.6.	Ort des Beginns und/oder des Endes des Arbeitstages	39
5.2.7.	Ereignisdaten	39
5.2.8.	Störungsdaten	40
5.2.9.	Kontrollaktivitätsdaten	40
5.2.10.	Kartenvorgangsdaten	40
5.2.11.	Daten zu spezifischen Bedingungen	40
5.3.	Werkstattkarte	41
5.3.1.	Sicherheits Elemente	41
5.3.2.	Kartenkennung	41
5.3.3.	Karteninhaberkennung	41
5.3.4.	Daten zu gefahrenen Fahrzeugen	41
5.3.5.	Fahrtfähigkeitsdaten	41
5.3.6.	Daten zum Beginn/Ende des Arbeitstages	41
5.3.7.	Ereignis- und Störungsdaten	41
5.3.8.	Kontrollaktivitätsdaten	41
5.3.9.	Kalibrierungs- und Zeiteinstellungsdaten	42
5.3.10.	Daten zu spezifischen Bedingungen	42
5.4.	Kontrollkarte	42

5.4.1.	Kartenkennung	42
5.4.2.	Karteninhaberkennung	42
5.4.3.	Kontrollaktivitätsdaten	42
5.5.	Unternehmenskarte	43
5.5.1.	Kartenkennung	43
5.5.2.	Karteninhaberkennung	43
5.5.3.	Unternehmensaktivitätsdaten	43
V.	EINBAU DES KONTROLLGERÄTS	43
1.	Einbau	43
2.	Einbauschild	44
3.	Plombierung	44
VI.	EINBAUPRÜFUNGEN, NACHPRÜFUNGEN UND REPARATUREN	45
1.	Zulassung der Installateure oder Werkstätten	45
2.	Prüfung neuer oder reparierter Geräte	45
3.	Einbauprüfung	45
4.	Regelmäßige Nachprüfungen	45
5.	Messung der Anzeigefehler	46
6.	Reparaturen	46
VII.	KARTENAUSGABE	46
VIII.	BAUARTGENEHMIGUNG VON KONTROLLGERÄTEN UND KONTROLLGERÄTKARTEN	46
1.	Allgemeines	46
2.	Sicherheitszertifikat	47
3.	Funktionszertifikat	47
4.	Interoperabilitätszertifikat	47
5.	Bauartgenehmigungsbogen	48
6.	Ausnahmeverfahren für die ersten Interoperabilitätszertifikate	48
Anlage 1:	Datenglossar	
Anlage 2:	Spezifikation der Kontrollgerätkarten	
Anlage 3:	Piktogramme	
Anlage 4:	Ausdrucke	
Anlage 5:	Anzeige	
Anlage 6:	Externe Schnittstellen	
Anlage 7:	Protokolle zum Herunterladen der Daten	
Anlage 8:	Kalibrierungsprotokoll	
Anlage 9:	Bauartgenehmigung — Mindestanforderungen an die durchzuführenden Prüfungen	
Anlage 10:	Allgemeine Sicherheitsanforderungen	
Anlage 11:	Gemeinsame Sicherheitsmechanismen	

I. BEGRIFFSBESTIMMUNGEN

Im Sinne dieses Anhangs bezeichnet der Ausdruck

a) **Aktivierung:**

Phase, in der das Kontrollgerät seine volle Einsatzbereitschaft erlangt und alle Funktionen, einschließlich Sicherheitsfunktionen, erfüllt;

Die Aktivierung eines Kontrollgeräts erfordert die Verwendung einer Werkstattkarte unter Eingabe des entsprechenden PIN-Codes.

b) **Authentisierung:**

Funktion zur Feststellung und Überprüfung der Identität einer Person;

c) **Authentizität:**

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

d) **Integrierter Test:**

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

e) **Kalendertag:**

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

f) **Kalibrierung:**

Aktualisierung oder Bestätigung von Fahrzeugparametern, die im Massenspeicher zu speichern sind. Zu den Fahrzeugparametern gehören die Fahrzeugkennung (Fahrzeugidentifizierungsnummer, amtliches Kennzeichen und zulassender Mitgliedstaat) sowie Fahrzeugmerkmale (Wegdrehzahl, Kontrollgerätkonstante, tatsächlicher Reifenumfang, Reifengröße, Einstellung des Geschwindigkeitsbegrenzers (wenn zutreffend), aktuelle UTC-Zeit, aktueller Kilometerstand);

Zum Kalibrieren eines Kontrollgeräts muss eine Werkstattkarte verwendet werden.

g) **Kartenummer:**

eine aus 16 alphanumerischen Zeichen bestehende Nummer zur eindeutigen Identifizierung einer Kontrollgerät-karte innerhalb eines Mitgliedstaates. Die Kartenummer enthält (gegebenenfalls) einen fortlaufenden Index, einen Ersatzindex und einen Erneuerungsindex.

Die eindeutige Zuordnung einer Karte erfolgt somit anhand des Codes des ausstellenden Mitgliedstaates und der Kartenummer.

h) **fortlaufender Kartenindex:**

das 14. alphanumerische Zeichen einer Kartenummer zur Unterscheidung der verschiedenen Karten, die für ein zum Empfang mehrerer Kontrollgerät-karten berechtigtes Unternehmen oder Gremium ausgestellt wurden. Die eindeutige Identifizierung des Unternehmens bzw. Gremiums erfolgt durch die 13 ersten Zeichen der Kartenummer;

i) **Kartenerneuerungsindex:**

das 16. alphanumerische Zeichen einer Kartenummer, das bei jeder Erneuerung der Kontrollgerät-karte um eine Stelle erhöht wird;

j) **Kartenersatzindex:**

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

k) **Wegdrehzahl des Kraftfahrzeugs:**

eine Kenngröße, die den Zahlenwert des Ausgangssignals angibt, das am Anschlussstutzen für das Kontrollgerät am Kraftfahrzeug (Getriebestutzen bzw. Radachse) bei einer unter normalen Prüfbedingungen zurückgelegten Wegstrecke von einem Kilometer (vgl. Kapitel VI.5.) entsteht. Die Wegdrehzahl wird in Impulsen je Kilometer ($w = \dots \text{ Imp/km}$) ausgedrückt;

l) **Unternehmenskarte:**

eine Kontrollgerätkarte, die dem Eigentümer von Fahrzeugen, in die das Kontrollgerät eingebaut ist, von den Behörden der Mitgliedstaaten zugeteilt wird;

Die Unternehmenskarte weist das Unternehmen aus und ermöglicht die Anzeige, das Herunterladen und den Ausdruck der Daten, die in dem Kontrollgerät gespeichert sind. Die Karte ist anderen Unternehmen gegenüber gesperrt.

m) **Konstante des Kontrollgeräts:**

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

n) **ununterbrochene Lenkzeit, im Kontrollgerät errechnet als ⁽¹⁾:**

die jeweiligen akkumulierten Lenkzeiten eines bestimmten Fahrers seit Ende seiner letzten BEREITSCHAFT oder UNTERBRECHUNG/RUHE oder UNBEKANNTEN Zeit ⁽²⁾ von 45 oder mehr Minuten (dieser Zeitraum kann in mehrere Zeiträume von 15 oder mehr Minuten aufgeteilt worden sein). Bei den Berechnungen werden nach Bedarf die auf der Fahrerkarte gespeicherten bisherigen Tätigkeiten berücksichtigt. Hat der Fahrer seine Karte nicht eingesteckt, beruhen die Berechnungen auf den Massenspeicheraufzeichnungen zu dem Zeitraum, in dem keine Karte eingesteckt war, und zum entsprechenden Lesegerät;

o) **Kontrollkarte:**

eine Kontrollgerätkarte, die einer zuständigen Kontrollbehörde von den Behörden eines Mitgliedstaates ausgestellt worden ist;

Die Kontrollkarte weist die Kontrollbehörde und möglicherweise den Kontrollbeamten aus und ermöglicht das Lesen, Ausdrucken und/oder Herunterladen der im Massenspeicher oder auf Fahrerkarten gespeicherten Daten.

p) **kumulative Unterbrechungszeit, im Kontrollgerät errechnet als ⁽¹⁾:**

die kumulative Lenkzeitunterbrechung eines bestimmten Fahrers wird errechnet als die jeweilige akkumulierte Zeit aus BEREITSCHAFT, UNTERBRECHUNG/RUHE oder UNBEKANNTEN Zeit ⁽²⁾ von 15 oder mehr Minuten seit dem Ende der letzten BEREITSCHAFT oder UNTERBRECHUNG/RUHE oder UNBEKANNTEN Zeit ⁽²⁾ von 45 oder mehr Minuten (dieser Zeitraum kann in mehrere Zeiträume von 15 oder mehr Minuten aufgeteilt worden sein).

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

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

q) **Massenspeicher:**

ein in das Kontrollgerät eingebautes Speichermedium;

r) **digitale Signatur:**

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

s) **Herunterladen:**

das Kopieren eines Teils oder aller im Massenspeicher eines Fahrzeugs oder der im Speicher einer Kontrollgerätkarte enthaltenen Daten zusammen mit der digitalen Signatur;

Beim Herunterladen dürfen gespeicherte Daten weder verändert noch gelöscht werden.

⁽¹⁾ Diese Art der Berechnung der ununterbrochenen Lenkzeit und der kumulativen Pausenzeit dient dem Kontrollgerät zur Errechnung der Warnung für ununterbrochene Lenkzeit. Sie stellt keinen Vorgriff auf die rechtliche Auslegung dieser Zeiten dar.

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

- t) **Fahrerkarte:**
- die von den Behörden eines Mitgliedstaates an die Fahrer ausgegebene Kontrollgerätkarte;
- Die Fahrerkarte enthält die Daten zur Identität des Fahrers und ermöglicht die Speicherung von Tätigkeitsdaten.*
- u) **tatsächlicher Umfang der Fahrzeugreifen:**
- den Mittelwert der von jedem Antriebsrad bei einer vollen Umdrehung zurückgelegten Wegstrecke. Die Messung dieser Wegstrecken muss unter normalen Prüfbedingungen erfolgen (Kapitel VI.5.) und wird in folgender Form ausgedrückt: $l = \dots$ mm. Fahrzeughersteller können die Messung dieser Wegstrecken durch eine theoretische Berechnung ersetzen, bei der die Achslastverteilung des fahrbereiten, unbeladenen Fahrzeugs berücksichtigt wird ⁽¹⁾. Die Verfahren für diese theoretische Berechnung werden von einer zuständigen Behörde des Mitgliedstaats genehmigt;
- v) **Ereignis:**
- vom Kontrollgerät festgestellter anormaler Betrieb, möglicherweise aufgrund eines Betrugsversuchs;
- w) **Störung/Fehlfunktion:**
- vom Kontrollgerät festgestellter anormaler Betrieb, möglicherweise aufgrund eines technischen Defekts oder einer technischen Störung;
- x) **Einbau:**
- die Montage des Kontrollgeräts in einem Fahrzeug;
- y) **Weg- und/oder Geschwindigkeitsgeber:**
- den Bestandteil des Kontrollgeräts, der ein Signal, der ein die Fahrzeuggeschwindigkeit und/oder die zurückgelegte Wegstrecke darstellendes Signal bereitstellt;
- z) **ungültige Karte:**
- eine Karte, die als fehlerhaft festgestellt wurde oder deren Erstauthentisierung fehlgeschlagen oder deren Gültigkeitsbeginn noch nicht erreicht oder deren Ablaufdatum überschritten ist;
- aa) **Kontrollgerät nicht erforderlich:**
- wenn die Anwendung des Kontrollgeräts gemäß den Bestimmungen der Verordnung (EWG) Nr. 3820/85 des Rates nicht erforderlich ist;
- bb) **Geschwindigkeitsüberschreitung:**
- die Überschreitung der zulässigen Fahrzeuggeschwindigkeit, definiert als Zeitraum von mehr als 60 Sekunden, in dem die gemessene Fahrzeuggeschwindigkeit den Höchstwert für die Einstellung des Geschwindigkeitsbegrenzers gemäß Richtlinie 92/6/EWG des Rates vom 10. Februar 1992 über Einbau und Benutzung von Geschwindigkeitsbegrenzern für bestimmte Kraftfahrzeugklassen in der Gemeinschaft ⁽²⁾ überschreitet;
- cc) **regelmäßige Nachprüfung:**
- einen Komplex von Arbeitsgängen zur Überprüfung der ordnungsgemäßen Funktion des Kontrollgeräts und der Übereinstimmung seiner Einstellungen mit den Fahrzeugparametern;
- dd) **Drucker:**
- eine Komponente des Kontrollgeräts, das Ausdrücke gespeicherter Daten liefert;
- ee) **Kontrollgerät:**
- sämtliche für den Einbau in Kraftfahrzeuge bestimmten Geräte zum vollautomatischen oder halbautomatischen Anzeigen, Aufzeichnen und Speichern von Angaben über die Fahrt des Fahrzeugs sowie über bestimmte Arbeitszeiten der Fahrer;

⁽¹⁾ Richtlinie 97/27/EG des Europäischen Parlaments und des Rates vom 22. Juli 1997 über die Massen und Abmessungen bestimmter Klassen von Kraftfahrzeugen und Kraftfahrzeuganhängern und zur Änderung der Richtlinie 70/156/EWG (ABl. L 233 vom 25.8.1997, S. 1).

⁽²⁾ ABl. L 57 vom 2.3.1992, S. 27.

ff) **Erneuerung:**

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

gg) **Reparatur:**

die Reparatur eines Weg- und/oder Geschwindigkeitsgebers oder einer Fahrzeugeinheit, wozu die Trennung von der Stromversorgung oder die Trennung von anderen Komponenten des Kontrollgeräts oder die Öffnung des Kontrollgeräts erforderlich ist;

hh) **Ersatz:**

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

ii) **Sicherheitszertifizierung:**

der Prozess der Zertifizierung durch eine ITSEC ⁽¹⁾-Zertifizierungsstelle, dass das untersuchte Kontrollgerät (oder die Komponente) oder die untersuchte Kontrollgerätkarte die in Anlage 10 „Allgemeine Sicherheitsanforderungen“ aufgeführten Sicherheitsanforderungen erfüllt;

jj) **Selbsttest:**

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

kk) **Kontrollgerätkarte:**

eine Chipkarte zur Verwendung mit dem Kontrollgerät. Kontrollgerätkarten ermöglichen dem Kontrollgerät die Feststellung der Identität (oder Identitätsgruppe) des Karteninhabers und gestatten die Übertragung und Speicherung von Daten. Es gibt folgende Arten von Kontrollgerätkarten:

- Fahrerkarte,
- Kontrollkarte,
- Werkstattkarte,
- Unternehmenskarte;

ll) **Bauartgenehmigung:**

ein Verfahren, mit dem durch einen Mitgliedstaat zertifiziert wird, dass das untersuchte Kontrollgerät (oder die Komponente) oder die untersuchte Kontrollgerätkarte die Anforderungen dieser Verordnung erfüllt;

mm) **Reifengröße:**

die Bezeichnung der Abmessungen der Reifen (äußere Antriebsräder) gemäß Richtlinie 92/23/EWG des Rates ⁽²⁾;

nn) **Fahrzeugkennung:**

Nummern, mit deren Hilfe das Fahrzeug identifiziert werden kann: amtliches Kennzeichen (VRN) mit Angabe des zulassenden Mitgliedstaates und Fahrzeugidentifizierungsnummer (VIN) ⁽³⁾;

oo) **Fahrzeugeinheit (FE):**

das Kontrollgerät ohne den Weg- und/oder Geschwindigkeitsgeber und die Verbindungskabel zum Weg- und/oder Geschwindigkeitsgeber. Die Fahrzeugeinheit kann entweder aus einem oder aus mehreren im Fahrzeug verteilten Geräten bestehen, solange sie den Sicherheitsanforderungen dieser Verordnung entspricht;

⁽¹⁾ Empfehlung des Rates 95/144/EG vom 7. April 1995 über gemeinsame Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ABl. L 93 vom 26.4.1995, S. 27).

⁽²⁾ ABl. L 129 vom 14.5.1992, S. 95.

⁽³⁾ Richtlinie 76/114/EWG des Rates vom 18.12.1975 (ABl. L 24 vom 30.1.1976, S. 1).

pp) **Woche zu Berechnungszwecken im Kontrollgerät:**

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

qq) **Werkstattkarte:**

eine Kontrollgerätkarte, die an eine(n) in einem Mitgliedstaat zugelassene(n) Kontrollgeräthersteller, Installateur, Fahrzeughersteller oder Werkstatt von den Behörden dieses Mitgliedstaates ausgegeben wurde.

Die Werkstattkarte weist den Karteninhaber aus und ermöglicht die Prüfung und Kalibrierung bzw. das Herunterladen der Daten des Kontrollgeräts.

II. ALLGEMEINE FUNKTIONSMERKMALE DES KONTROLLGERÄTS

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

1. Allgemeine Merkmale

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

- 001 Das Kontrollgerät besteht aus Verbindungskabeln, einem Weg- bzw. Geschwindigkeitsgeber und einer Fahrzeugeinheit.
- 002 Die Fahrzeugeinheit besteht aus einem Prozessor, einem Massenspeicher, einer Echtzeituhr, zwei Chipkartenschnittstellen (Fahrer und zweiter Fahrer), einem Drucker, einem Display, einer optischen Warneinrichtung, einem Anschluss zum Kalibrieren/Herunterladen sowie aus Eingabeeinrichtungen.

Über weitere Stecker kann das Kontrollgerät mit anderen Geräten verbunden sein.

- 003 Werden Zusatzeinrichtungen in das Kontrollgerät eingebaut oder daran angeschlossen, dürfen sie unabhängig davon, ob sie zugelassen sind, die einwandfreie Arbeitsweise des Kontrollgeräts und die Bestimmungen der Verordnung weder faktisch noch potentiell beeinträchtigen.

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

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

Das Kontrollgerät zeichnet Daten auf und speichert sie in seinem Massenspeicher und auf Kontrollgerätkarten.

Dies geschieht in Übereinstimmung mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ⁽¹⁾.

2. Funktionen

- 005 Mit dem Kontrollgerät müssen folgende Funktionen gewährleistet sein:

- Überwachung des Einsteckens und Entnehmens von Karten,
- Geschwindigkeits- und Wegstreckenmessung,
- Zeitmessung,
- Überwachung der Fahrtätigkeiten,
- Überwachung des Status der Fahrzeugführung,
- manuelle Eingabe durch die Fahrer:
 - Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages,
 - manuelle Eingabe der Fahrtätigkeiten,
 - Eingabe spezifischer Bedingungen,

⁽¹⁾ ABl. L 281 vom 23.11.1995, S. 31.

- Unternehmenssperrn,
- Überwachung von Kontrollen,
- Feststellung von Ereignissen und/oder Störungen,
- Integrierte Tests und Selbsttests,
- Auslesen von Daten aus dem Massenspeicher,
- Aufzeichnung und Speicherung von Daten im Massenspeicher,
- Auslesen von Daten aus Kontrollgerätkarten,
- Aufzeichnung und Speicherung von Daten auf Kontrollgerätkarten,
- Anzeige,
- Ausdrucken,
- Warnung,
- Herunterladen von Daten auf externe Datenträger,
- Datenausgabe an zusätzliche externe Geräte,
- Kalibrierung,
- Zeiteinstellung.

3. Betriebsarten

006 Das Kontrollgerät verfügt über vier Betriebsarten:

- Betrieb,
- Kontrolle,
- Kalibrierung,
- Unternehmen.

007 Je nachdem, welche gültige Kontrollgerätkarte in die Kartenschnittstellen eingesteckt ist, schaltet das Kontrollgerät auf folgende Betriebsart:

Betriebsart		Steckplatz Fahrer				
		Keine Karte	Fahrerkarte	Kontrollkarte	Werkstattkarte	Unternehmenskarte
Steckplatz 2. Fahrer	Keine Karte	Betrieb	Betrieb	Kontrolle	Kalibrierung	Unternehmen
	Fahrerkarte	Betrieb	Betrieb	Kontrolle	Kalibrierung	Unternehmen
	Kontrollkarte	Kontrolle	Kontrolle	Kontrolle (*)	Betrieb	Betrieb
	Werkstattkarte	Kalibrierung	Kalibrierung	Betrieb	Kalibrierung (*)	Betrieb
	Unternehmenskarte	Unternehmen	Unternehmen	Betrieb	Betrieb	Unternehmen (*)

008 (*) In diesen Zuständen verwendet das Kontrollgerät nur die im Fahrersteckplatz eingesetzte Kontrollgerätkarte.

- 009 Ungültige Karten, die eingesteckt werden, sind vom Kontrollgerät zu ignorieren, doch müssen das Anzeigen, Ausdrucken oder Herunterladen von auf abgelaufenen Karten gespeicherten Daten möglich sein.
- 010 Alle in II.2 aufgeführten Funktionen sind in jeder Betriebsart zu gewährleisten, wobei folgende Ausnahmen gelten:
- die Funktion Kalibrierung ist nur in der Betriebsart Kalibrierung verfügbar,
 - die Funktion Zeiteinstellung ist außerhalb der Betriebsart Kalibrierung nur begrenzt verfügbar,
 - die Funktionen der manuellen Eingabe durch den Fahrer sind nur in den Betriebsarten Betrieb und Kalibrierung verfügbar,
 - die Funktion Unternehmenssperre ist nur in der Betriebsart Unternehmen verfügbar,
 - die Funktion Überwachung der Kontrollen ist nur in der Kontrollbetriebsart verfügbar,
 - die Funktion Herunterladen von Daten ist in der Betriebsart Betrieb nicht verfügbar (außer gemäß Randnummer 150).
- 011 Das Kontrollgerät kann jegliche Daten an Anzeige-, Drucker- oder externe Schnittstellen ausgeben, wobei folgende Ausnahmen gelten:
- in der Betriebsart Betrieb werden persönliche Daten (Vor- und Zuname), die nicht zur einer eingesteckten Kontrollgerätkarte gehören, ausgeblendet, und eine Kartenummer, die nicht zu einer eingesteckten Kontrollgerätkarte gehört, wird teilweise ausgeblendet (von links nach rechts jedes zweite Zeichen),
 - in der Betriebsart Unternehmen (Randnummern 081, 084 und 087) lassen sich Fahrerdaten nur für Zeiträume ausgeben, die nicht von einem anderen Unternehmen (ausgewiesen durch die ersten 13 Stellen der Unternehmenskartenummer) gesperrt sind,
 - ist keine Karte in das Kontrollgerät eingesteckt, lassen sich Fahrerdaten nur für den aktuellen und die acht vorhergehenden Kalendertage ausgeben.

4. Sicherheit

Durch die Systemsicherheit soll folgender Schutz gewährleistet sein: Schutz des Massenspeichers, dass ein unbefugter Zugriff auf die Daten und deren Manipulierung ausgeschlossen ist und alle entsprechenden Versuche entdeckt werden, Schutz der Integrität und Authentizität der zwischen Weg- und/oder Geschwindigkeitsgeber und Fahrzeugeinheit ausgetauschten Daten, Schutz der Integrität und Authentizität der zwischen Kontrollgerät und den Kontrollgerätkarten ausgetauschten Daten sowie Überprüfung der Integrität und Authentizität heruntergeladener Daten.

- 012 Um die Systemsicherheit zu gewährleisten, muss das Kontrollgerät die in den allgemeinen Sicherheitsvorgaben für den Weg- und/oder Geschwindigkeitsgeber und die Fahrzeugeinheit spezifizierten Sicherheitsanforderungen erfüllen (Anhang 10).

III. BAUART- UND FUNKTIONSMERKMALE DES KONTROLLGERÄTS

1. Überwachung des Einsteckens und Entnehmens der Karten

- 013 Das Kontrollgerät überwacht die Kartenschnittstellen und erkennt das Einstecken und Entnehmen einer Karte.
- 014 Beim Einstecken einer Karte erkennt das Kontrollgerät, ob es sich um eine gültige Kontrollgerätkarte handelt, und identifiziert in diesem Fall die Kartenart.
- 015 Das Kontrollgerät muss so ausgelegt sein, dass die Kontrollgerätkarten nach dem ordnungsgemäßen Einstecken in die Kartenschnittstelle einrasten.
- 016 Das Entnehmen der Kontrollgerätkarten darf nur bei stehendem Fahrzeug und nach der Speicherung der jeweiligen Daten auf die Karten sowie durch entsprechende Einwirkung des Benutzers möglich sein.

2. Geschwindigkeits- und Wegstreckenmessung

- 017 Diese Funktion muss kontinuierlich den Kilometerstand entsprechend der gesamten vom Fahrzeug zurückgelegten Wegstrecke messen und angeben können.
- 018 Diese Funktion muss kontinuierlich die Geschwindigkeit des Fahrzeugs messen und angeben können.

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

Geräte zur Anzeige der Geschwindigkeit (Tachometer) und der zurückgelegten Gesamtwegstrecke (Kilometerzähler), die in einem mit einem verordnungsgemäßen Kontrollgerät ausgerüsteten Fahrzeug eingebaut sind, müssen den Vorschriften über die in diesem Anhang (Kapitel III.2.1 und III.2.2) festgelegten zulässigen Fehlergrenzen entsprechen.

2.1. *Messung der zurückgelegten Wegstrecke*

- 020 Die zurückgelegte Wegstrecke kann gemessen werden:
- als Kumulierung sowohl der Vorwärts- als auch der Rückwärtsfahrt oder
 - nur beim Vorwärtsfahren.
- 021 Das Kontrollgerät misst Wegstrecken von 0 bis 9 999 999,9 km.
- 022 Die gemessene Wegstrecke muss innerhalb folgender Fehlergrenzen liegen (Strecken von mindestens 1 000 m):
- $\pm 1 \%$ vor dem Einbau,
 - $\pm 2 \%$ beim Einbau und bei den regelmäßigen Nachprüfungen,
 - $\pm 4 \%$ während des Betriebs.
- 023 Die Wegstreckenmessung erfolgt auf mindestens 0,1 km genau.

2.2. *Geschwindigkeitsmessung*

- 024 Das Kontrollgerät misst die Geschwindigkeit von 0 bis 220 km/h.
- 025 Zur Gewährleistung einer zulässigen Fehlergrenze der angezeigten Geschwindigkeit im Betrieb von ± 6 km/h und unter Berücksichtigung
- einer Fehlergrenze von ± 2 km/h für Inputabweichungen (Reifenabweichungen, ...),
 - einer Fehlergrenze von ± 1 km/h bei Messungen beim Einbau oder bei den regelmäßigen Nachprüfungen
- misst das Kontrollgerät bei Geschwindigkeiten zwischen 20 und 180 km/h und bei Wegdrehzahlen des Fahrzeugs zwischen 4 000 und 25 000 Imp/km die Geschwindigkeit innerhalb einer Fehlergrenze von ± 1 km/h (bei konstanter Geschwindigkeit).
- Anmerkung: Aufgrund der Auflösung der Datenspeicherung ergibt sich eine weitere zulässige Fehlergrenze von $\pm 0,5$ km/h für die vom Kontrollgerät gespeicherte Geschwindigkeit.
- 025a Die Geschwindigkeit muss innerhalb der zulässigen Fehlergrenzen innerhalb von 2 Sekunden nach Abschluss einer Geschwindigkeitsänderung korrekt gemessen werden, wenn sich die Geschwindigkeit mit bis zu 2 m/s^2 geändert hat.
- 026 Die Geschwindigkeitsmessung erfolgt auf mindestens 1 km/h genau.

3. *Zeitmessung*

- 027 Die Zeitmessfunktion läuft ständig und stellt Datum und Uhrzeit digital in UTC bereit.
- 028 Für Datumsangaben im Kontrollgerät (Aufzeichnungen, Ausdrücke, Datenaustausch, Anzeige, ...) sind durchgängig Datum und Uhrzeit in UTC zu verwenden.
- 029 Zur Anzeige der Ortszeit muss es möglich sein, die sichtbare Zeitangabe in Halbstundenschritten zu verändern.
- 030 Die Zeitabweichung darf ± 2 Sekunden/Tag unter Bauartgenehmigungsbedingungen betragen.
- 031 Die Zeitmessung erfolgt auf mindestens 1 Sekunde genau.
- 032 Die Zeitmessung darf durch eine Unterbrechung der externen Stromversorgung von weniger als 12 Monaten unter Bauartgenehmigungsbedingungen nicht beeinträchtigt werden.

4. Überwachung der Fahrtätigkeiten

- 033 Diese Funktion überwacht ständig und gesondert die Tätigkeiten des Fahrers und des zweiten Fahrers.
- 034 Fahrtätigkeiten sind LENKEN, ARBEIT, BEREITSCHAFT und UNTERBRECHUNG/RUHE.
- 035 ARBEIT, BEREITSCHAFT sowie UNTERBRECHUNG/RUHE müssen vom Fahrer und/oder vom zweiten Fahrer manuell ausgewählt werden können.
- 036 Während der Fahrt wird für den Fahrer automatisch LENKEN und für den zweiten Fahrer automatisch BEREITSCHAFT ausgewählt.
- 037 Bei Halt wird für den Fahrer automatisch ARBEIT ausgewählt.
- 038 Bei der ersten Tätigkeitsänderung innerhalb von 120 Sekunden nach dem automatischen Wechsel auf ARBEIT wird davon ausgegangen, dass sie bei Stillstand des Fahrzeugs eingetreten ist (so dass möglicherweise der Wechsel auf ARBEIT aufgehoben wird).
- 039 Die Ausgabe von Tätigkeitsveränderungen an die Aufzeichnungsfunktionen erfolgt auf eine Minute genau.
- 040 Tritt zu irgendeinem Zeitpunkt innerhalb einer Kalenderminute die Tätigkeit LENKEN auf, gilt die gesamte Minute als LENK-Zeit.
- 041 Tritt zu irgendeinem Zeitpunkt innerhalb der unmittelbar der Kalenderminute vorausgehenden und nachfolgenden Minute die Tätigkeit LENKEN auf, gilt die gesamte Minute als LENK-Zeit.
- 042 Für eine Kalenderminute, die aufgrund der vorstehenden Anforderungen nicht als LENK-Zeit gilt, wird die Tätigkeit angesetzt, die als längste Tätigkeit innerhalb der Minute ausgeführt wurde (oder bei gleichlangen Tätigkeiten diejenige, die zuletzt ausgeführt wurde).
- 043 Diese Funktion dient auch der ständigen Überwachung der ununterbrochenen Lenkzeit und der kumulativen Pausenzeit des Fahrers.

5. Überwachung des Status der Fahrzeugführung

- 044 Diese Funktion überwacht ständig und automatisch den Status der Fahrzeugführung.
- 045 Wenn zwei gültige Fahrerkarten in das Gerät eingesteckt sind, wird automatisch der Status TEAM gewählt, in allen anderen Fällen der Status EINMANNBETRIEB.

6. Manuelle Eingaben durch die Fahrer

6.1. Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages

- 046 Diese Funktion ermöglicht dem Fahrer und/oder dem zweiten Fahrer die Eingabe des Ortes, an dem der Arbeitstag beginnt und/oder endet.
- 047 Als Ort gilt ein Land und gegebenenfalls zusätzlich die entsprechende Region.
- 048 Bei Entnahme einer Fahrerkarte (oder Werkstattkarte) wird der Fahrer/zweite Fahrer vom Gerät aufgefordert, den Ort des Endes des Arbeitstages einzugeben.
- 049 Das Kontrollgerät lässt ein Ignorieren dieser Aufforderung zu.
- 050 Die Eingabe des Orts des Beginns und/oder des Endes des Arbeitstages ist auch ohne eingesetzte Karte sowie zu anderen Zeitpunkten als beim Einstecken oder Entnehmen der Karte möglich.

6.2. Manuelle Eingabe der Fahrtätigkeiten

- 050a Beim Einstecken der Fahrerkarte (oder der Werkstattkarte), und nur zu diesem Zeitpunkt,
- zeigt das Gerät dem Karteninhaber Datum und Uhrzeit der letzten Kartenentnahme an und
 - fordert den Karteninhaber auf anzugeben, ob das jetzige Einstecken der Karte eine Fortsetzung des laufenden Arbeitstages darstellt.

Das Kontrollgerät ermöglicht dem Karteninhaber, die Frage ohne Antwort zu ignorieren oder mit Ja bzw. Nein zu beantworten:

- Ignoriert der Karteninhaber die Frage, fordert ihn das Kontrollgerät zur Eingabe eines ‚Orts des Beginns des Arbeitstages‘ auf. Diese Aufforderung kann ignoriert werden. Wird ein Ort eingegeben, so wird dieser zusammen mit der Karteneinsteckzeit im Massenspeicher sowie auf der Kontrollgerätkarte aufgezeichnet.
- Bei Bejahung oder Verneinung fordert das Kontrollgerät den Karteninhaber zur manuellen Eingabe der Tätigkeiten ARBEIT, BEREITSCHAFT oder UNTERBRECHUNG/RUHE mit Datum und Uhrzeit für Beginn und Ende auf, und zwar ausschließlich für den Zeitraum zwischen der letzten Entnahme und dem jetzigen Einstecken der Karte und ohne die Möglichkeit einer Überlappung dieser Tätigkeiten. Dies geschieht nach folgenden Verfahren:
 - Beantwortet der Karteninhaber die Frage mit Ja, fordert ihn das Kontrollgerät zur manuellen Eingabe der Tätigkeiten in chronologischer Reihenfolge für den Zeitraum zwischen der letzten Entnahme und dem jetzigen Einstecken der Karte auf. Der Vorgang endet, wenn die Endzeit einer manuell eingegebenen Tätigkeit der Karteneinsteckzeit entspricht.
 - Beantwortet der Karteninhaber die Frage mit Nein,
 - fordert ihn das Kontrollgerät zur manuellen Eingabe der Tätigkeiten in chronologischer Reihenfolge vom Zeitpunkt der Kartenentnahme bis zum Zeitpunkt des Endes des entsprechenden Arbeitstages auf (oder der Tätigkeiten in Bezug auf dieses Fahrzeug, sofern der Arbeitstag auf einem Schaublatt fortgeführt wird). Bevor also das Kontrollgerät dem Karteninhaber die manuelle Eingabe der einzelnen Aktivitäten gestattet, fordert es ihn auf anzugeben, ob die Endzeit der letzten aufgezeichneten Tätigkeit das Ende einer früheren Arbeitszeit darstellt (siehe Anmerkung).

Anmerkung: Gibt der Karteninhaber nicht das Ende der früheren Arbeitszeit an und gibt manuell eine Tätigkeit ein, deren Endzeit der Karteneinsteckzeit entspricht,

- geht das Kontrollgerät davon aus, dass der Arbeitstag zu Beginn der ersten RUHE-Zeit (oder verbleibenden UNBEKANNTEN Zeit) nach der Kartenentnahme oder zum Zeitpunkt der Kartenentnahme endete, wenn keine Ruhezeit eingegeben wurde (und wenn kein Zeitraum UNBEKANNT bleibt),
- geht das Kontrollgerät davon aus, dass die Anfangszeit gleich der Karteneinsteckzeit ist,
- führt das Kontrollgerät die unten angegebenen Schritte aus.
- Stimmen das Ende der entsprechenden Arbeitszeit und der Zeitpunkt der Kartenentnahme nicht überein oder wurde zu jenem Zeitpunkt kein Ort des Endes des Arbeitstages eingegeben, erhält der Karteninhaber vom Kontrollgerät folgende Aufforderung: ‚Bestätigung/Eingabe Ort des Endes des Arbeitstages‘ (Ignorieren möglich). Wird ein Ort eingegeben, wird er, bezogen auf den Endzeitpunkt des Arbeitstages, nur auf der Kontrollgerätkarte und nur dann aufgezeichnet, wenn sich die Eingabe vom bei der Kartenentnahme eingegebenen Ort unterscheidet.
- Danach erhält der Karteninhaber die Aufforderung: ‚Eingabe Anfangszeit‘ des laufenden Arbeitstages (oder der Tätigkeiten in Bezug auf das derzeitige Fahrzeug, wenn der Karteninhaber zuvor ein Schaublatt während dieses Arbeitstages verwendet hat), sowie die Eingabeaufforderung ‚Ort Beginn des Arbeitstages‘ (Ignorieren möglich). Bei Eingabe eines Ortes wird dieser, bezogen auf diese Anfangszeit, auf der Kontrollgerätkarte aufgezeichnet. Stimmt diese Anfangszeit mit der Karteneinsteckzeit überein, wird der Ort auch im Massenspeicher aufgezeichnet.
- Stimmt diese Anfangszeit nicht mit der Karteneinsteckzeit überein, wird der Karteninhaber zur manuellen Eingabe der Tätigkeiten in chronologischer Reihenfolge von dieser Anfangszeit bis zum Zeitpunkt des Einsteckens der Karte aufgefordert. Der Vorgang endet, wenn die Endzeit einer manuell eingegebenen Tätigkeit der Karteneinsteckzeit entspricht.
- Anschließend erhält der Karteninhaber vom Kontrollgerät die Möglichkeit, Änderungen an den eingegebenen Tätigkeiten vorzunehmen, bis mit Hilfe eines speziellen Kommandos die endgültige Bestätigung erfolgt; danach sind keine Änderungen mehr möglich.
- Antworten auf die erste Frage ohne darauffolgende Eingabe von Tätigkeiten werden vom Kontrollgerät als Ignorieren der Frage durch den Karteninhaber ausgelegt.

Während des gesamten Vorgangs gilt für die Eingabe folgendes Zeitlimit:

- 1 Minute — erfolgt innerhalb dieser 60 Sekunden an den Bedienelementen keine Interaktion (trotz einer visuellen und möglicherweise akustischen Warnung nach 30 Sekunden) oder
- wird die Karte entnommen bzw. eine andere Fahrerkarte (oder Werkstattkarte) eingesteckt oder
- setzt sich das Fahrzeug in Bewegung,

so validiert das Kontrollgerät alle bis dahin gemachten Eingaben.

6.3. *Eingabe spezifischer Bedingungen*

050b Das Kontrollgerät gestattet dem Fahrer die Eingabe der folgenden beiden spezifischen Bedingungen in Echtzeit:

- ‚KONTROLLGERÄT NICHT ERFORDERLICH‘ (Anfang, Ende)
- ‚FÄHRÜBERFAHRT/ZUGFAHRT‘

Bei eingeschalteter Bedingung ‚KONTROLLGERÄT NICHT ERFORDERLICH‘ darf keine ‚FÄHRÜBERFAHRT/ZUGFAHRT‘ erfolgen.

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

7. **Unternehmenssperrern**

- 051 Diese Funktion ermöglicht die Verwaltung der Sperren, die ein Unternehmen einsetzt, um den Datenzugang in der Betriebsart Unternehmen auf sich selbst zu beschränken.
- 052 Unternehmenssperrern bestehen aus einem Anfangszeitpunkt (Datum/Uhrzeit) (Sperrung, Lock-in) und einem Endzeitpunkt (Datum/Uhrzeit) (Entsperrung, Lock-out) im Zusammenhang mit der Identifizierung des Unternehmens anhand der Unternehmenskartennummer (bei der Sperrung).
- 053 Sperren können nur in Echtzeit ein- oder ausgeschaltet werden.
- 054 Das Ausschalten der Sperre kann nur durch das Unternehmen (ausgewiesen durch die ersten 13 Stellen der Unternehmenskartennummer) erfolgen, dessen Sperre eingeschaltet ist, oder
- 055 erfolgt automatisch, wenn ein anderes Unternehmen seine Sperre einschaltet.
- 055a In dem Fall, dass ein Unternehmen die Sperrung aktiviert (lock-in) und die vorhergehende Sperrung für dasselbe Unternehmen war, dann wird angenommen, dass vorher keine Entsperrung vorgenommen worden ist und die Sperre noch eingeschaltet ist.

8. **Überwachung von Kontrollaktivitäten**

- 056 Diese Funktion überwacht die Aktivitäten ANZEIGE, DRUCK, FAHRZEUGEINHEIT und HERUNTERLADEN von der Karte in der Betriebsart Kontrolle.
- 057 Diese Funktion überwacht darüber hinaus in der Betriebsart Kontrolle die Aktivitäten KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG. Eine Kontrolle Geschwindigkeitsüberschreitung gilt als erfolgt, wenn in der Betriebsart Kontrolle der Ausdruck ‚Geschwindigkeitsüberschreitung‘ an den Drucker oder an das Display gesandt wurde oder wenn ‚Ereignis- und Störungsdaten‘ aus dem Massenspeicher der Fahrzeugeinheit heruntergeladen wurden.

9. **Feststellung von Ereignissen und/oder Störungen**

- 058 Diese Funktion stellt folgende Ereignisse und/oder Störungen fest:

9.1. *Ereignis ‚Einstecken einer ungültigen Karte‘*

- 059 Dieses Ereignis wird beim Einstecken einer ungültigen Karte und/oder beim Ablauf der Gültigkeit einer eingesteckten gültigen Karte ausgelöst.

9.2. Ereignis ‚Kartenkonflikt‘

- 060 Dieses Ereignis wird ausgelöst, wenn eine der in der folgenden Tabelle mit X gekennzeichneten Kombinationen von gültigen Karten vorliegen:

Kartenkonflikt		Steckplatz Fahrer				
		Keine Karte	Fahrerkarte	Kontrollkarte	Werkstattkarte	Unternehmenskarte
Steckplatz 2. Fahrer	Keine Karte					
	Fahrerkarte				X	
	Kontrollkarte			X	X	X
	Werkstattkarte		X	X	X	X
	Unternehmenskarte			X	X	X

9.3. Ereignis ‚Zeitüberlappung‘

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

9.4. Ereignis ‚Lenken ohne geeignete Karte‘

- 062 Dieses Ereignis wird bei einer in der folgenden Tabelle mit X gekennzeichneten Kontrollgerätkartenkombination ausgelöst, wenn die Fahrtätigkeit auf LENKEN wechselt oder wenn während der Fahrtätigkeit LENKEN eine Änderung der Betriebsart erfolgt.

Lenken ohne geeignete Karte		Steckplatz Fahrer				
		Keine (oder ungültige) Karte	Fahrerkarte	Kontrollkarte	Werkstattkarte	Unternehmenskarte
Steckplatz 2. Fahrer	Keine (oder ungültige) Karte	X		X		X
	Fahrerkarte	X		X	X	X
	Kontrollkarte	X	X	X	X	X
	Werkstattkarte	X	X	X		X
	Unternehmenskarte	X	X	X	X	X

9.5. Ereignis ‚Einstecken der Karte während des Lenkens‘

- 063 Dieses Ereignis wird ausgelöst, wenn eine Kontrollgerätkarte während der Fahrtätigkeit LENKEN in einen der Steckplätze eingesetzt wird.

9.6. Ereignis ‚Letzter Vorgang nicht korrekt abgeschlossen‘

- 064 Dieses Ereignis wird ausgelöst, wenn das Kontrollgerät beim Einstecken der Karte feststellt, dass trotz der Bestimmungen in Kapitel III.1. der vorherige Kartenvorgang nicht korrekt abgeschlossen wurde (Kartenentnahme, bevor alle relevanten Daten auf der Karte gespeichert wurden). Dieses Ereignis spielt nur für Fahrer- und Werkstattkarten eine Rolle.

9.7. Ereignis ‚Geschwindigkeitsüberschreitung‘

- 065 Dieses Ereignis wird bei jeder Geschwindigkeitsüberschreitung ausgelöst.

9.8. Ereignis ‚Unterbrechung der Stromversorgung‘

- 066 Dieses Ereignis wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet, bei einer 200 Milli-sekunden überschreitenden Unterbrechung der Stromversorgung des Weg- und/oder Geschwindigkeitsgebers und/oder der Fahrzeugeinheit ausgelöst. Die Unterbrechungsschwelle wird vom Hersteller festgelegt. Nicht ausgelöst wird das Ereignis durch den Stromabfall beim Starten des Fahrzeugmotors.

9.9. Ereignis ‚Datenfehler Weg und Geschwindigkeit‘

- 067 Dieses Ereignis wird bei einer Unterbrechung des normalen Datenflusses zwischen dem Weg- und/oder Geschwindigkeitsgeber und der Fahrzeugeinheit und/oder bei einem Datenintegritäts- oder Datenauthentizitätsfehler während des Datenaustauschs zwischen Weg- und/oder Geschwindigkeitsgeber und Fahrzeugeinheit ausgelöst.

9.10. Ereignis ‚Versuch Sicherheitsverletzung‘

- 068 Dieses Ereignis wird, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet, bei jedem sonstigen Ereignis ausgelöst, das die Sicherheit des Weg- und/oder Geschwindigkeitsgebers und/oder der Fahrzeugeinheit entsprechend den allgemeinen Sicherheitszielen dieser Komponenten beeinträchtigt.

9.11. Störung ‚Kartenfehlfunktion‘

- 069 Diese Störung wird ausgelöst, wenn während des Betriebs eine Fehlfunktion der Kontrollgerätkarte auftritt.

9.12. Störung ‚Kontrollgerät‘

- 070 Diese Störung wird bei folgenden Fehlern ausgelöst, sofern sich das Kontrollgerät nicht in der Betriebsart Kalibrierung befindet:

- interne Störung FE
- Druckerstörung
- Anzeigestörung
- Störung Herunterladen
- Sensorstörung

10. Integrierte Tests und Selbsttests

- 071 Mit Hilfe der Funktion ‚Integrierte Tests und Selbsttests‘ muss das Kontrollgerät zur automatischen Fehlererkennung anhand der folgenden Tabelle in der Lage sein:

Zu testende Baugruppe	Selbsttest	Integrierter Test
Software		Integrität
Massenspeicher	Zugriff	Zugriff, Datenintegrität
Kartenschnittstellen	Zugriff	Zugriff
Tastatur		Manuelle Prüfung
Drucker	(dem Hersteller überlassen)	Ausdruck
Display		Visuelle Prüfung
Herunterladen (Ausführung nur während des Herunterladens)	Korrektter Betrieb	
Sensor	Korrektter Betrieb	Korrektter Betrieb

11. Auslesen von Daten aus dem Massenspeicher

- 072 Das Kontrollgerät muss sämtliche in seinem Massenspeicher gespeicherte Daten auslesen können.

12. Aufzeichnung und Speicherung von Daten im Massenspeicher

Im Sinne dieses Absatzes

- sind ‚365 Tage‘ 365 Kalendertage mit durchschnittlicher Fahrtätigkeit in einem Fahrzeug. Als durchschnittliche Tätigkeit je Tag in einem Fahrzeug gelten mindestens 6 Fahrer oder zweite Fahrer, 6 Karteneinsteck-/entnahmevorgänge und 256 Tätigkeitswechsel. Somit umfassen ‚365 Tage‘ mindestens 2 190 Fahrer/zweite Fahrer, 2 190 Karteneinsteck-/entnahmevorgänge und 93 440 Tätigkeitswechsel,
- erfolgt die Zeitaufzeichnung auf eine Minute genau, sofern nicht anders angegeben,
- erfolgt die Aufzeichnung des Kilometerstands auf einen Kilometer genau,
- erfolgt die Geschwindigkeitsaufzeichnung auf 1 km/h genau.

073 Die im Massenspeicher gespeicherten Daten dürfen durch eine Unterbrechung der externen Stromversorgung von weniger als 12 Monaten unter Bauartgenehmigungsbedingungen nicht beeinträchtigt werden.

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

12.1. **Gerätekenndaten**

12.1.1. *Kenndaten der Fahrzeugeinheit*

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

- Name des Herstellers,
- Anschrift des Herstellers,
- Teilnummer,
- Seriennummer,
- Softwareversionsnummer,
- Installationsdatum der Softwareversion,
- Herstellungsjahr,
- Bauartgenehmigungsnummer.

076 Die Kenndaten der Fahrzeugeinheit werden von deren Hersteller aufgezeichnet und dauerhaft gespeichert; eine Ausnahme bildet die softwarebezogenen Daten sowie die Bauartgenehmigungsnummer, die bei einer Aktualisierung der Software verändert werden dürfen.

12.1.2. *Kenndaten des Weg- und/oder Geschwindigkeitsgebers*

077 Der Weg- und/oder Geschwindigkeitsgeber muss in seinem Speicher folgende Kenndaten speichern können:

- Name des Herstellers,
- Teilnummer,
- Seriennummer,
- Bauartgenehmigungsnummer,
- Bezeichner der eingebetteten Sicherheitskomponenten (z. B. Teilnummer des internen Chips/Prozessors),
- Betriebssystembezeichner (z. B. Softwareversionsnummer).

078 Die Kenndaten des Weg- und/oder Geschwindigkeitsgebers werden von dessen Hersteller aufgezeichnet und dauerhaft gespeichert.

079 Die Fahrzeugeinheit muss in ihrem Massenspeicher folgende Kenndaten des derzeit gekoppelten Weg- und/oder Geschwindigkeitsgebers speichern können:

- Seriennummer,
- Bauartgenehmigungsnummer,
- erstes Koppelungsdatum.

12.2. **Sicherheitselemente**

080 Das Kontrollgerät muss die folgenden Sicherheitselemente speichern können:

- den europäischen öffentlichen Schlüssel,
- das Zertifikat des Mitgliedstaates,
- das Gerätezertifikat,
- den privaten Geräteschlüssel.

Die Sicherheitselemente des Kontrollgeräts werden vom Hersteller der Fahrzeugeinheit in das Gerät eingefügt.

12.3. **Einsteck- und Entnahmedaten der Fahrerkarte**

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

- Name und Vorname(n) des Karteninhabers in der auf der Karte gespeicherten Form,
- Kartennummer, ausstellender Mitgliedstaat und Ablauf der Gültigkeit in der auf der Karte gespeicherten Form,
- Datum und Uhrzeit des Einsteckens,
- Kilometerstand beim Einstecken der Karte,
- Steckplatz, in den die Karte eingesetzt wurde,
- Datum und Uhrzeit der Entnahme,
- Kilometerstand bei Entnahme der Karte,
- folgende Informationen über das zuvor vom Fahrer benutzte Fahrzeug in der auf der Karte gespeicherten Form:
 - amtliches Kennzeichen und zulassender Mitgliedstaat,
 - Datum und Uhrzeit der Kartenentnahme,
- Merker zur Angabe, ob der Karteninhaber beim Einstecken Tätigkeiten manuell eingegeben hat oder nicht.

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

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

12.4. Fahrtächtigkeitsdaten

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

- der Status der Fahrzeugführung (TEAM, EINMANNBETRIEB)
- der Steckplatz (FAHRER, ZWEITER FAHRER)
- der Kartenstatus im jeweiligen Steckplatz (INGESTECKT, NICHT INGESTECKT) (siehe Anmerkung)
- die Tätigkeit (LENKEN, BEREITSCHAFT, ARBEIT, UNTERBRECHUNG/RUHE)
- Datum und Uhrzeit des Wechsels.

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

Anmerkung: Vom Fahrer manuell eingegebene Tätigkeitsdaten werden im Massenspeicher nicht aufgezeichnet.

085 Die Speicherdauer der Fahrtächtigkeitsdaten im Massenspeicher muss mindestens 365 Tage betragen können.

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

12.5. Ort des Beginns und/oder des Endes des Arbeitstages

087 Gibt ein Fahrer oder zweiter Fahrer den Ort des Beginns und/oder Endes des Arbeitstages ein, wird im Massenspeicher des Kontrollgeräts Folgendes aufgezeichnet und gespeichert:

- gegebenenfalls die Nummer der (Zweit-)Fahrerkarte und den ausstellenden Mitgliedstaat,
- Datum und Uhrzeit der Eingabe (oder Datum und Uhrzeit, auf die sich die Eingabe bezieht, wenn die Eingabe während des manuellen Eingabevorgangs erfolgt),
- Art der Eingabe (Beginn oder Ende, Eingabebedingung),
- eingegebenes Land und eingegebene Region,
- Kilometerstand.

088 Die Speicherdauer der Anfangs- und/oder Enddaten des Arbeitstages im Massenspeicher muss mindestens 365 Tage betragen können (unter der Annahme, dass ein Fahrer zwei Datensätze pro Tag eingibt).

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

12.6. Kilometerstandsdaten

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

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

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

12.7. Detaillierte Geschwindigkeitsdaten

093 Das Kontrollgerät registriert und speichert in seinem Massenspeicher zu jeder Sekunde mindestens der letzten 24 Stunden, in denen sich das Fahrzeug bewegt hat, die Momentangeschwindigkeit des Fahrzeugs mit den dazugehörigen Datums- und Uhrzeitangaben.

12.8. Ereignisdaten

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

094 Bei jedem festgestellten Ereignis registriert und speichert das Kontrollgerät die folgenden Daten entsprechend den nachfolgend aufgeführten Speichervorschriften:

Ereignis	Speichervorschriften	Je Ereignis aufzuzeichnende Daten
Kartenkonflikt	— die 10 jüngsten Ereignisse	— Beginn des Ereignisses — Datum und Uhrzeit, — Ende des Ereignisses — Datum und Uhrzeit, — Kartenart, Nummer und ausstellender Mitgliedstaat der beiden Karten, die den Konflikt hervorrufen
Lenken ohne geeignete Karte	— das jeweils längste Ereignis an den letzten 10 Tagen des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen	— Beginn des Ereignisses — Datum und Uhrzeit, — Ende des Ereignisses — Datum und Uhrzeit, — Kartenart, Nummer und ausstellender Mitgliedstaat einer zu Beginn und/oder zum Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag
Einstecken der Karte während des Lenkens	— das jeweils letzte Ereignis an den letzten 10 Tagen des Auftretens	— Datum und Uhrzeit des Ereignisses, — Kartenart, Nummer und ausstellender Mitgliedstaat, — Anzahl gleichartiger Ereignisse an diesem Tag
Letzter Vorgang nicht korrekt abgeschlossen	— die 10 jüngsten Ereignisse	— Datum und Uhrzeit des Einsteckens der Karte — Kartenart, Nummer und ausstellender Mitgliedstaat, — aus der Karte ausgelesene Daten des letzten Vorgangs: — Datum und Uhrzeit des Einsteckens der Karte — amtliches Kennzeichen und zulassender Mitgliedstaat
Geschwindigkeitsüberschreitung ⁽¹⁾	— das jeweils gravierendste Ereignis an den letzten 10 Tagen des Auftretens (d. h. das Ereignis mit der höchsten Durchschnittsgeschwindigkeit), — die 5 gravierendsten Ereignisse in den letzten 365 Tagen, — das erste Ereignis nach der letzten Kalibrierung	— Beginn des Ereignisses — Datum und Uhrzeit, — Ende des Ereignisses — Datum und Uhrzeit, — während des Ereignisses gemessene Höchstgeschwindigkeit — während des Ereignisses gemessene arithmetische Durchschnittsgeschwindigkeit — Kartenart, Nummer und ausstellender Mitgliedstaat des Fahrers (wenn zutreffend), — Anzahl gleichartiger Ereignisse an diesem Tag

Ereignis	Speicherungsvorschriften	Je Ereignis aufzuzeichnende Daten
Unterbrechung der Stromversorgung ⁽²⁾	— das jeweils längste Ereignis an den letzten 10 Tagen des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen	— Beginn des Ereignisses — Datum und Uhrzeit, — Ende des Ereignisses — Datum und Uhrzeit, — Kartenart, Nummer und ausstellender Mitgliedstaat einer zu Beginn und/oder zum Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag
Datenfehler Weg und Geschwindigkeit	— das jeweils längste Ereignis an den letzten 10 Tagen des Auftretens, — die 5 längsten Ereignisse in den letzten 365 Tagen	— Beginn des Ereignisses — Datum und Uhrzeit, — Ende des Ereignisses — Datum und Uhrzeit, — Kartenart, Nummer und ausstellender Mitgliedstaat einer zu Beginn und/oder zum Ende des Ereignisses eingesteckten Karte, — Anzahl gleichartiger Ereignisse an diesem Tag
Versuch Sicherheitsverletzung	— die 10 jüngsten Ereignisse nach Ereignisart	— Beginn des Ereignisses — Datum und Uhrzeit, — Ende des Ereignisses — Datum und Uhrzeit (sofern relevant), — Kartenart, Nummer und ausstellender Mitgliedstaat einer zu Beginn und/oder zum Ende des Ereignisses eingesteckten Karte, — Art des Ereignisses

095

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

- Datum und Uhrzeit der letzten KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG,
- Datum und Uhrzeit der ersten Geschwindigkeitsüberschreitung, die dieser KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG folgt,
- Anzahl der Geschwindigkeitsüberschreitungsergebnisse seit der letzten KONTROLLE GESCHWINDIGKEITSÜBERSCHREITUNG.

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

12.9. Störungsdaten

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

096

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

Störung	Speicherungsvorschriften	Je Störung aufzuzeichnende Daten
Kartenfehlfunktion	— die 10 jüngsten Fahrerkartenfehlfunktionen	— Beginn der Störung — Datum und Uhrzeit, — Ende der Störung — Datum und Uhrzeit, — Kartenart, Nummer und ausstellender Mitgliedstaat
Kontrollgerätstörung	— die 10 jüngsten Störungen jeder Störungsart — die erste Störung nach der letzten Kalibrierung	— Beginn der Störung — Datum und Uhrzeit, — Ende der Störung — Datum und Uhrzeit, — Art der Störung — Kartenart, Nummer und ausstellender Mitgliedstaat einer zu Beginn und/oder zum Ende der Störung eingesteckten Karte

12.10. Kalibrierungsdaten

- 097 Das Kontrollgerät registriert und speichert in seinem Massenspeicher Daten in Bezug auf:
- bekannte Kalibrierungsparameter zum Zeitpunkt der Aktivierung,
 - seine erste Kalibrierung nach der Aktivierung,
 - seine erste Kalibrierung im derzeitigen Fahrzeug (identifiziert anhand von dessen Fahrzeugidentifizierungsnummer)
 - die 5 jüngsten Kalibrierungen (erfolgen an einem Kalendertag mehrere Kalibrierungen, ist nur die letzte des Tages zu speichern).
- 098 Zu den einzelnen Kalibrierungen sind folgende Daten zu speichern:
- Zweck der Kalibrierung (Aktivierung, Ersteinbau, Einbau, regelmäßige Nachprüfung)
 - Name und Anschrift der Werkstatt,
 - Werkstattkartennummer, ausstellender Mitgliedstaat und Ablauf der Gültigkeit der Karte,
 - Fahrzeugkennung,
 - aktualisierte und bestätigte Parameter: Wegdrehzahl (w), Kontrollgerätkonstante (k), tatsächlicher Reifenumfang (l), Reifengröße, Einstellung des Geschwindigkeitsbegrenzers, Kilometerstand (alt und neu), Datum und Uhrzeit (alte und neue Werte).
- 099 Der Weg- und/oder Geschwindigkeitsgeber registriert und speichert in seinem Speicher die folgenden Installationsdaten:
- erste Koppelung mit einer Fahrzeugeinheit (Datum, Uhrzeit, FE-Bauartgenehmigungsnummer, FE-Seriennummer),
 - letzte Koppelung mit einer Fahrzeugeinheit (Datum, Uhrzeit, FE-Bauartgenehmigungsnummer, FE-Seriennummer).

12.11. Zeiteinstellungsdaten

- 100 Das Kontrollgerät registriert und speichert in seinem Massenspeicher Daten in Bezug auf:
- die jüngste Zeiteinstellung,
 - die 5 größten Zeiteinstellungen seit der letzten Kalibrierung,
- ausgeführt in der Betriebsart Kalibrierung und nicht im Rahmen einer normalen Kalibrierung (Begriffsbestimmung f).
- 101 Zu den einzelnen Zeiteinstellungen sind folgende Daten zu speichern:
- Datum und Uhrzeit, alter Wert,
 - Datum und Uhrzeit, neuer Wert,
 - Name und Anschrift der Werkstatt,
 - Werkstattkartennummer, ausstellender Mitgliedstaat und Ablauf der Gültigkeit der Karte.

12.12. Kontrolldaten

- 102 Das Kontrollgerät registriert und speichert in seinem Massenspeicher folgende Daten in Bezug auf die 20 jüngsten Kontrollen:
- Datum und Uhrzeit der Kontrolle,
 - Kontrollkartennummer und ausstellender Mitgliedstaat,
 - Art der Kontrolle (Anzeigen und/oder Drucken und/oder Herunterladen von der Fahrzeugeinheit und/oder Herunterladen von der Karte).

- 103 Beim Herunterladen sind zudem die ältesten und die jüngsten heruntergeladenen Tage aufzuzeichnen.

12.13. **Unternehmenssperrdaten**

- 104 Das Kontrollgerät registriert und speichert in seinem Massenspeicher folgende Daten in Bezug auf die 20 jüngsten Unternehmenssperrern:

- Sperrung (Lock-in) — Datum und Uhrzeit,
- Entsperrung (Lock-out) — Datum und Uhrzeit,
- Unternehmenskartennummer und ausstellender Mitgliedstaat,
- Name und Anschrift des Unternehmens.

12.14. **Erfassen des Herunterladens**

- 105 Das Kontrollgerät registriert und speichert in seinem Massenspeicher in Bezug auf das letzte Herunterladen vom Massenspeicher auf externe Datenträger in den Betriebsarten Unternehmen oder Kalibrierung folgende Daten:

- Datum und Uhrzeit des Herunterladens,
- Unternehmens- oder Werkstattkartennummer und ausstellender Mitgliedstaat,
- Name des Unternehmens oder der Werkstatt.

12.15. **Daten zu spezifischen Bedingungen**

- 105a Das Kontrollgerät registriert und speichert in seinem Massenspeicher folgende Daten in Bezug auf spezifische Bedingungen:

- Datum und Uhrzeit des Eintrags,
- Art der spezifischen Bedingung.

- 105b Die Speicherdauer der Daten zu spezifischen Bedingungen im Massenspeicher muss mindestens 365 Tage betragen können (unter der Annahme, dass pro Tag eine Bedingung ein- und ausgeschaltet wird). Ist die Speicherkapazität erschöpft, werden die ältesten Daten durch neue überschrieben.

13. **Auslesen von Daten aus Kontrollgerätkarten**

- 106 Das Kontrollgerät muss aus Kontrollgerätkarten die erforderlichen Daten

- zur Identifizierung der Kartenart, des Karteninhabers, des zuvor genutzten Fahrzeugs, des Datums und der Uhrzeit der letzten Kartenentnahme und der zu jenem Zeitpunkt gewählten Tätigkeit,
 - zur Kontrolle des korrekten Abschlusses des letzten Kartenvorgangs,
 - zur Berechnung der ununterbrochenen Lenkzeit, der kumulativen Pausenzeit und der kumulierten Lenkzeit für die vorangegangene und für die laufende Woche,
 - zur Anfertigung von Ausdrucken von auf einer Fahrerkarte aufgezeichneten Daten,
 - zum Herunterladen einer Fahrerkarte auf externe Datenträger
- auslesen können.

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

14. **Aufzeichnung und Speicherung von Daten auf Kontrollgerätkarten**

- 108 Sofort nach dem Einstecken der Karte stellt das Kontrollgerät die ‚Kartenvorgangsdaten‘ auf der Fahrer- oder Werkstattkarte ein.

- 109 Das Kontrollgerät aktualisiert die auf gültigen Fahrer-, Werkstatt- und/oder Kontrollkarten gespeicherten Daten mit sämtlichen erforderlichen Daten, die für den Karteninhaber und für den Zeitraum, in dem die Karte eingesteckt ist, relevant sind. Die auf diesen Karten gespeicherten Daten sind in Kapitel IV spezifiziert.
- 109a Das Kontrollgerät aktualisiert die auf gültigen Fahrer- und Werkstattkarten gespeicherten Fahrertätigkeits- und Ortsdaten (gemäß Kapitel IV.5.2.5 und 5.2.6) mit Tätigkeits- und Ortsdaten, die vom Karteninhaber manuell eingegeben werden.
- 110 Die Aktualisierung der Kontrollgerätkarten erfolgt so, dass bei Bedarf und unter Berücksichtigung der Speicherkapazität der Karte die jeweils ältesten Daten durch die jüngsten Daten ersetzt werden.
- 111 Bei einem Schreibfehler verwendet das Kontrollgerät maximal dreimal erneut den gleichen Schreibbefehl. Schlagen alle Versuche fehl, wird die Karte für fehlerhaft und ungültig erklärt.
- 112 Vor der Entnahme einer Fahrerkarte und nach Speicherung aller relevanten Daten auf der Karte setzt das Kontrollgerät alle ‚Kartenvorgangsdaten‘ zurück.

15. Anzeige

- 113 Die Anzeige enthält mindestens 20 Zeichen.
- 114 Die Mindesthöhe der Zeichen beträgt 5 mm und die Mindestbreite 3,5 mm.
- 114a Die Anzeige unterstützt die Zeichensätze Latin-1 und Griechisch gemäß ISO 8859, Teil 1 und 7, spezifiziert in Anlage 1 Kapitel 4 ‚Zeichensätze‘. Die Anzeige kann vereinfachte Zeichen verwenden (z. B. können mit Akzent versehene Zeichen ohne Akzent oder Kleinbuchstaben als Großbuchstaben dargestellt werden).
- 115 Die Anzeige ist mit einer blendfreien Beleuchtung auszustatten.
- 116 Die in der Anzeige dargestellten Zeichen müssen von außerhalb des Kontrollgeräts gut sichtbar sein.
- 117 Vom Kontrollgerät müssen folgende Daten angezeigt werden können:
- Standarddaten,
 - Warndaten,
 - Menüzugangsdaten,
 - andere von einem Benutzer angeforderte Daten.

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

- 118 Die Anzeige des Kontrollgeräts verwendet die in Anlage 3 aufgeführten Piktogramme oder Piktogrammkombinationen. Es können auch zusätzliche Piktogramme oder Kombinationen angezeigt werden, sofern sie sich deutlich von den genannten Piktogrammen und Kombinationen unterscheiden.
- 119 Die Anzeige muss sich bei fahrendem Fahrzeug stets im eingeschalteten Zustand befinden.
- 120 Das Kontrollgerät kann eine manuelle oder automatische Abschaltvorrichtung für die Anzeige aufweisen, wenn sich das Fahrzeug nicht in Fahrt befindet.

Das Anzeigeformat ist in Anlage 5 spezifiziert.

15.1. Standardanzeige

- 121 Wenn keine anderen Informationen angezeigt werden müssen, sind vom Kontrollgerät standardmäßig folgende Angaben anzuzeigen:
- die Ortszeit (UTC + Einstellung durch den Fahrer),
 - die Betriebsart,
 - die derzeitige Tätigkeit des Fahrers und die derzeitige Tätigkeit des zweiten Fahrers,

- Informationen zum Fahrer:
 - bei derzeitiger Tätigkeit LENKEN: aktuelle ununterbrochene Lenkzeit und aktuelle kumulative Pausenzeit,
 - derzeitige Tätigkeit nicht LENKEN: aktuelle Dauer der anderen Tätigkeit (seit der Auswahl) und aktuelle kumulative Pausenzeit,
- Informationen zum zweiten Fahrer:
 - aktuelle Dauer seiner Tätigkeit (seit der Auswahl).

- 122 Die Anzeige von Daten zu den Fahrern muss klar, deutlich und eindeutig sein. Lassen sich Fahrer- und Zweitfahrerinformationen nicht gleichzeitig anzeigen, zeigt das Kontrollgerät standardmäßig die Informationen zum Fahrer und ermöglicht dem Benutzer, auf die Anzeige der Informationen zum zweiten Fahrer umzuschalten.
- 123 Lässt die Anzeigebreite eine ständige Anzeige der Betriebsart nicht zu, zeigt das Kontrollgerät bei Betriebsartwechsel die neue Betriebsart kurz an.
- 124 Beim Einstecken der Karte wird der Name des Karteninhabers kurz angezeigt.
- 124a Ist die Bedingung ‚KONTROLLGERÄT NICHT ERFORDERLICH‘ eingeschaltet, muss die Standardanzeige das entsprechende Piktogramm aufweisen (es ist zulässig, dass die aktuelle Fahrertätigkeit nicht gleichzeitig angezeigt wird).

15.2. **Warnanzeige**

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

15.3. **Menübedienung**

- 126 Das Kontrollgerät stellt die erforderlichen Befehle über eine geeignete Menüstruktur bereit.

15.4. **Sonstige Anzeigen**

- 127 Nach Bedarf müssen sich folgende Anzeigen auswählen lassen:
- Datum und Uhrzeit in UTC,
 - Betriebsart (wenn nicht ständig angezeigt),
 - ununterbrochene Lenkzeit und kumulative Pausenzeit des Fahrers,
 - ununterbrochene Lenkzeit und kumulative Pausenzeit des zweiten Fahrers,
 - kumulierte Lenkzeit des Fahrers für die Vorwoche und die laufende Woche,
 - kumulierte Lenkzeit des zweiten Fahrers für die Vorwoche und die laufende Woche,
 - der Inhalt der sechs Ausdrücke im gleichen Format wie die Ausdrücke selbst.
- 128 Die Anzeige des Ausdruckinhalts erfolgt sequentiell, Zeile für Zeile. Beträgt die Anzeigebreite weniger als 24 Zeichen, erhält der Benutzer die vollständige Information durch ein geeignetes Mittel (mehrere Zeilen, Rollen usw.). Für handschriftliche Einträge vorgesehene Ausdruckzeilen brauchen nicht angezeigt zu werden.

16. **Drucken**

- 129 Das Kontrollgerät muss Informationen aus seinem Massenspeicher und/oder von Kontrollgerätkarten anhand der folgenden sechs Ausdrücke drucken können:
- täglicher Ausdruck Fahrertätigkeiten von der Karte,
 - täglicher Ausdruck Fahrertätigkeiten von der Fahrzeugeinheit,

- Ausdruck Ereignisse und Störungen von der Karte,
- Ausdruck Ereignisse und Störungen von der Fahrzeugeinheit,
- Ausdruck Technische Daten,
- Ausdruck Geschwindigkeitsüberschreitung.

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

Am Ende der Ausdrücke können zusätzliche Daten bereitgestellt werden.

Vom Kontrollgerät können auch zusätzliche Ausdrücke bereitgestellt werden, sofern sie von den vorgenannten sechs Ausdrücken deutlich unterscheidbar sind.

- 130 Der ‚tägliche Ausdruck Fahrertätigkeiten von der Karte‘ und der ‚Ausdruck Ereignisse und Störungen von der Karte‘ dürfen verfügbar sein, wenn eine Fahrerkarte oder eine Werkstattkarte in das Kontrollgerät eingesetzt sind. Das Kontrollgerät muss die auf der betreffenden Karten gespeicherten Daten vor Beginn des Ausdrucks aktualisieren.
- 131 Zur Herstellung des ‚täglichen Ausdrucks Fahrertätigkeiten von der Karte‘ und des ‚Ausdrucks Ereignisse und Störungen von der Karte‘
- wählt das Kontrollgerät entweder automatisch die Fahrerkarte oder die Werkstattkarte, wenn nur eine dieser Karten eingesetzt ist,
 - oder ermöglicht einen Befehl zur Auswahl der Quellenkarte oder zur Auswahl der Karte im Fahrersteckplatz, wenn beide Kartenarten im Kontrollgerät eingesetzt sind.
- 132 Der Drucker muss 24 Zeichen pro Zeile drucken können.
- 133 Die Mindesthöhe der Zeichen beträgt 2,1 mm und die Mindestbreite 1,5 mm.
- 133a Der Drucker unterstützt die Zeichensätze Latin-1 und Griechisch gemäß ISO 8859, Teil 1 und 7, spezifiziert in Anlage 1 Kapitel 4 ‚Zeichensätze‘.
- 134 Drucker müssen von ihrer Auslegung her diese Ausdrücke mit einem Auflösungs niveau liefern, das Missverständnisse beim Lesen ausschließt.
- 135 Die Abmessungen der Ausdrücke und die Eintragungen auf den Ausdrücken dürfen unter normalen Feuchtigkeits- (10 bis 90 %) und Temperaturbedingungen keinerlei Veränderungen unterliegen.
- 136 Auf dem vom Kontrollgerät verwendeten Papier sind das Prüfzeichen und der Typ/die Typen des Kontrollgeräts anzugeben, mit denen es eingesetzt werden kann. Die Ausdrücke müssen unter normalen Aufbewahrungsbedingungen hinsichtlich Lichtintensität, Feuchtigkeit und Temperatur mindestens ein Jahr lang deutlich lesbar und identifizierbar bleiben.
- 137 Es muss möglich sein, auf diesen Ausdrücken zusätzliche manuelle Eintragungen wie die Unterschrift des Fahrers vorzunehmen.
- 138 Tritt während des Druckens das Ereignis ‚Kein Papier‘ auf, startet das Kontrollgerät nach dem Nachladen des Papiers den Druckvorgang vom Anfang des Ausdrucks oder setzt den Druck fort, wobei ein eindeutiger Hinweis auf den zuvor gedruckten Teil erfolgt.

17. Warnungen

- 139 Bei Feststellung eines Ereignisses und/oder einer Störung erhält der Fahrer vom Kontrollgerät ein Warnsignal.
- 140 Die Warnung für das Ereignis Unterbrechung der Stromversorgung kann bis zur Wiederherstellung der Stromversorgung aufgeschoben werden.
- 141 Das Kontrollgerät warnt den Fahrer 15 Minuten vor dem Zeitpunkt sowie zum Zeitpunkt der Überschreitung von 4 Std. 30 Min. ununterbrochener Lenkzeit.
- 142 Die Warnungen erfolgen optisch. Zusätzlich zu optischen können auch akustische Warnsignale abgegeben werden.

- 143 Optische Warnungen müssen für den Benutzer eindeutig erkennbar sein, sich im Sichtfeld des Fahrers befinden und sowohl am Tage als auch in der Nacht deutlich lesbar sein.
- 144 Optische Warnungen können in das Kontrollgerät eingebaut oder gerätefern installiert sein.
- 145 Im letzteren Fall erfolgt die Kennzeichnung mit einem „T“-Symbol und in der Farbe gelb oder orange.
- 146 Die Warnsignale haben eine Dauer von mindestens 30 Sekunden, sofern sie nicht vom Benutzer durch Betätigen einer Taste am Kontrollgerät bestätigt werden. Mit dieser ersten Bestätigung darf die im nächsten Absatz angeführte Anzeige des Grundes für die Warnung nicht gelöscht werden.
- 147 Der Grund für die Warnung wird am Kontrollgerät angezeigt und bleibt so lange sichtbar, bis der Benutzer ihn mit einer bestimmten Taste oder mit einem bestimmten Befehl über das Kontrollgerät bestätigt.
- 148 Es können zusätzliche Warnsignale abgegeben werden, solange sie bei den Fahrern zu keinen Verwechslungen mit den vorstehend festgelegten Warnsignalen führen.

18. Herunterladen von Daten auf externe Datenträger

- 149 Das Kontrollgerät muss bei Bedarf über den Anschluss zum Kalibrieren/Herunterladen Daten aus seinem Massenspeicher oder von einer Fahrerkarte an externe Speichermedien herunterladen können. Das Kontrollgerät muss die auf der betreffenden Karte gespeicherten Daten vor Beginn des Ausdrucks aktualisieren.
- 150 Zusätzlich und als optionales Leistungsmerkmal kann das Kontrollgerät in jeder Betriebsart Daten über einen anderen Anschluss an ein über diesen Anschluss authentisiertes Unternehmen herunterladen. In diesem Fall gelten für das Herunterladen die Datenzugriffsrechte der Betriebsart Unternehmen.
- 151 Beim Herunterladen dürfen gespeicherte Daten weder verändert noch gelöscht werden.

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

Die Protokolle zum Herunterladen sind in Anlage 7 spezifiziert.

19. Datenausgabe an externe Zusatzgeräte

- 152 Wenn am Kontrollgerät keine Funktion für die Anzeige der Geschwindigkeit und/oder des Kilometerstands gegeben ist, stellt das Kontrollgerät (ein) Ausgangssignal(e) für die Anzeige der Fahrzeuggeschwindigkeit und/oder für die vom Fahrzeug insgesamt zurückgelegte Wegstrecke zur Verfügung.
- 153 Die Fahrzeugeinheit muss darüber hinaus zur Ausgabe der folgenden Daten über eine geeignete dedizierte serielle Verbindung unabhängig von einer optionalen CAN-Busverbindung (ISO 11898 Straßenfahrzeuge — Austausch digitaler Informationen — Controller Area Network (CAN) für hohe Übertragungsraten) in der Lage sein, so dass deren Verarbeitung durch andere im Fahrzeug installierte elektronische Geräte möglich ist:

- aktuelle(s) Datum und Uhrzeit in UTC,
- Fahrzeuggeschwindigkeit,
- Kilometerstand,
- zur Zeit gewählte Tätigkeit des Fahrers und des zweiten Fahrers,
- Information, ob im Steckplatz des Fahrers oder des zweiten Fahrers zur Zeit eine Karte eingesteckt ist und (gegebenenfalls) Informationen über die entsprechende Kartenkennung (Kartennummer und ausstellender Mitgliedstaat).

Über diese Minimalliste hinaus können noch weitere Daten ausgegeben werden.

Bei eingeschalteter Zündung werden diese Daten ständig ausgesendet. Ist die Zündung ausgeschaltet, ruft zumindest ein Tätigkeitswechsel des Fahrers oder des zweiten Fahrers und/oder das Einstecken oder die Entnahme einer Kontrollgerätekarte eine Datenausgabe hervor. Wurden Daten bei ausgeschalteter Zündung zurückgehalten, so werden diese Daten sofort nach Einschalten der Zündung bereitgestellt.

20. Kalibrierung

154 Die Kalibrierungsfunktion gestattet folgende Vorgänge:

- automatische Koppelung des Weg- und/oder Geschwindigkeitsgebers mit der Fahrzeugeinheit,
- digitale Angleichung der Konstante des Kontrollgeräts (k) an die Wegdrehzahl des Fahrzeugs (w) (Kraftfahrzeuge mit mehreren Hinterachsuntersetzungen müssen mit einer Umschalteneinrichtung ausgerüstet sein, durch die die verschiedenen Untersetzungsverhältnisse automatisch auf die Wegdrehzahl gebracht werden, für die das Gerät auf das Fahrzeug abgestimmt wurde),
- Einstellung (ohne Beschränkung) der aktuellen Zeit,
- Einstellung des aktuellen Kilometerstands,
- Aktualisierung der im Massenspeicher gespeicherten Kenndaten des Weg- und/oder Geschwindigkeitsgebers,
- Aktualisierung oder Bestätigung anderer dem Kontrollgerät bekannten Parameter: Fahrzeugkennung, Wegdrehzahl (w), Reifenumfang (l), Reifengröße und gegebenenfalls Einstellung des Geschwindigkeitsbegrenzers.

155 Die Kopplung des Weg- und/oder Geschwindigkeitsgebers mit der Fahrzeugeinheit besteht mindestens

- in der Aktualisierung der vom Weg- und/oder Geschwindigkeitsgeber gespeicherten Installationsdaten (nach Bedarf),
- im Kopieren erforderlicher Kenndaten des Weg- und/oder Geschwindigkeitsgebers von diesem in den Massenspeicher der Fahrzeugeinheit.

156 Mit der Kalibrierungsfunktion muss es möglich sein, die erforderlichen Daten über den Anschluss zum Kalibrieren/Herunterladen gemäß dem in Anlage 8 festgelegten Kalibrierungsprotokoll einzugeben. Die Eingabe von Daten durch die Kalibrierungsfunktion kann auch über andere Anschlüsse erfolgen.

21. Zeiteinstellung

157 Die Funktion Zeiteinstellung ermöglicht im Abstand von mindestens 7 Tagen eine Anpassung der aktuellen Uhrzeit um höchstens 1 Minute.

158 In der Betriebsart Kalibrierung ist mit der Funktion Zeiteinstellung eine Anpassung der aktuellen Uhrzeit ohne Einschränkung möglich.

22. Leistungsmerkmale

159 Die Fahrzeugeinheit muss im Temperaturbereich von – 20 °C bis 70 °C, und der Weg- und/oder Geschwindigkeitsgeber im Temperaturbereich von – 40 °C bis 135 °C voll einsatzbereit sein. Der Inhalt des Massenspeichers muss bis zu Temperaturen von – 40 °C erhalten bleiben.

160 Das Kontrollgerät muss bei einer Luftfeuchtigkeit von 10 bis 90 % voll einsatzbereit sein.

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

162 Das Kontrollgerät muss hinsichtlich der elektromagnetischen Verträglichkeit der Richtlinie 95/54/EG der Kommission ⁽¹⁾ zur Anpassung der Richtlinie 72/245/EWG des Rates ⁽²⁾ entsprechen und gegen elektrostatische Entladungen und Störgrößen geschützt sein.

23. Werkstoffe

163 Alle Bauteile des Kontrollgeräts müssen aus Werkstoffen mit hinreichender Stabilität und mechanischer Festigkeit sowie mit elektrischer und magnetischer Stabilität bestehen.

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

165 Die Fahrzeugeinheit muss den Schutzgrad IP 40 und der Weg- und/oder Geschwindigkeitsgeber den Schutzgrad IP 64 gemäß Norm IEC 529 erfüllen.

⁽¹⁾ ABl. L 266 vom 8.11.1995, S. 1.

⁽²⁾ ABl. L 152 vom 6.7.1972, S. 15.

- 166 Das Kontrollgerät muss den geltenden technischen Spezifikationen hinsichtlich der ergonomischen Gestaltung genügen.
- 167 Das Kontrollgerät muss gegen unbeabsichtigte Beschädigungen geschützt sein.

24. Markierungen

- 168 Sind am Kontrollgerät Kilometerstand und Geschwindigkeit ablesbar, müssen in der Anzeige folgende Angaben erscheinen:
- in der Nähe der Zahl, die die zurückgelegte Wegstrecke anzeigt, die Maßeinheit der zurückgelegten Wegstrecken mit der Abkürzung ,km'
 - in der Nähe der Zahl, die die Geschwindigkeit anzeigt, die Abkürzung ,km/h'.
- Kann das Kontrollgerät auch auf eine Geschwindigkeitsanzeige in Meilen pro Stunde umgeschaltet werden; wird in diesem Fall als Maßeinheit der zurückgelegten Wegstrecke die Abkürzung ,mph' angezeigt.
- 169 An jeder gesonderten Komponente des Kontrollgeräts ist ein Typenschild mit folgenden Angaben anzubringen:
- Name und Anschrift des Herstellers,
 - Teilnummer und Baujahr,
 - Seriennummer des Geräts,
 - Prüfzeichen des Kontrollgerätetyps.
- 170 Reicht der Platz für alle genannten Angaben nicht aus, muss das Typenschild mindestens folgende Angaben enthalten: Name oder Logo des Herstellers und Teilnummer des Kontrollgeräts.

IV. BAUART- UND KONSTRUKTIONSMERKMALE DER KONTROLLGERÄTKARTEN

1. Sichtbare Daten

Die Vorderseite enthält:

- 171 je nach Kartentyp die großgedruckten Wörter ,Fahrerkarte' oder ,Kontrollkarte' oder ,Werkstattkarte' oder ,Unternehmenskarte' in der Sprache bzw. den Sprachen des ausstellenden Mitgliedstaats;
- 172 die gleichen Wörter in den anderen Gemeinschaftssprachen, und zwar so gedruckt, dass sie den Hintergrund der Karte bilden:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	KAPTA ΟΔΗΓΟΥ	KAPTA ΕΛΕΓΧΟΥ	KAPTA ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	KAPTA ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OFFICINA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTOLEKAART	WERKPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTTILLA	VALVONTA KORTTILLA	TESTAUSASEMA KORTTILLA	YRITYSKORTTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

- 173 den Namen des Mitgliedstaats, der die Karte ausstellt (fakultativ);

174 das Unterscheidungszeichen des ausstellenden Mitgliedstaats im Negativdruck in einem blauen Rechteck, umgeben von zwölf gelben Sternen:

B	Belgien
DK	Dänemark
D	Deutschland
GR	Griechenland
E	Spanien
F	Frankreich
IRL	Irland
I	Italien
L	Luxemburg
NL	Niederlande
A	Österreich
P	Portugal
FIN	Finnland
S	Schweden
UK	Vereinigtes Königreich

175 wie folgt nummerierte Angaben zu der ausgestellten Karte:

	Fahrerkarte	Kontrollkarte	Unternehmens- oder Werkstattkarte
1.	Name des Fahrers	Name der Kontrollstelle	Name des Unternehmens oder der Werkstatt
2.	Vorname(n)	Name des Kontrolleurs (wenn zutreffend)	Name des Karteninhabers (wenn zutreffend)
3.	Geburtsdatum	Vorname(n) des Kontrolleurs (wenn zutreffend)	Vorname(n) des Karteninhabers (wenn zutreffend)
4.(a)	Gültig ab		
(b)	Gültig bis		
(c)	Ausstellende Behörde (kann auf Seite 2 angegeben werden)		
(d)	eine andere als unter 5. genannte Nummer für Verwaltungszwecke (fakultativ)		
5.(a)	Führerscheinnummer (am Ausstellungstag der Fahrerkarte)		
5.(b)	Kartennummer		
6.	Lichtbild des Fahrers	Lichtbild des Kontrolleurs (fakultativ)	—
7.	Unterschrift des Fahrers	Unterschrift des Inhabers (fakultativ)	
8.	Wohnort oder Anschrift des Inhabers (fakultativ)	Anschrift der Kontrollstelle	Anschrift des Unternehmens oder der Werkstatt

176 Die zu verwendende Datumsform ist ,TT/MM/JJJJ' oder ,TT.MM.JJJJ' (Tag, Monat, Jahr).

Die Rückseite enthält:

177 eine Erläuterung zu den nummerierten Angaben auf der Vorderseite der Karte;

178 gegebenenfalls und mit ausdrücklicher schriftlicher Zustimmung des Inhabers Angaben, die nicht mit der Verwaltung der Fahrerkarte im Zusammenhang stehen; jede Erschwerung der Verwendung des Modells als Fahrerkarte durch derartige Zusätze ist auszuschließen.

GEMEINSCHAFTSMODELL FAHRTENSCHREIBERKARTEN	
VORDERSEITE	RÜCKSEITE
FAHRERKARTE MITGLIEDSTAAT 1.  2.  3.  4a.  4b.  4c.  5a.  5b.  6.  7.  (8.)  (8.) 	1. Name 2. Vorname(n) 3. Geburtsdatum 4a. Gültig ab 4b. Gültig bis 4c. Ausstellende Behörde (4d.) Nr. für nationale Verwaltungszwecke 5a. Führerscheinnummer 5b. Karten-Nr. 6. Lichtbild 7. Unterschrift (8.) Anschrift Bitte zurücksenden an: NAME DER BEHÖRDE UND ANSCHRIFT
KONTROLLKARTE MITGLIEDSTAAT 1.  2.  (2.)  (3.)  4a.  4b.  4c.  4d.  5b.  7.  (8.)  (8.) 	1. Kontrollstelle (2.) Name (3.) Vorname(n) 4a. Gültig ab 4b. Gültig bis 4c. Ausstellende Behörde (4d.) Nr. für nationale Verwaltungszwecke 5b. Kartenummer 6. Lichtbild 7. Unterschrift 8. Anschrift Bitte zurücksenden an: NAME DER BEHÖRDE UND ANSCHRIFT
WERKSTATTKARTE MITGLIEDSTAAT 1.  2.  (2.)  (3.)  4a.  4b.  4c.  4d.  5b.  7.  (8.)  (8.) 	1. Name d. Werkstatt (2.) Name (3.) Vorname(n) 4a. Gültig ab 4b. Gültig bis 4c. Ausstellende Behörde (4d.) Nr. für nationale Verwaltungszwecke 5b. Kartenummer 7. Unterschrift 8. Anschrift Bitte zurücksenden an: NAME DER BEHÖRDE UND ANSCHRIFT
UNTERNEHMENSKARTE MITGLIEDSTAAT 1.  2.  (2.)  (3.)  4a.  4b.  4c.  4d.  5b.  7.  (8.)  (8.) 	1. Name d. Untern. (2.) Name (3.) Vorname(n) 4a. Gültig ab 4b. Gültig bis 4c. Ausstellende Behörde (4d.) Nr. für nationale Verwaltungszwecke 5b. Kartenummer 7. Unterschrift 8. Anschrift Bitte zurücksenden an: NAME DER BEHÖRDE UND ANSCHRIFT

179 Die Kontrollgerätarten werden mit folgender Hintergrundfarbe gedruckt:

- Fahrerkarte: weiß,
- Kontrollkarte: blau,
- Werkstattkarte: rot,
- Unternehmenskarte: gelb.

180 Zum Schutz vor Fälschung und unbefugten Änderungen weisen die Kontrollgerätarten mindestens folgende Merkmale auf:

- ein Sicherheitshintergrunddesign mit feingemustertem Guillochen und Irisdruck,
- im Bereich des Lichtbilds eine Überlappung des Sicherheitshintergrunddesigns mit dem Lichtbild,
- mindestens eine zweifarbige Mikrodruckzeile.

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

2. Sicherheit

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

- 182 Zur Gewährleistung der Systemsicherheit müssen die Kontrollgerätkarten die in den allgemeinen Sicherheitsvorgaben für Kontrollgerätkarten (Anlage 10) festgelegten Anforderungen erfüllen.
- 183 Kontrollgerätkarten müssen mit anderen Geräten, wie z. B. Personalcomputern, lesbar sein.

3. Normen

- 184 Die Kontrollgerätkarten müssen den folgenden Normen entsprechen:
- ISO/IEC 7810 Identifikationskarten — Physikalische Eigenschaften,
 - ISO/IEC 7816 Identifikationskarten — Chipkarten mit Kontakten:
 - Teil 1: Physikalische Eigenschaften,
 - Teil 2: Abmessungen und Lokalisierung der Kontakte,
 - Teil 3: Elektronische Eigenschaften und Protokolle zum Herunterladen,
 - Teil 4: Interindustrielle Kommandos,
 - Teil 8: Interindustrielle sicherheitsbezogene Kommandos,
 - ISO/IEC 10373 Identifikationskarten; Prüfverfahren.

4. Spezifikationen für Umgebung und Elektrizität

- 185 Die Kontrollgerätkarten müssen unter allen klimatischen Bedingungen, die im Gebiet der Gemeinschaft gewöhnlich anzutreffen sind, ordnungsgemäß funktionieren können, mindestens im Temperaturbereich -25 °C bis $+70\text{ °C}$ mit gelegentlichen Spitzen bis zu $+85\text{ °C}$, wobei 'gelegentlich' jeweils nicht mehr als 4 Stunden und nicht mehr als 100mal während der Lebensdauer der Karte bedeutet.
- 186 Die Kontrollgerätkarten müssen bei einer Luftfeuchtigkeit von 10 bis 90 % ordnungsgemäß funktionieren können.
- 187 Die Kontrollgerätkarten müssen bei Verwendung gemäß den Spezifikationen für Umgebung und Elektrizität während einer Dauer von fünf Jahren ordnungsgemäß funktionieren können.
- 188 Während des Betriebs müssen die Kontrollgerätkarten hinsichtlich der elektromagnetischen Verträglichkeit der Richtlinie 95/54/EG entsprechen und gegen elektrostatische Entladungen geschützt sein.

5. Datenspeicherung

Im Sinne dieses Absatzes

- erfolgt die Zeitaufzeichnung auf eine Minute genau, sofern nicht anders angegeben,
- erfolgt die Aufzeichnung des Kilometerstands auf einen Kilometer genau,
- erfolgt die Geschwindigkeitsaufzeichnung auf 1 km/h genau.

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

- 189 In diesem Absatz ist die Mindestspeicherkapazität für die verschiedenen Anwendungsdaten festgelegt. Die Kontrollgerätkarten müssen dem Kontrollgerät die tatsächliche Speicherkapazität dieser Dateien anzeigen können.

Alle zusätzlichen auf Kontrollgerätkarten gespeicherten Daten in Bezug auf andere Anwendungen, für die die Karte sonst noch vorgesehen ist, müssen gemäß der Richtlinie 95/46/EG gespeichert werden.

5.1. **Kenn- und Sicherheitsdaten der Karte**

5.1.1. *Anwendungskennung*

- 190 Die Kontrollgerätkarten müssen die folgenden Anwendungsdaten speichern können:

- Kennnummer der Kontrollgerätanwendung,
- Kontrollgerätkartenartkennung.

5.1.2. *Chipkennung*

- 191 Die Kontrollgerätkarten müssen die folgenden Kenndaten des integrierten Schaltkreises (IS) speichern können:

- IS-Seriennummer,
- IS-Fertigungsangaben.

5.1.3. *IS-Kartenkennung*

- 192 Die Kontrollgerätkarten müssen die folgenden Chipkartenkenndaten speichern können:

- Seriennummer der Karte (einschl. Fertigungsangaben),
- Bauartgenehmigungsnummer der Karte
- Kennung der Karten-Personalisierung (ID),
- Kartenhersteller-ID,
- IS-Bezeichner.

5.1.4. *Sicherheitselemente*

- 193 Die Kontrollgerätkarten müssen die folgenden Sicherheitselementdaten speichern können:

- europäischer öffentlicher Schlüssel,
- Mitgliedstaatzzertifikat,
- Kartenzertifikat,
- privater Schlüssel der Karte.

5.2. **Fahrerkarte**

5.2.1. *Kartenkennung*

- 194 Die Fahrerkarte muss die folgenden Kartenkenndaten speichern können:

- Kartennummer,
- ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum
- gültig ab, gültig bis.

5.2.2. Karteninhabererkennung

195 Die Fahrerkarte muss die folgenden Karteninhaberdaten speichern können:

- Name des Inhabers,
- Vorname(n) des Inhabers,
- Geburtsdatum,
- Muttersprache.

5.2.3. Führerscheininformationen

196 Die Fahrerkarte muss die folgenden Führerscheindaten speichern können:

- ausstellender Mitgliedstaat, Name der ausstellenden Behörde,
- Führerscheinnummer (am Ausstellungstag der Karte).

5.2.4. Daten zu gefahrenen Fahrzeugen

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

- Datum und Uhrzeit des ersten Einsatzes des Fahrzeugs (d. h. erstes Karteneinstecken für diesen Betriebszeitraum des Fahrzeugs oder 0.00 Uhr, wenn der Betriebszeitraum zu diesem Zeitpunkt andauert),
- Kilometerstand zu diesem Zeitpunkt,
- Datum und Uhrzeit des letzten Einsatzes des Fahrzeugs (d. h. letzte Kartenentnahme für diesen Betriebszeitraum des Fahrzeugs oder 23.59 Uhr, wenn der Betriebszeitraum zu jenem Zeitpunkt andauert),
- Kilometerstand zu diesem Zeitpunkt,
- amtliches Kennzeichen und zulassender Mitgliedstaat.

198 Die Fahrerkarte muss mindestens 84 derartige Datensätze speichern können.

5.2.5. Fahrttächtigkeitsdaten

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

- Datum,
- Tagesanwesenheitszähler (wird für jeden dieser Kalendertage um den Wert Eins erhöht),
- die vom Fahrer an diesem Tag zurückgelegte Gesamtwegstrecke,
- den Fahrerstatus um 0.00 Uhr,
- jedes Mal, wenn der Fahrer die Tätigkeit gewechselt und/oder den Status der Fahrzeugführung verändert und/oder seine Karte eingesteckt oder entnommen hat:
 - den Status der Fahrzeugführung (EINMANNBETRIEB, TEAM),
 - den Steckplatz (FAHRER, 2. FAHRER)
 - den Kartenstatus (EINGESTECKT, NICHT EINGESTECKT)
 - die Tätigkeit (LENKEN, BEREITSCHAFT, ARBEIT, UNTERBRECHUNG/RUHE),
 - den Zeitpunkt der Veränderung.

200 Der Speicher der Fahrerkarte muss die Fahrttächtigkeitsdaten mindestens 28 Tage lang gespeichert halten können (die durchschnittliche Tätigkeit eines Fahrers ist mit 93 Tätigkeitsveränderungen pro Tag definiert).

- 201 Die in den Randnummern 197 und 199 aufgeführten Daten werden so gespeichert, dass — auch bei zeitlichen Überschneidungen — ein Abrufen der Tätigkeiten in der Reihenfolge ihres Auftretens möglich ist.

5.2.6. Ort des Beginns und/oder des Endes des Arbeitstages

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

- Datum und Uhrzeit der Eingabe (oder Datum/Uhrzeit bezogen auf die Eingabe, wenn diese während des manuellen Eingabevorgangs erfolgt),
- Art der Eingabe (Beginn oder Ende, Eingabebedingung),
- eingegebene(s) Land und Region,
- Kilometerstand.

- 203 Der Speicher der Fahrerkarte muss mindestens 42 derartige Datensatzpaare gespeichert halten können.

5.2.7. Ereignisdaten

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

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

- Zeitüberlappung (wenn die Karte Ursache des Ereignisses ist),
- Einstecken der Karte während des Lenkens (wenn die Karte Gegenstand des Ereignisses ist),
- Letzter Kartenvorgang nicht korrekt abgeschlossen (wenn die Karte Gegenstand des Ereignisses ist),
- Unterbrechung der Stromversorgung,
- Datenfehler Weg und Geschwindigkeit,
- Versuch Sicherheitsverletzung.

- 205 Die Fahrerkarte muss die folgenden Daten für diese Ereignisse speichern können:

- Ereigniscode,
- Datum und Uhrzeit des Ereignisbeginns (oder der Kartenentnahme, wenn das Ereignis andauerte),
- Datum und Uhrzeit des Ereignisendes (oder der Kartenentnahme, wenn das Ereignis andauerte),
- amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem das Ereignis eintrat.

Anmerkung: Für das Ereignis ‚Zeitüberlappung‘:

- Datum und Uhrzeit des Ereignisbeginns müssen Datum und Uhrzeit der Kartenentnahme aus dem vorherigen Fahrzeug entsprechen,
- Datum und Uhrzeit des Ereignisendes müssen Datum und Uhrzeit des Einsteckens der Karte in das derzeitige Fahrzeug entsprechen,
- Fahrzeugdaten müssen dem derzeitigen Fahrzeug entsprechen, das das Ereignis auslöst.

Anmerkung: Für das Ereignis ‚Letzter Kartenvorgang nicht korrekt abgeschlossen‘:

- Datum und Uhrzeit des Ereignisbeginns müssen Datum und Uhrzeit des Einsteckens der Karte bei dem nicht korrekt abgeschlossenen Vorgang entsprechen,
- Datum und Uhrzeit des Ereignisendes müssen Datum und Uhrzeit des Einsteckens der Karte bei dem Vorgang entsprechen, während dessen das Ereignis festgestellt wurde (derzeitiger Vorgang),
- Fahrzeugdaten müssen dem Fahrzeug entsprechen, in dem der Vorgang nicht korrekt abgeschlossen wurde.

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

5.2.8. *Störungsdaten*

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

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

- Kartenfehler (wenn die Karte Gegenstand der Störung ist),
- Störung Kontrollgerät.

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

- Störungscode,
- Datum und Uhrzeit des Störungsbeginns (oder der Kartenentnahme, wenn die Störung andauerte),
- Datum und Uhrzeit des Störungsendes (oder der Kartenentnahme, wenn die Störung andauerte),
- amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Störung eintrat.

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

5.2.9. *Kontrollaktivitätsdaten*

210 Die Fahrerkarte muss in Bezug auf Kontrollaktivitäten die folgenden Daten speichern können:

- Datum und Uhrzeit der Kontrolle,
- Kontrollkartennummer und ausstellender Mitgliedstaat,
- Art der Kontrolle (Anzeige, Drucken, Herunterladen von der Fahrzeugeinheit, Herunterladen von der Karte (siehe Anmerkung)),
- Heruntergeladener Zeitraum beim Herunterladen,
- amtliches Kennzeichen und zulassender Mitgliedstaat des kontrollierten Fahrzeugs.

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

211 Die Fahrerkarte muss einen derartigen Datensatz gespeichert halten können.

5.2.10. *Kartenvorgangsdaten*

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

- Datum und Uhrzeit der Einleitung des Vorgangs (d. h. Einstecken der Karte) auf 1 Sekunde genau,
- amtliches Kennzeichen und zulassender Mitgliedstaat.

5.2.11. *Daten zu spezifischen Bedingungen*

212a Die Fahrerkarte muss die folgenden Daten in Bezug auf spezifische Bedingungen speichern können, die bei eingesetzter Karte (ungeachtet des Steckplatzes) eingegeben wurden:

- Datum und Uhrzeit der Eingabe,
- Art der spezifischen Bedingung.

212b Die Fahrerkarte muss 56 derartige Datensätze gespeichert halten können.

5.3. Werkstattkarte

5.3.1. Sicherheitselemente

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

214 Die Werkstattkarte muss die kryptografischen Schlüssel speichern können, die für die Koppelung der Weg- und/oder Geschwindigkeitsgeber mit den Kontrollgeräten erforderlich sind.

5.3.2. Kartenkennung

215 Die Werkstattkarte muss die folgenden Kartenkenndaten speichern können:

- Kartennummer,
- ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum
- gültig ab, gültig bis.

5.3.3. Karteninhaberkennung

216 Die Fahrerkarte muss die folgenden Karteninhaberkenndaten speichern können:

- Name der Werkstatt
- Anschrift der Werkstatt
- Name des Inhabers,
- Vorname(n) des Inhabers,
- Muttersprache.

5.3.4. Daten zu gefahrenen Fahrzeugen

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

218 Die Werkstattkarte muss mindestens 4 derartige Datensätze speichern können.

5.3.5. Fahrertätigkeitsdaten

219 Die Werkstattkarte muss Fahrertätigkeitsdaten so speichern können wie eine Fahrerkarte.

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

5.3.6. Daten zum Beginn/Ende des Arbeitstages

221 Die Werkstattkarte muss Datensätze zum Beginn/Ende des Arbeitstages so speichern können wie eine Fahrerkarte.

222 Die Werkstattkarte muss mindestens 3 derartige Datensatzpaare gespeichert halten können.

5.3.7. Ereignis- und Störungsdaten

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

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

5.3.8. Kontrollaktivitätsdaten

225 Die Werkstattkarte muss einen Kontrollaktivitätsdatensatz so speichern können wie eine Fahrerkarte.

5.3.9. Kalibrierungs- und Zeiteinstellungsdaten

- 226 Die Werkstattkarte muss Datensätze zu Kalibrierungen und/oder Zeiteinstellungen gespeichert halten können, die ausgeführt werden, während die Karte in ein Kontrollgerät eingesetzt ist.
- 227 In jedem Kalibrierungsdatensatz müssen folgende Daten enthalten sein:
- Zweck der Kalibrierung (Ersteinbau, Einbau, regelmäßige Nachprüfung),
 - Fahrzeugkennung,
 - aktualisierte oder bestätigte Parameter (Wegdrehzahl, Kontrollgerätkonstante, tatsächlicher Reifenumfang, Reifengröße, Einstellung des Geschwindigkeitsbegrenzers, Kilometerstand (alt und neu), Datum und Uhrzeit (alte und neue Werte),
 - Kontrollgerätkenntung (FE-Teilnummer, FE-Seriennummer, Seriennummer des Weg- und/oder Geschwindigkeitsgebers).
- 228 Die Werkstattkarte muss mindestens 88 derartige Datensätze speichern können.
- 229 Die Werkstattkarte führt einen Zähler, der die Gesamtzahl der mit der Karte ausgeführten Kalibrierungen angibt.
- 230 Die Werkstattkarte führt einen Zähler, der die Anzahl der seit dem letzten Herunterladen durchgeführten Kalibrierungen angibt.

5.3.10. Daten zu spezifischen Bedingungen

- 230a Die Werkstattkarte muss Daten in Bezug auf spezifische Bedingungen so wie die Fahrerkarte speichern können. Die Werkstattkarte muss 2 derartige Datensätze speichern können.

5.4. Kontrollkarte

5.4.1. Kartenkennung

- 231 Die Kontrollkarte muss die folgenden Kartenkenndaten speichern können:
- Kartennummer,
 - ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum
 - gültig ab, gültig bis (sofern zutreffend).

5.4.2. Karteninhaberkennung

- 232 Die Kontrollkarte muss die folgenden Karteninhaberkennndaten speichern können:
- Name der Kontrollstelle,
 - Anschrift der Kontrollstelle,
 - Name des Inhabers,
 - Vorname(n) des Inhabers,
 - Muttersprache.

5.4.3. Kontrollaktivitätsdaten

- 233 Die Kontrollkarte muss die folgenden Daten in Bezug auf Kontrollaktivitäten speichern können:
- Datum und Uhrzeit der Kontrolle,
 - Art der Kontrolle (Anzeige, Drucken, Herunterladen von der Fahrzeugeinheit, Herunterladen von der Karte),

- heruntergeladenerer Zeitraum (sofern zutreffend),
- amtliches Kennzeichen und zulassender Mitgliedstaat des kontrollierten Fahrzeugs,
- Kartenummer und ausstellender Mitgliedstaat der kontrollierten Fahrerkarte.

234 Die Kontrollkarte muss mindestens 230 derartige Datensätze gespeichert halten können.

5.5. **Unternehmenskarte**

5.5.1. *Kartenkennung*

235 Die Unternehmenskarte muss die folgenden Kartenkenndaten speichern können:

- Kartenummer,
- ausstellender Mitgliedstaat, Name der ausstellenden Behörde, Ausstellungsdatum
- gültig ab, gültig bis (wenn zutreffend).

5.5.2. *Karteninhabererkennung*

236 Die Unternehmenskarte muss die folgenden Karteninhaberkenndaten speichern können:

- Name des Unternehmens,
- Anschrift des Unternehmens.

5.5.3. *Unternehmensaktivitätsdaten*

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

- Datum und Uhrzeit der Aktivität,
- Art der Aktivität (Sperrungen/Entsperrungen der Fahrzeugeinheit, Herunterladen von der Fahrzeugeinheit, Herunterladen von der Karte),
- heruntergeladenerer Zeitraum (wenn zutreffend),
- amtliches Kennzeichen und Zulassungsbehörde des Mitgliedstaates des Fahrzeugs,
- Kartenummer und ausstellender Mitgliedstaat (beim Herunterladen von der Karte).

238 Die Unternehmenskarte muss mindestens 230 derartige Datensätze gespeichert halten können.

V. EINBAU DES KONTROLLGERÄTS

1. **Einbau**

239 Neue Kontrollgeräte werden in nichtaktiviertem Zustand an Installateure oder Fahrzeughersteller geliefert, wobei alle in Kapitel III.20 aufgeführten Kalibrierungsparameter auf geeignete und gültige Standardwerte eingestellt sind. Liegt kein bestimmter Wert vor, sind Buchstaben-Parameter auf Strings mit „?“ und numerische Parameter auf „0“ zu setzen.

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

241 Vor seiner Aktivierung darf das Kontrollgerät die in III.12.3 bis III.12.9 sowie III.12.12 bis III.12.14 genannten Daten weder aufzeichnen noch speichern.

242 Während des Einbaus werden alle bekannten Parameter vom Fahrzeughersteller voreingestellt.

- 243 Der Fahrzeughersteller oder Installateur aktiviert das eingebaute Kontrollgerät, bevor das Fahrzeug den Einbaustandort verlässt.
- 244 Die Aktivierung des Kontrollgeräts wird durch das erstmalige Einstecken einer Werkstattkarte in eine der beiden Kartenschnittstellen automatisch ausgelöst.
- 245 Gegebenenfalls erforderliche spezifische Koppelungsoperationen zwischen dem Weg- und/oder Geschwindigkeitsgeber und der Fahrzeugeinheit müssen automatisch vor oder während der Aktivierung stattfinden.
- 246 Nach seiner Aktivierung sorgt das Kontrollgerät für die vollständige Anwendung aller Funktionen und Datenzugriffsrechte.
- 247 Die Aufzeichnungs- und Speicherfunktion des Kontrollgeräts muss nach seiner Aktivierung voll wirksam sein.
- 248 Nach dem Einbau erfolgt eine Kalibrierung. Bei der Erstkalibrierung, die innerhalb von 2 Wochen nach dem Einbau oder nach der Zuteilung des amtlichen Kennzeichens erfolgt, je nachdem, welches Ereignis zuletzt eintritt, wird das amtliche Kennzeichen eingegeben.
- 248a Das Kontrollgerät ist im Fahrzeug so anzubringen, dass für den Fahrer alle notwendigen Funktionen vom Fahrersitz aus zugänglich sind.

2. Einbauschild

- 249 Nach der Einbauprüfung beim Ersteinbau wird am oder im Kontrollgerät selbst oder neben dem Gerät gut sichtbar ein Einbauschild angebracht. Nach jedem Eingriff eines zugelassenen Installateurs oder einer zugelassenen Werkstatt ist das Einbauschild durch ein neues Schild zu ersetzen.
- 250 Das Einbauschild muss mindestens die nachstehenden Angaben enthalten:
- Name, Anschrift oder Firmenzeichen des zugelassenen Installateurs oder der zugelassenen Werkstatt,
 - Wegdrehzahl des Kraftfahrzeugs in der Form ‚w = ... Imp/km‘,
 - Konstante des Kontrollgeräts in der Form ‚k = ... Imp/km‘,
 - tatsächlicher Reifenumfang in der Form ‚l = ... mm‘,
 - Reifengröße,
 - Datum der Bestimmung der Wegdrehzahl des Kraftfahrzeugs und der Messung des tatsächlichen Reifenumfangs,
 - Fahrzeugidentifizierungsnummer.

3. Plombierung

- 251 Folgende Geräteteile müssen plombiert werden:
- jeder Anschluss, sofern es bei einer Trennung der Verbindung zu nicht nachweisbaren Änderungen oder nicht feststellbaren Datenverlusten kommen würde;
 - das Einbauschild, es sei denn, es ist so angebracht, dass es sich nicht ohne Vernichtung der Angaben entfernen lässt.
- 252 Die genannten Plombierungen dürfen entfernt werden:
- in Notfällen,
 - um einen Geschwindigkeitsbegrenzer oder ein anderes der Sicherheit im Straßenverkehr dienendes Gerät einzubauen, zu justieren oder zu reparieren, sofern das Kontrollgerät auch dann noch zuverlässig und ordnungsgemäß arbeitet und von einem zugelassenen Installateur oder einer zugelassenen Werkstatt (gemäß Kapitel VI) unmittelbar nach dem Einbau des Geschwindigkeitsbegrenzers bzw. eines anderen der Sicherheit im Straßenverkehr dienenden Gerätes oder andernfalls spätestens nach sieben Tagen wieder plombiert wird.

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

VI. EINBAUPRÜFUNGEN, NACHPRÜFUNGEN UND REPARATUREN

Die in Artikel 12 Absatz 5 der Verordnung (EWG) Nr. 3821/85, zuletzt geändert durch die Verordnung (EG) Nr. 2135/98, genannten Umstände, unter denen die Versiegelungen entfernt werden dürfen, sind in Kapitel V.3 dieses Anhangs festgelegt.

1. Zulassung der Installateure oder Werkstätten

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

- den Einbau,
- Einbauprüfungen,
- Nachprüfungen und
- Reparaturen

vornehmen.

Im Rahmen von Artikel 12 Absatz 1 der Verordnung werden Werkstattkarten, sofern keine entsprechende Begründung erfolgt, nur an für die Aktivierung und/oder Kalibrierung des Kontrollgeräts gemäß diesem Anhang zugelassene Installateure und/oder Werkstätten ausgegeben,

- die keinen Anspruch auf eine Unternehmenskarte haben;
- und deren sonstige unternehmerische Tätigkeit keine potentielle Gefährdung der Gesamtsicherheit des Systems gemäß Anlage 10 darstellt.

2. Prüfung neuer oder reparierter Geräte

- 254 Für jedes neue oder reparierte Einzelgerät werden die ordnungsgemäße Arbeitsweise und die Genauigkeit der Anzeigen und Aufzeichnungen innerhalb der in Kapitel III.2.1 und III.2.2 festgelegten Grenzen durch die in Kapitel V.3 vorgesehene Plombierung sowie durch Kalibrierung geprüft.

3. Einbauprüfung

- 255 Beim Einbau in ein Fahrzeug muss die Gesamtanlage (einschließlich des Kontrollgeräts) den Vorschriften über die in Kapitel III.2.1 und III.2.2 festgelegten zulässigen Fehlergrenzen entsprechen.

4. Regelmäßige Nachprüfungen

- 256 Regelmäßige Nachprüfungen der im Kraftfahrzeug eingebauten Ausrüstung erfolgen nach jeder Reparatur der Ausrüstung, jeder Änderung der Wegdrehzahl oder des tatsächlichen Reifenumfangs, wenn die UTC-Zeit von der korrekten Zeit um mehr als 20 Minuten abweicht oder wenn sich das amtliche Kennzeichen geändert hat, und mindestens einmal innerhalb von zwei Jahren (24 Monaten) seit der letzten Überprüfung.

- 257 Überprüft werden zumindest:

- die ordnungsgemäße Arbeitsweise des Kontrollgeräts, einschließlich der Funktion Datenspeicherung auf Kontrollgerätkarten,
- die Einhaltung der Bestimmungen von Kapitel III.2.1 und III.2.2 über die zulässigen Fehlergrenzen des Geräts in eingebautem Zustand,
- das Vorhandensein des Prüfzeichens auf dem Kontrollgerät,
- das Vorhandensein des Einbauschilds,
- die Unversehrtheit der Plombierung des Geräts und der anderen Einbauteile,
- die Reifengröße und der tatsächliche Reifenumfang.

258 Bestandteil dieser Überprüfungen muss eine Kalibrierung sein.

5. Messung der Anzeigefehler

259 Die Messung der Anzeigefehler beim Einbau und während der Benutzung wird unter folgenden Bedingungen durchgeführt, die als normale Prüfbedingungen anzusehen sind:

- unbeladenes Fahrzeug in fahrbereitem Zustand,
- Reifendrücke gemäß den Angaben des Herstellers,
- Reifenabnutzung innerhalb der nach den einzelstaatlichen Rechtsvorschriften zulässigen Grenzen,
- Bewegungen des Fahrzeugs:
 - Das Fahrzeug muss sich mit eigener Motorkraft geradlinig auf ebenem Gelände und mit einer Geschwindigkeit von 50 ± 5 km/h fortbewegen. Die Messstrecke muss mindestens 1 000 m betragen.
- die Prüfung kann auch mit anderen Methoden, so auf einem geeigneten Prüfstand, durchgeführt werden, sofern eine vergleichbare Genauigkeit gewährleistet ist.

6. Reparaturen

260 Die Werkstätten müssen Daten vom Kontrollgerät herunterladen können, um die Daten dem entsprechenden Transportunternehmen zu übergeben.

261 Die zugelassenen Werkstätten stellen den Transportunternehmen eine Bescheinigung über die Unmöglichkeit des Herunterladens der Daten aus, wenn das Herunterladen von aufgezeichneten Daten aufgrund eines Defekts des Kontrollgeräts auch nach der Reparatur durch diese Werkstätten nicht möglich ist. Eine Kopie jeder ausgestellten Bescheinigung ist von den Werkstätten mindestens ein Jahr lang aufzubewahren.

VII. KARTENAUSGABE

Die von den Mitgliedstaaten eingerichteten Kartenausgabeverfahren müssen folgenden Vorschriften entsprechen:

- 262 Die Kartenummer der Erstaussgabe einer Kontrollgerätkarte an einen Antragsteller hat einen fortlaufenden Index (wenn zutreffend) sowie einen Ersatzindex und einen auf ,0' gesetzten Erneuerungsindex.
- 263 Die Kartenummern aller an dieselbe Kontrollstelle oder dieselbe Werkstatt oder dasselbe Transportunternehmen ausgegebenen nicht personengebundenen Kontrollgerätkarten weisen die gleichen ersten 13 Stellen sowie einen unterschiedlichen laufenden Index auf.
- 264 Eine als Ersatz einer vorhandenen Kontrollgerätkarte ausgegebene Kontrollgerätkarte weist die gleiche Kartenummer auf wie die ersetzte Karte, wobei jedoch der Ersatzindex um ,1' (in der Reihenfolge 0, ..., 9, A, ..., Z) erhöht ist.
- 265 Eine als Ersatz für eine vorhandene Kontrollgerätkarte ausgegebene Karte weist das gleiche Datum für den Ablauf der Gültigkeit auf wie die ersetzte Karte.
- 266 Eine zur Erneuerung einer vorhandenen Kontrollgerätkarte ausgegebene Karte trägt die gleiche Kartenummer wie die erneuerte Karte, wobei jedoch der Ersatzindex auf ,0' zurückgesetzt und der Erneuerungsindex um ,1' erhöht ist (in der Reihenfolge 0, ..., 9, A, ..., Z).
- 267 Der Austausch einer vorhandenen Kontrollgerätkarte zwecks Änderung von Verwaltungsdaten richtet sich bei Erneuerung innerhalb desselben Mitgliedstaates nach den Vorschriften für die Erneuerung und bei Ausführung durch einen anderen Mitgliedstaat nach den Vorschriften für die Erstaussgabe.
- 268 Bei nicht personengebundenen Werkstatt- oder Kontrollkarten wird in der Rubrik ,Name des Inhabers' der Name der Werkstatt bzw. der Kontrollstelle eingetragen.

VIII. BAUARTGENEHMIGUNG VON KONTROLLGERÄTEN UND KONTROLLGERÄTKARTEN

1. Allgemeines

Im Sinne dieses Kapitels ist unter dem Ausdruck ,Kontrollgerät' das ,Kontrollgerät oder seine Komponenten' zu verstehen. Für das/die Verbindungskabel zwischen Weg- und/oder Geschwindigkeitsgeber und Fahrzeugeinheit ist keine Bauartgenehmigung erforderlich. Das zur Verwendung durch das Kontrollgerät bestimmte Papier ist als Komponente des Kontrollgeräts zu betrachten.

- 269 Kontrollgeräte sind zusammen mit allen integrierten Zusatzgeräten zur Bauartgenehmigung vorzulegen.
- 270 Die Bauartgenehmigung von Kontrollgeräten und Kontrollgerätkarten beinhaltet Sicherheitsprüfungen, Funktionsprüfungen und Interoperabilitätsprüfungen. Die positiven Ergebnisse der einzelnen Prüfungen werden in einem geeigneten Zertifikat ausgewiesen.
- 271 Die Behörden der Mitgliedstaaten erteilen nur dann eine Bauartgenehmigung gemäß Artikel 5 dieser Verordnung, wenn ihnen
- ein Sicherheitszertifikat,
 - ein Funktionszertifikat und
 - ein Interoperabilitätszertifikat
- für das Kontrollgerät oder die Kontrollgerätkarte, für die die Bauartgenehmigung beantragt wurde, vorliegt.
- 272 Änderungen an der Software oder Hardware des Geräts oder an den für seine Herstellung verwendeten Werkstoffen sind vor ihrer Umsetzung der Behörde zu melden, die die Bauartgenehmigung für das Gerät erteilt hat. Diese Behörde bestätigt dem Hersteller die Erweiterung der Bauartgenehmigung oder verlangt eine Aktualisierung oder Bestätigung des entsprechenden Funktions-, Sicherheits- und/oder Interoperabilitätszertifikats.
- 273 Verfahren zur Versionsaufrüstung der Software bereits eingebauter Kontrollgeräte sind von der Behörde zu genehmigen, die die Bauartgenehmigung für das Kontrollgerät erteilt hat. Durch die Softwareaufrüstung dürfen im Kontrollgerät gespeicherte Fahrtfähigkeitsdaten nicht verändert oder gelöscht werden. Die Softwareaufrüstung darf nur unter der Verantwortung des Geräteherstellers erfolgen.

2. Sicherheitszertifikat

- 274 Das Sicherheitszertifikat wird gemäß den Bestimmungen von Anlage 10 dieses Anhangs erteilt.

3. Funktionszertifikat

- 275 Jeder Antragsteller einer Bauartgenehmigung legt der Bauartgenehmigungsbehörde des Mitgliedstaats sämtliche Materialien und Unterlagen vor, die die Behörde für notwendig erachtet.
- 276 Ein Funktionszertifikat ist dem Hersteller erst dann zu erteilen, nachdem mindestens alle in Anlage 9 spezifizierten Prüfungen erfolgreich bestanden wurden.
- 277 Das Funktionszertifikat wird von der Bauartgenehmigungsbehörde erteilt. Auf diesem Zertifikat ist neben dem Namen des Empfängers und der Modellkennung eine ausführliche Liste der durchgeführten Prüfungen und der erzielten Ergebnisse anzuführen.

4. Interoperabilitätszertifikat

- 278 Interoperabilitätsprüfungen werden von einer einzigen Prüfstelle durchgeführt, die der Europäischen Kommission untersteht und sich in ihrer Verantwortung befindet.
- 279 Die Prüfstelle registriert von den Herstellern gestellte Anträge auf Interoperabilitätsprüfungen in der Reihenfolge ihres Eintreffens.
- 280 Anträge werden nur dann amtlich registriert, wenn der Prüfstelle folgende Unterlagen vorliegen:
- sämtliche Materialien und Dokumente, die für diese Interoperabilitätsprüfungen erforderlich sind,
 - das entsprechende Sicherheitszertifikat,
 - das entsprechende Funktionszertifikat.

Das Registrierungsdatum des Antrags wird dem Hersteller mitgeteilt.

- 281 Für ein Kontrollgerät oder eine Kontrollgerätkarte, für die kein Sicherheitszertifikat und kein Funktionszertifikat erteilt wurden, werden keine Interoperabilitätsprüfungen durchgeführt.
- 282 Jeder Hersteller, der Interoperabilitätsprüfungen beantragt, verpflichtet sich, der damit beauftragten Prüfstelle sämtliche Materialien und Dokumente zu überlassen, die er für die Durchführung der Prüfungen bereitgestellt hat.

- 283 Die Interoperabilitätsprüfungen werden gemäß den Bestimmungen von Anlage 9 Absatz 5 dieses Anhangs für jeweils alle Modelle von Kontrollgeräten oder Kontrollgerätkarten durchgeführt,
- deren Bauartgenehmigung noch gültig ist oder
 - für die eine Bauartgenehmigung beantragt wurde und die ein gültiges Interoperabilitätszertifikat besitzen.
- 284 Das Interoperabilitätszertifikat wird dem Hersteller von der Prüfstelle erst erteilt, nachdem alle erforderlichen Interoperabilitätsprüfungen erfolgreich bestanden wurden.
- 285 Sind die Interoperabilitätsprüfungen bei einem oder mehreren Kontrollgeräten oder bei einer oder mehreren Kontrollgerätkarten entsprechend Randnummer 283 nicht erfolgreich, wird das Interoperabilitätszertifikat erst dann erteilt, wenn der antragstellende Hersteller die erforderlichen Änderungen vorgenommen und die Interoperabilitätsprüfungen bestanden hat. Die Prüfstelle stellt mit Hilfe des von diesem Interoperabilitätsfehler betroffenen Herstellers die Ursache des Problems fest und bemüht sich, den antragstellenden Hersteller bei der Suche nach einer technischen Lösung zu unterstützen. Hat der Hersteller sein Produkt verändert, muss er sich bei den zuständigen Behörden vergewissern, dass das Sicherheitszertifikat und die Funktionszertifikate noch gültig sind.
- 286 Das Interoperabilitätszertifikat ist sechs Monate gültig. Hat der Hersteller bei Ablauf dieser Frist keine entsprechende Bauartgenehmigung erhalten, wird es ihm wieder entzogen. Das Interoperabilitätszertifikat wird vom Hersteller an die Bauartgenehmigungsbehörde des Mitgliedstaats weitergeleitet, die das Funktionszertifikat erteilt hat.
- 287 Ein Element, das möglicherweise einem Interoperabilitätsfehler zugrunde liegt, darf nicht gewinnbringend oder zur Errichtung einer beherrschenden Stellung verwendet werden.

5. Bauartgenehmigungsbogen

- 288 Die Bauartgenehmigungsbehörde des Mitgliedstaates darf die Bauartgenehmigung erteilen, sobald ihr die drei benötigten Zertifikate vorliegen.
- 289 Bei der Erteilung der Bauartgenehmigung an den Hersteller fertigt die Bauartgenehmigungsbehörde eine Kopie des Bauartgenehmigungsbogens für die mit den Interoperabilitätsprüfungen betraute Prüfstelle an.
- 290 Die für Interoperabilitätsprüfungen zuständige Prüfstelle unterhält eine öffentliche Website mit einer aktuellen Liste der Modelle von Kontrollgeräten und Kontrollgerätkarten,
- für die ein Antrag auf Interoperabilitätsprüfungen registriert wurde,
 - für die ein Interoperabilitätszertifikat (auch ein vorläufiges Interoperabilitätszertifikat) erteilt wurde,
 - für die eine Bauartgenehmigung erteilt wurde.

6. Ausnahmeverfahren für die ersten Interoperabilitätszertifikate

- 291 Innerhalb von vier Monaten, nachdem ein erster Satz von Kontrollgerät und Kontrollgerätkarten (Fahrer-, Werkstatt-, Kontroll- und Unternehmenskarte) als interoperabel zertifiziert wurden, gilt jedes Interoperabilitätszertifikat (auch dieses erste), das in diesem Zeitraum auf entsprechenden Antrag ausgestellt wird, als vorläufig.
- 292 Sind am Ende dieses Zeitraums sämtliche betreffenden Produkte interoperabel, erhalten sämtliche entsprechenden Interoperabilitätszertifikate endgültigen Charakter.
- 293 Werden in diesem Zeitraum Interoperabilitätsfehler festgestellt, ermittelt die mit den Interoperabilitätsprüfungen betraute Prüfstelle die Ursachen der Probleme mit Hilfe aller beteiligten Hersteller und fordert diese auf, die erforderlichen Änderungen vorzunehmen.
- 294 Liegen am Ende dieses Zeitraums weiterhin Interoperabilitätsprobleme vor, ermittelt die mit den Interoperabilitätsprüfungen betraute Prüfstelle in Zusammenarbeit mit den betreffenden Herstellern und mit den Bauartgenehmigungsbehörden, die die entsprechenden Funktionszertifikate erteilt haben, die Ursachen der Interoperabilitätsfehler und gibt an, welche Änderungen von den einzelnen betroffenen Herstellern vorzunehmen sind. Die Suche nach technischen Lösungen dauert maximal zwei Monate; ist nach Ablauf dieses Zeitraums keine gemeinsame Lösung gefunden worden, entscheidet die Kommission nach Rücksprache mit der mit den Interoperabilitätsprüfungen betrauten Prüfstelle unter Angabe von Gründen, welchen Geräte und Karten ein endgültiges Interoperabilitätszertifikat erteilt wird.
- 295 Anträge auf Interoperabilitätsprüfungen, die von der Prüfstelle zwischen dem Ende der Viermonatsfrist nach Erteilung des ersten vorläufigen Interoperabilitätszertifikats und dem Datum der in Randnummer 294 genannten Entscheidung der Kommission registriert werden, sind bis zur Lösung der ursprünglichen Interoperabilitätsprobleme zurückzustellen. Anschließend werden diese Anträge in der Reihenfolge ihrer Registrierung bearbeitet.
-

Anlage 1

DATENGLOSSAR

INHALTSVERZEICHNIS

1.	Einführung	54
1.1.	Grundlage für die Definition von Datentypen	54
1.2.	Referenzdokumente	54
2.	Datentypdefinitionen	55
2.1.	ActivityChangeInfo	55
2.2.	Address	56
2.3.	BCDString	56
2.4.	CalibrationPurpose	56
2.5.	CardActivityDailyRecord	57
2.6.	CardActivityLengthRange	57
2.7.	CardApprovalNumber	57
2.8.	CardCertificate	57
2.9.	CardChipIdentification	57
2.10.	CardConsecutiveIndex	58
2.11.	CardControlActivityDataRecord	58
2.12.	CardCurrentUse	58
2.13.	CardDriverActivity	58
2.14.	CardDrivingLicenceInformation	59
2.15.	CardEventData	59
2.16.	CardEventRecord	59
2.17.	CardFaultData	60
2.18.	CardFaultRecord	60
2.19.	CardIccIdentification	60
2.20.	CardIdentification	61
2.21.	CardNumber	61
2.22.	CardPlaceDailyWorkPeriod	61
2.23.	CardPrivateKey	62
2.24.	CardPublicKey	62
2.25.	CardRenewalIndex	62
2.26.	CardReplacementIndex	62
2.27.	CardSlotNumber	62
2.28.	CardSlotsStatus	62
2.29.	CardStructureVersion	63

2.30.	CardVehicleRecord	63
2.31.	CardVehiclesUsed	63
2.32.	Certificate	64
2.33.	CertificateContent	64
2.34.	CertificateHolderAuthorisation	64
2.35.	CertificateRequestID	65
2.36.	CertificationAuthorityKID	65
2.37.	CompanyActivityData	65
2.38.	CompanyActivityType	66
2.39.	CompanyCardApplicationIdentification	66
2.40.	CompanyCardHolderIdentification	66
2.41.	ControlCardApplicationIdentification	67
2.42.	ControlCardControlActivityData	67
2.43.	ControlCardHolderIdentification	67
2.44.	ControlType	68
2.45.	CurrentDateTime	68
2.46.	DailyPresenceCounter	68
2.47.	Datef	69
2.48.	Distance	69
2.49.	DriverCardApplicationIdentification	69
2.50.	DriverCardHolderIdentification	69
2.51.	EntryTypeDailyWorkPeriod	70
2.52.	EquipmentType	70
2.53.	EuropeanPublicKey	70
2.54.	EventFaultType	70
2.55.	EventFaultRecordPurpose	71
2.56.	ExtendedSerialNumber	72
2.57.	FullCardNumber	72
2.58.	HighResOdometer	72
2.59.	HighResTripDistance	72
2.60.	HolderName	72
2.61.	K-ConstantOfRecordingEquipment	73
2.62.	KeyIdentifier	73
2.63.	L-TyreCircumference	73
2.64.	Language	73
2.65.	LastCardDownload	73
2.66.	ManualInputFlag	73
2.67.	ManufacturerCode	74

2.68.	MemberStateCertificate	74
2.69.	MemberStatePublicKey	75
2.70.	Name	75
2.71.	NationAlpha	75
2.72.	NationNumeric	76
2.73.	NoOfCalibrationRecords	77
2.74.	NoOfCalibrationSinceDownload	77
2.75.	NoOfCardPlaceRecords	77
2.76.	NoOfCardVehicleRecords	77
2.77.	NoOfCompanyActivityRecords	77
2.78.	NoOfControlActivityRecords	78
2.79.	NoOfEventsPerType	78
2.80.	NoOfFaultsPerType	78
2.81.	OdometerValueMidnight	78
2.82.	OdometerShort	78
2.83.	OverspeedNumber	78
2.84.	PlaceRecord	78
2.85.	PreviousVehicleInfo	79
2.86.	PublicKey	79
2.87.	RegionAlpha	79
2.88.	RegionNumeric	79
2.89.	RSAPublicModulus	80
2.90.	RSAPrivateExponent	80
2.91.	RSAPublicExponent	80
2.92.	SensorApprovalNumber	80
2.93.	SensorIdentification	80
2.94.	SensorInstallation	81
2.95.	SensorInstallationSecData	81
2.96.	SensorOSIdentifier	81
2.97.	SensorPaired	81
2.98.	SensorPairingDate	82
2.99.	SensorSerialNumber	82
2.100.	SensorSCIdentifier	82
2.101.	Signature	82
2.102.	SimilarEventsNumber	82
2.103.	SpecificConditionType	82
2.104.	SpecificConditionRecord	82
2.105.	Speed	83

2.106.	SpeedAuthorised	83
2.107.	SpeedAverage	83
2.108.	SpeedMax	83
2.109.	TDesSessionKey	83
2.110.	TimeReal	83
2.111.	TyreSize	83
2.112.	VehicleIdentificationNumber	84
2.113.	VehicleRegistrationIdentification	84
2.114.	VehicleRegistrationNumber	84
2.115.	VuActivityDailyData	84
2.116.	VuApprovalNumber	84
2.117.	VuCalibrationData	84
2.118.	VuCalibrationRecord	85
2.119.	VuCardIWDData	85
2.120.	VuCardIWRecord	86
2.121.	VuCertificate	86
2.122.	VuCompanyLocksData	86
2.123.	VuCompanyLocksRecord	87
2.124.	VuControlActivityData	87
2.125.	VuControlActivityRecord	87
2.126.	VuDataBlockCounter	87
2.127.	VuDetailedSpeedBlock	87
2.128.	VuDetailedSpeedData	88
2.129.	VuDownloadablePeriod	88
2.130.	VuDownloadActivityData	88
2.131.	VuEventData	88
2.132.	VuEventRecord	89
2.133.	VuFaultData	89
2.134.	VuFaultRecord	89
2.135.	VuIdentification	90
2.136.	VuManufacturerAddress	90
2.137.	VuManufacturerName	90
2.138.	VuManufacturingDate	90
2.139.	VuOverSpeedingControlData	91
2.140.	VuOverSpeedingEventData	91
2.141.	VuOverSpeedingEventRecord	91
2.142.	VuPartNumber	91
2.143.	VuPlaceDailyWorkPeriodData	92

2.144.	VuPlaceDailyWorkPeriodRecord	92
2.145.	VuPrivateKey	92
2.146.	VuPublicKey	92
2.147.	VuSerialNumber	92
2.148.	VuSoftInstallationDate	92
2.149.	VuSoftwareIdentification	92
2.150.	VuSoftwareVersion	93
2.151.	VuSpecificConditionData	93
2.152.	VuTimeAdjustmentData	93
2.153.	VuTimeAdjustmentRecord	93
2.154.	W-VehicleCharacteristicConstant	93
2.155.	WorkshopCardApplicationIdentification	94
2.156.	WorkshopCardCalibrationData	94
2.157.	WorkshopCardCalibrationRecord	94
2.158.	WorkshopCardHolderIdentification	95
2.159.	WorkshopCardPIN	95
3.	Definitionen für Wert- und Größenbereiche	96
3.1.	Definitionen für die Fahrerkarte	96
3.2.	Definitionen für die Werkstattkarte	96
3.3.	Definitionen für die Kontrollkarte	96
3.4.	Definitionen für die Unternehmenskarte	96
4.	Zeichensätze	96
5.	Kodierung	96

1. EINFÜHRUNG

Diese Anlage enthält die Spezifizierung der zur Verwendung im Kontrollgerät und auf den Kontrollgerätkarten vorgesehenen Datenformate, -elemente und -strukturen.

1.1. Grundlage für die Definition von Datentypen

Die Definition der Datentypen in dieser Anlage beruht auf der Notation Eins für abstrakte Syntax (ASN.1), da es auf diese Weise möglich ist, einfache und strukturierte Daten ohne Implizierung einer spezifischen, anwendungs- und umgebungsabhängigen Transfersyntax (Kodierungsregeln) festzulegen.

Die ASN.1-Typbenennungskonventionen werden gemäß ISO/IEC 8824-1 verwendet. Das heißt:

- In den gewählten Benennungen ist soweit möglich die Bedeutung des Datentyps implizit erkennbar.
- Handelt es sich bei einem Datentyp um eine Zusammensetzung aus anderen Datentypen, ist die Datentypbenennung zwar weiterhin eine Folge von alphabetischen Zeichen, die mit einem Großbuchstaben beginnen, doch werden innerhalb der Benennung Großbuchstaben verwendet, um die entsprechende Bedeutung zu vermitteln.
- Generell stehen die Datentypbenennungen in Beziehung zu den Benennungen der Datentypen, aus denen sie aufgebaut sind, zu dem Gerät, in denen die Daten gespeichert werden, und zu der mit den Daten verbundenen Funktion.

Ist ein ASN.1-Typ bereits im Rahmen einer anderen Norm definiert und für den Gebrauch im Kontrollgerät von Bedeutung, wird dieser ASN.1-Typ in dieser Anlage definiert.

Um mehrere Arten von Kodierungsregeln zu ermöglichen, sind einige ASN.1-Typen dieser Anlage mit Wertbereichsbezeichnungen versehen, die in Abschnitt 3 definiert sind.

1.2. Referenzdokumente

In dieser Anlage werden folgende Referenzdokumente herangezogen:

ISO 639	Code for the representation of names of languages. First Edition: 1988. (Code für Sprachennamen)Code for the representation of names of languages. First Edition: 1988. (Code für Sprachennamen)
EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Identifikationskartensysteme — Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke — Teil 3: Applikationsunabhängige Anforderungen an die Karte)
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983. (Straßenfahrzeuge; Fahrzeugidentifizierungsnummer (VIN) — Inhalt und Struktur)
ISO/IEC 7816-5	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996. (Informationstechnik — Identifikationskarten — Chipkarten mit Kontakten — Teil 5: Nummerierungssystem und Registrierverfahren für Anwendungsbezeichner; Deutsche Fassung EN ISO/IEC 7816-5:1995 + A1:1997)
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998. (Informationstechnik — Notation Eins für abstrakte Syntax (ASN.1): Spezifikation der Basisnotation)
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998. (Informationstechnik — Kodierungsregeln für ASN.1: Spezifikation für gepackte Kodierungsregeln (PER))
ISO/IEC 8859-1	Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 1998. (Informationstechnik — einzelbytekodierte 8-Bit-Schriftzeichensätze — Teil 1: Lateinisches Alphabet Nr. 1)
ISO/IEC 8859-7	Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. First edition: 1987. (Informationstechnik — einzelbytekodierte 8-Bit-Schriftzeichensätze — Teil 1: Lateinisch-griechisches Alphabet Nr. 1)
ISO 16844-3	Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99. (Straßenfahrzeuge — Kontrollgerätsysteme — Schnittstelle Weg- und Geschwindigkeitsgeber)

2. DATENTYPDEFINITIONEN

Bei allen folgenden Datentypen besteht der Standardwert für einen ‚unbekannten‘ oder einen ‚nicht zutreffenden‘ Inhalt in der Ausfüllung des Datenelements mit ‚FF‘-Bytes.

2.1. ActivityChangeInfo

Mit diesem Datentyp ist es möglich, den Steckplatz- und Fahrerstatus um 0.00 Uhr und für einen Fahrer oder einen 2. Fahrer Tätigkeitsänderungen und/oder Veränderungen des Status der Fahrzeugführung und/oder Veränderungen des Kartenstatus innerhalb eines Zwei-Byte-Wortes zu kodieren. Dieser Datentyp bezieht sich auf die Randnummern 084, 109a, 199 und 219.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Wertzuweisung — Oktettanordnung: „scpaattttttttttt“B (16 Bit)

Für Aufzeichnungen im Massenspeicher (oder den Steckplatz-Status):

,s'B Steckplatz:

,0'B: FAHRER,

,1'B: 2. FAHRER,

,c'B Status der Fahrzeugführung:

„O‘B: EINMANNBETRIEB,

,1'B: TEAM,

„pB“ Status der Fahrerkarte (oder Werkstattkarte) im entsprechenden Steckplatz:

,0'B: EINGESTECKT, eine Karte ist eingesteckt,

,1'B: NICHT EINGESTECKT, keine Karte eingesteckt (oder Karte entnommen),

aa'B Tätigkeit:

,00'B: UNTERBRECHUNG/RUHE,

,01'B: BEREITSCHAFT,

,10'B: ARBEIT,

,11'B: LENKEN,

Zeitpunkt der Veränderung: Anzahl der Minuten seit 0.00 Uhr an diesem Tag.

Für Aufzeichnungen auf der Fahrerkarte (oder Werkstattkarte) (und den Fahrerstatus):

,s'B Steckplatz (nicht von Belang, wenn ,p' = 1 außer siehe Anmerkung):

,0'B: FAHRER,

,1'B: 2. FAHRER,

„c“B Status der Fahrzeugführung (Fall „p“ = 0) oder Status der Folgetätigkeit (Fall „p“ = 1):

,0'B: EINMANNBETRIEB, ,0'B: UNBEKANNT

,1'B: TEAM, ,1'B: BEKANNT (= manuell eingegeben)

,p'B Kartenstatus:

„0‘B: EINGESTECKT, Karte ist in ein Kontrollgerät eingesteckt,

1'B: NICHT EINGESTECKT, keine Karte eingesteckt (oder Karte entnommen),

,aa'B Tätigkeit (nicht von Belang, wenn ,p' = 1 und ,c' = 0. Ausnahmebedingung siehe Anmerkung):

,00'B: UNTERBRECHUNG/RUHE,

,01'B: BEREITSCHAFT,

,10'B: ARBEIT,

,11'B: LENKEN,

,tttttttttt'B Zeit der Veränderung: Anzahl der Minuten seit 0.00 Uhr an diesem Tag.

Anmerkung für den Fall ,Kartenentnahme':

Wenn die Karte entnommen wurde, gilt folgendes:

- ,s' ist relevant und gibt den Steckplatz an, aus dem die Karte entnommen wurde,
- ,c' muss auf 0 gesetzt sein,
- ,p' muss auf 1 gesetzt sein,
- ,aa' muss die zu dieser Zeit gewählte laufende Tätigkeit kodieren.

Infolge eines manuellen Eintrags können die (auf der Karte gespeicherten) Bits ,c' and ,aa' des Worts später zur Berücksichtigung des Eintrags überschrieben werden.

2.2. Address

Eine Adresse.

```
Address ::= SEQUENCE {
    codePage                               INTEGER (0..255),
    address                                OCTET STRING (SIZE(35))
}
```

codePage gibt den Teil der ISO/IEC 8859 an, der zur Kodierung der Adresse verwendet wurde,

address ist eine gemäß ISO/IEC 8859-Codepage kodierte Adresse.

2.3. BCDString

BCDString wird für die Darstellung von binär kodierten Dezimalzahlen (BCD) angewendet. Dieser Datentyp dient der Darstellung einer Dezimalziffer in einer 4-Bit-Gruppe. BCDString basiert auf ,CharacterStringType' der ISO/IEC 8824-1.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
    identification ( WITH COMPONENTS {
        fixed PRESENT } ) } )
```

BCDString verwendet eine ,hstring'-Notation. Die äußerste linke Hexadezimalziffer ist die höchstwertige 4-Bit-Gruppe des ersten Oktetts. Um ein Vielfaches der Oktette zu erhalten, werden nach Bedarf von der Position der äußersten linken 4-Bit-Gruppe im ersten Oktett 4-Bit-Gruppen mit rechtsstehenden Nullen eingefügt.

Zulässige Ziffern: 0, 1, ... 9.

2.4. CalibrationPurpose

Code zur Erläuterung, warum ein bestimmter Satz von Kalibrierungsparametern aufgezeichnet wurde. Dieser Datentyp bezieht sich auf die Randnummern 097 und 098.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Wertzuweisung:

,00'H reservierter Wert,

,01'H Aktivierung: Aufzeichnung von bekannten Kalibrierungsparametern zum Zeitpunkt der FE-Aktivierung

,02'H Ersteinbau: Erste Kalibrierung der FE nach ihrer Aktivierung.

,03'H Einbau: Erste Kalibrierung der FE im derzeitigen Fahrzeug.

,04'H regelmäßige Nachprüfung.

2.5. CardActivityDailyRecord

Auf einer Karte gespeicherte Informationen zu den Fahrertätigkeiten an einem bestimmten Kalendertag. Dieser Datentyp bezieht sich auf die Randnummern 199 und 219.

```
CardActivityDailyRecord ::= SEQUENCE {
    activityPreviousRecordLength      INTEGER(0..CardActivityLengthRange),
    activityRecordDate                TimeReal,
    activityDailyPresenceCounter      DailyPresenceCounter,
    activityDayDistance               Distance,
    activityChangeInfo                SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength — Gesamtlänge des vorherigen Tagesdatensatzes in Byte. Der Höchstwert wird durch die Länge des OCTET STRING angegeben, der diese Datensätze enthält (siehe CardActivityLengthRange, Abschnitt 3). Ist dieser Datensatz der älteste Tagesdatensatz, muss der Wert von activityPreviousRecordLength auf 0 gesetzt werden.

activityRecordLength — Gesamtlänge dieses Datensatzes in Byte. Der Höchstwert wird durch die Länge des OCTET STRING angegeben, das diese Datensätze enthält.

activityRecordDate — Datum des Datensatzes.

activityDailyPresenceCounter — Tagesanwesenheitszähler für die Karte an diesem Tag.

activityDayDistance — die an diesem Tag zurückgelegte Gesamtwegstrecke.

activityChangeInfo — Menge der ActivityChangeInfo-Daten für den Fahrer an diesem Tag. Kann maximal 1 440 Werte enthalten (1 Tätigkeitsänderung je Minute). Dieser Datensatz enthält stets auch den ActivityChangeInfo-Wert für den Fahrerstatus um 0.00 Uhr.

2.6. CardActivityLengthRange

Anzahl der Bytes auf einer Fahrer- oder Werkstattkarte, die für die Speicherung von Datensätzen zur Fahrertätigkeit zur Verfügung stehen.

```
CardActivityLengthRange ::= INTEGER(0..216-1)
```

Wertzuweisung: siehe Abschnitt 3.

2.7. CardApprovalNumber

Bauartgenehmigungsnummer der Karte.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Wertzuweisung: nicht spezifiziert.

2.8. CardCertificate

Zertifikat des öffentlichen Schlüssels einer Karte.

CardCertificate ::= Certificate

2.9. CardChipIdentification

Auf einer Karte gespeicherte Information zur Identifizierung des integrierten Schaltkreises der Karte (Randnummer 191).

```
CardChipIdentification ::= SEQUENCE {
    icSerialNumber                OCTET STRING (SIZE(4)),
    icManufacturingReferences     OCTET STRING (SIZE(4))
}
```

icSerialNumber — IS-Seriennummer laut Definition in EN 726-3.

icManufacturingReferences — IS-Herstellerbezeichner und Fertigungselement laut Definition in EN 726-3.

2.10. CardConsecutiveIndex

Fortlaufender Kartenindex (Begriffsbestimmung h)).

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

Wertzuweisung: (siehe Kapitel VII in diesem Anhang)

Reihenfolge für die Erhöhung: ,0, ..., 9, A, ... , Z, a, ... , z‘

2.11. CardControlActivityDataRecord

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information über die letzte Kontrolle, welcher der Fahrer unterzogen wurde (Randnummer 210 und 225).

```
CardControlActivityDataRecord ::= SEQUENCE {
    controlType                controlType,
    controlTime                TimeReal,
    controlCardNumber          FullCardNumber,
    controlVehicleRegistration  VehicleRegistrationIdentification,
    controlDownloadPeriodBegin TimeReal,
    controlDownloadPeriodEnd   TimeReal,
}
```

controlType — Art der Kontrolle.

controlTime — Datum und Uhrzeit der Kontrolle.

controlCardNumber — FullCardNumber des ausführenden Kontrollleurs.

controlVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Kontrolle stattfand.

controlDownloadPeriodBegin und **controlDownloadPeriodEnd** — übertragener Zeitraum bei Übertragungen.

2.12. CardCurrentUse

Information über die aktuelle Benutzung der Karte (Randnummer 212).

```
CardCurrentUse ::= SEQUENCE {
    sessionOpenTime          TimeReal,
    sessionOpenVehicle       VehicleRegistrationIdentification
}
```

sessionOpenTime — Uhrzeit, zu der die Karte für die aktuelle Benutzung eingesteckt wird. Bei Kartenentnahme wird dieses Element auf Null gesetzt.

sessionOpenVehicle — Kennung des derzeit gefahrenen Fahrzeugs, gesetzt beim Einstecken der Karte. Bei Kartenentnahme wird dieses Element auf Null gesetzt.

2.13. CardDriverActivity

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information über die Tätigkeiten des Fahrers (Randnummer 199 und 219).

[illegible]

activityPointerOldestDayRecord — Angabe des Beginns des Speicherortes (Anzahl der Bytes vom Anfang des Strings) des ältesten vollständigen Tagesdatensatzes im String activityDailyRecords. Der Höchstwert ist durch die Länge des Strings gegeben.

activityPointerNewestRecord — Angabe des Beginns des Speicherortes (Anzahl der Bytes vom Anfang des Strings) des jüngsten vollständigen Tagesdatensatzes im String activityDailyRecords. Der Höchstwert ist durch die Länge des Strings gegeben.

activityDailyRecords — der für die Fahrtfähigkeitsdaten zur Verfügung stehende Speicherplatz (Datenstruktur: Card ActivityDailyRecord) für jeden Kalendertag, an dem die Karte benutzt wurde.

Wertzuweisung: Dieser Oktettstring wird zyklisch mit CardActivityDailyRecord-Datensätzen gefüllt. Bei der ersten Benutzung beginnt die Speicherung beim ersten Byte des Strings. Alle neuen Datensätze werden am Ende des vorigen angefügt. Ist der String voll, wird die Speicherung am ersten Byte des Strings unabhängig davon fortgesetzt, ob es innerhalb eines Datenelements zu einem Bruch kommt. Bevor (zur Vergrößerung des aktuellen activityDailyRecord oder zum Einsetzen eines neuen activityDailyRecord) neue Tätigkeitsdaten in den String gesetzt werden, die ältere Tätigkeitsdaten ersetzen, muss activityPointerOldestDayRecord aktualisiert werden, um den neuen Platz des ältesten vollständigen Tagesdatensatzes auszuweisen, und activityPreviousRecordLength dieses (neuen) ältesten vollständigen Tagesdatensatzes muss auf 0 zurückgesetzt werden.

2.14. CardDrivingLicenceInformation

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Führerscheindaten des Karteninhabers (Randnummer 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
    drivingLicenceIssuingAuthority      Name,
    drivingLicenceIssuingNation         NationNumeric,
    drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority — die für die Ausstellung des Führerscheins zuständige Behörde.

drivingLicenceIssuingNation — Nationalität der Ausstellungsbehörde des Führerscheins.

drivingLicenceNumber — Nummer des Führerscheins.

2.15. CardEventData

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Ereignissen im Zusammenhang mit dem Karteninhaber (Randnummer 204 und 223).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
    cardEventRecords SET                               SIZE(NoOfEventsPerType) OF
                                                         CardEventRecord
}
```

CardEventData — eine nach absteigendem Wert von EventFaultType geordnete Folge von cardEventRecords (mit Ausnahme von Versuchen der Sicherheitsverletzung, die in der letzten Gruppe der Folge zusammengefasst sind).

cardEventRecords — Ereignisdatensätze einer bestimmten Ereignisart (oder Kategorie bei Ereignissen Versuch Sicherheitsverletzung).

2.16. CardEventRecord

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu einem Ereignis im Zusammenhang mit dem Karteninhaber (Randnummer 205 und 223).

```
CardEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventBeginTime            TimeReal,
    eventEndTime              TimeReal,
    eventVehicleRegistration  VehicleRegistrationIdentification
}
```

eventType — Art des Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

eventVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem das Ereignis eingetreten ist.

2.17. CardFaultData

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu den Störungen im Zusammenhang mit dem Karteninhaber (Randnummer 207 und 223).

```
CardFaultData ::= SEQUENCE SIZE (2) OF {
    cardFaultRecords                               SET SIZE (NoOfFaultsPerType) OF
                                                    CardFaultRecord
}
```

CardFaultData — eine Folge von Datensätzen mit Kontrollgerätstörungen, gefolgt von Datensätzen mit Kartenfehlfunktionen.

cardFaultRecords — Störungsdatensätze einer bestimmten Störungskategorie (Kontrollgerät oder Karte).

2.18. CardFaultRecord

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zu einer Störung im Zusammenhang mit dem Karteninhaber (Randnummer 208 und 223).

```
CardFaultRecord ::= SEQUENCE {
    faultType                                     EventFaultType,
    faultBeginTime                               TimeReal,
    faultEndTime                                 TimeReal,
    faultVehicleRegistration                     VehicleRegistrationIdentification
}
```

faultType — Art der Störung.

faultBeginTime — Datum und Uhrzeit des Störungsbeginns.

faultEndTime — Datum und Uhrzeit des Störungsendes.

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

2.19. CardIccIdentification

Auf einer Karte gespeicherte Information zur Identifizierung der Chipkarte (Randnummer 192).

```
CardIccIdentification ::= SEQUENCE {
    clockStop                                     OCTET STRING (SIZE (1)),
    cardExtendedSerialNumber                     ExtendedSerialNumber,
    cardApprovalNumber                           CardApprovalNumber
    cardPersonaliserID                           OCTET STRING (SIZE (1)),
    embedderIcAssemblerId                       OCTET STRING (SIZE (5)),
    icIdentifier                                 OCTET STRING (SIZE (2))
}
```

clockStop — Clockstop-Modus laut Definition in EN 726-3.

cardExtendedSerialNumber — Seriennummer sowie Fertigungsangabe der Chipkarte laut Definition in EN 726-3 und laut weiterer Spezifikation durch den Datentyp ExtendedSerialNumber.

cardApprovalNumber — Bauartgenehmigungsnummer der Karte.

cardPersonaliserID — Karten-Personaliser-ID laut Definition in EN 726-3.

embedderId — Kartenhersteller-/IS-Assembler-Bezeichner laut Definition in EN 726-3.

icIdentifier — Bezeichner des IS auf der Karte und des IS-Herstellers laut Definition in EN 726-3.

2.20. CardIdentification

Auf der Karte gespeicherte Information zur Identifikation der Karte (Randnummer 194, 215, 231, 235).

`CardIdentification ::= SEQUENCE`

```

    cardIssuingMemberState      NationNumeric,
    cardNumber                  CardNumber,
    cardIssuingAuthorityName    Name,
    cardIssueDate               TimeReal,
    cardValidityBegin           TimeReal,
    cardExpiryDate              TimeReal
}

```

cardIssuingMemberState — Code des Mitgliedstaates, der die Karte ausgestellt hat.

cardNumber — Kartennummer.

cardIssuingAuthorityName — Name der Behörde, die die Karte ausgestellt hat.

cardIssueDate — Datum der Ausstellung der Karte an den derzeitigen Inhaber.

cardValidityBegin — Datum, an dem die Gültigkeit der Karte beginnt.

cardExpiryDate — Datum, an dem die Gültigkeit der Karte abläuft.

2.21. CardNumber

Kartennummer nach Definition g).

`CardNumber ::= CHOICE {`

```

    SEQUENCE {
        driverIdentification      IA5String(SIZE(14)),
        cardReplacementIndex      CardReplacementIndex,
        cardRenewalIndex          CardRenewalIndex
    }
    SEQUENCE {
        ownerIdentification       IA5String(SIZE(13)),
        cardConsecutiveIndex      CardConsecutiveIndex,
        cardReplacementIndex      CardReplacementIndex,
        cardRenewalIndex          CardRenewalIndex
    }
}

```

driverIdentification — eindeutige Kennung eines Fahrers in einem Mitgliedstaat.

ownerIdentification — eindeutige Kennung eines Unternehmens oder einer Werkstatt oder einer Kontrollstelle in einem Mitgliedstaat.

cardConsecutiveIndex — fortlaufender Kartenindex.

cardReplacementIndex — Kartenersatzindex.

cardRenewalIndex — Kartenerneuerungsindex.

Die erste Folge der Auswahl eignet sich zur Kodierung einer Fahrerkartennummer, die zweite Folge zur Kodierung der Werkstatt-, Kontroll- und Unternehmenskartennummer.

2.22. CardPlaceDailyWorkPeriod

Auf einer Fahrer- oder Werkstattkarte gespeicherte Information zum Ort des Beginns und/oder des Endes des Arbeitstages (Randnummer 202 und 221).

```

CardPlaceDailyWorkPeriod ::= SEQUENCE {
    placePointerNewestRecord          INTEGER(0..NoOfCardPlaceRecords-1),
    placeRecords                      SET SIZE (NoOfCardPlaceRecords) OF PlaceRe-
                                     cord
}

```

placePointerNewestRecord — Index des zuletzt aktualisierten Ortsdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Ortsdatensatzes entspricht, beginnend mit ,0' für das erste Auftreten der Ortsdatensätze in der Struktur.

placeRecords — Datensätze mit Informationen zu den eingegebenen Orten.

2.23. CardPrivateKey

Der private Schlüssel einer Karte.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. CardPublicKey

Der öffentliche Schlüssel einer Karte.

```
CardPublicKey ::= PublicKey
```

2.25. CardRenewalIndex

Ein Kartenerneuerungsindex (Begriffsbestimmung i)).

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

Wertzuweisung: (siehe Kapitel VII in diesem Anhang).

,0' Erstaussstellung.

Reihenfolge für die Erhöhung: ,0, ..., 9, A, ..., Z'

2.26. CardReplacementIndex

Ein Kartenersatzindex (Begriffsbestimmung j)).

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

Wertzuweisung: (siehe Kapitel VII in diesem Anhang).

,0' Originalkarte.

Reihenfolge für die Erhöhung: ,0, ..., 9, A, ..., Z'

2.27. CardSlotNumber

Code zur Unterscheidung der beiden Steckplätze einer Fahrzeugeinheit.

```

CardSlotNumber ::= INTEGER {
    driverSlot          (0),
    co-driverSlot       (1)
}

```

Wertzuweisung: nicht näher spezifiziert.

2.28. CardSlotsStatus

Code zur Angabe der in den beiden Steckplätzen der Fahrzeugeinheit eingesetzten Kartenarten.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

```
CardVehiclesUsed := SEQUENCE {
    vehiclePointerNewestRecord      INTEGER(0..NoOfCardVehicleRecords-1),
    cardVehicleRecords              SET SIZE (NoOfCardVehicleRecords) OF
                                   CardVehicleRecord
}
```

vehiclePointerNewestRecord — Index des zuletzt aktualisierten Fahrzeugdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Fahrzeugdatensatzes entspricht, beginnend mit ,0' für das erste Auftreten der Fahrzeugdatensätze in der Struktur.

cardVehicleRecords — Datensätze mit Informationen zu den gefahrenen Fahrzeugen.

2.32. Certificate

Das von einer Zertifizierungsstelle ausgestellte Zertifikat eines öffentlichen Schlüssels.

`Certificate ::= OCTET STRING (SIZE(194))`

Wertzuweisung: digitale Signatur mit teilweiser Wiederherstellung eines CertificateContent gemäß Anlage 11 ‚Gemeinsame Sicherheitsmechanismen‘: Signature (128 Byte) || Public Key remainder (58 Byte) || Certification Authority Reference (8 Byte).

2.33. CertificateContent

Der (Klartext-) Inhalt des Zertifikats eines öffentlichen Schlüssels gemäß Anlage 11 ‚Gemeinsame Sicherheitsmechanismen‘.

```
CertificateContent ::= SEQUENCE {
    certificateProfileIdentifier      INTEGER(0..255),
    certificationAuthorityReference  KeyIdentifier,
    certificateHolderAuthorisation    CertificateHolderAuthorisation,
    certificateEndOfValidity          TimeReal,
    certificateHolderReference        KeyIdentifier,
    publicKey                        PublicKey
}
```

certificateProfileIdentifier — Version des entsprechenden Zertifikats.

Wertzuweisung: ,01h' für diese Version.

CertificationAuthorityReference identifiziert die das Zertifikat ausstellende Zertifizierungsstelle und enthält darüber hinaus einen Verweis auf den öffentlichen Schlüssel dieser Zertifizierungsstelle.

certificateHolderAuthorisation identifiziert die Rechte des Zertifikatsinhabers.

certificateEndOfValidity — Datum, an dem die Gültigkeit des Zertifikats administrativ endet.

certificateHolderReference identifiziert den Zertifikatsinhaber und enthält zugleich einen Verweis auf dessen öffentlichen Schlüssel.

publicKey — der öffentliche Schlüssel, der durch dieses Zertifikat zertifiziert wird.

2.34. CertificateHolderAuthorisation

Identifizierung der Rechte eines Zertifikatsinhabers.

```
CertificateHolderAuthorisation ::= SEQUENCE {
    tachographApplicationID          OCTET STRING(SIZE(6))
    equipmentType                     EquipmentType
}
```

tachographApplicationID — Anwendungsbezeichner für die Kontrollgerätenwendung.

Wertzuweisung: ,FFh' ,54h' ,41h' ,43h' ,48h' ,4Fh'. Dieser AID ist ein proprietärer nichtregistrierter Anwendungsbezeichner gemäß ISO/IEC 7816-5.

equipmentType ist die Kennung des Gerätetyps, für den das Zertifikat bestimmt ist.

Wertzuweisung: entsprechend dem Datentyp EquipmentType. 0, wenn es sich um ein Zertifikat eines Mitgliedstaates handelt.

2.35. CertificateRequestID

Eindeutige Kennung eines Zertifikatsantrags. Kann auch als Bezeichner des öffentlichen Schlüssels einer Fahrzeugeinheit verwendet werden, wenn die Seriennummer der Fahrzeugeinheit, für die der Schlüssel bestimmt ist, zum Zeitpunkt der Erzeugung des Zertifikats nicht bekannt ist.

```
CertificateRequestID ::= SEQUENCE {
    requestSerialNumber      INTEGER(0..232-1)
    requestMonthYear         BCDString(SIZE(2))
    crIdentifier             OCTET STRING(SIZE(1))
    manufacturerCode        ManufacturerCode
}
```

requestSerialNumber — einmalige Seriennummer des Zertifikatsantrags für den im Folgenden angegebenen Hersteller und Monat.

requestMonthYear — Kennung für den Monat und das Jahr des Zertifikatsantrags.

Wertzuweisung: BCD-Kodierung des Monats (zwei Stellen) und des Jahres (die beiden letzten Stellen).

crIdentifier — Bezeichner zur Unterscheidung eines Zertifikatsantrags von einer erweiterten Seriennummer.

Wertzuweisung: ‚FFh‘.

manufacturerCode — numerischer Code des Herstellers, der das Zertifikat beantragt.

2.36. CertificationAuthorityKID

Bezeichner des öffentlichen Schlüssels einer Zertifizierungsstelle (Mitgliedstaatliche Stelle oder Europäische Zertifizierungsstelle).

```
CertificationAuthorityKID ::= SEQUENCE {
    nationNumeric            NationNumeric
    nationAlpha             NationAlpha
    keySerialNumber         INTEGER(0..255)
    additionalInfo          OCTET STRING(SIZE(2))
    caIdentifier            OCTET STRING(SIZE(1))
}
```

nationNumeric — numerischer Landescode der Zertifizierungsstelle.

nationAlpha — alphanumerischer Landescode der Zertifizierungsstelle.

keySerialNumber — eine Seriennummer zur Unterscheidung der verschiedenen Schlüssel der Zertifizierungsstelle für den Fall des Wechsels von Schlüsseln.

additionalInfo — 2-Byte-Feld für Zusatzkodierung (je nach Zertifizierungsstelle).

caIdentifier — Bezeichner zur Unterscheidung des Schlüsselbezeichners einer Zertifizierungsstelle von anderen Schlüsselbezeichnern.

Wertzuweisung: ‚01h‘.

2.37. CompanyActivityData

Auf einer Unternehmenskarte gespeicherte Information zu den mit der Karte ausgeführten Tätigkeiten (Randnummer 237).

```
CompanyActivityData ::= SEQUENCE {
    companyPointerNewestRecord    INTEGER(0..NoOfCompanyActivityRecords-1),
    companyActivityRecords       SET SIZE(NoOfCompanyActivityRecords) OF
        companyActivityRecord    SEQUENCE {
            companyActivityType    CompanyActivityType,
            companyActivityTime     TimeReal,
            cardNumberInformation   FullCardNumber,
```

```

        vehicleRegistrationInformation      VehicleRegistrationIdentification,
        downloadPeriodBegin                TimeReal,
        downloadPeriodEnd                   TimeReal
    }
}

```

companyPointerNewestRecord — Index des zuletzt aktualisierten companyActivityRecord.

Wertzuweisung: Zahl, die dem Zähler des Unternehmenstätigkeitsdatensatzes entspricht, beginnend mit ,0' für das erste Auftreten des Unternehmenstätigkeitsdatensatzes in der Struktur.

companyActivityRecords — sämtliche Unternehmenstätigkeitsdatensätze.

companyActivityRecord — Folge von Informationen zu einer Unternehmenstätigkeit.

companyActivityType — Art der Unternehmenstätigkeit.

companyActivityTime — Datum und Uhrzeit der Unternehmenstätigkeit.

cardNumberInformation — gegebenenfalls Kartenummer und ausstellender Mitgliedstaat der heruntergeladenen Karte.

vehicleRegistrationInformation — amtliches Kennzeichen und zulassender Mitgliedstaat des heruntergeladenen bzw. des gesperrten oder entsperrten Fahrzeugs.

downloadPeriodBegin und **downloadPeriodEnd** — gegebenenfalls der von der FE heruntergeladene Zeitraum.

2.38. CompanyActivityType

Code für die von einem Unternehmen unter Nutzung seiner Unternehmenskarte ausgeführte Tätigkeit.

```

CompanyActivityType ::= INTEGER {
    card downloading                (1),
    VU downloading                  (2),
    VU lock-in                       (3),
    VU lock-out                      (4)
}

```

2.39. CompanyCardApplicationIdentification

Auf einer Unternehmenskarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Randnummer 190).

```

CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion              CardStructureVersion,
    noOfCompanyActivityRecords        NoOfCompanyActivityRecords
}

```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion gibt die Version der auf der Karte implementierten Struktur an.

noOfCompanyActivityRecords — Anzahl der Unternehmenstätigkeitsdatensätze, die die Karte speichern kann.

2.40. CompanyCardHolderIdentification

Auf einer Unternehmenskarte gespeicherte Information zur Identifizierung des Karteninhabers (Randnummer 236).

```

CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                      Name,
    companyAddress                    Address,
    cardHolderPreferredLanguage      Language
}

```

companyName — Name des Unternehmens, dem die Karte gehört.

companyAddress — Anschrift des Unternehmens, dem die Karte gehört.

cardHolderPreferredLanguage — Muttersprache des Karteninhabers.

2.41. **ControlCardApplicationIdentification**

Auf einer Kontrollkarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Randnummer 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion             CardStructureVersion,
    noOfControlActivityRecords       NoOfControlActivityRecords
}
```

typeOfTachographCardId gibt den implementierten Kartentyp an.

cardStructureVersion gibt die Version der auf der Karte implementierten Struktur an.

noOfControlActivityRecords — Anzahl der Kontrolltätigkeitsdatensätze, die die Karte speichern kann.

2.42. **ControlCardControlActivityData**

Auf einer Kontrollkarte gespeicherte Information zur mit der Karte durchgeführten Kontrollaktivität (Randnummer 233).

```
ControlCardControlActivityData ::= SEQUENCE {
    controlPointerNewestRecord        INTEGER(0..NoOfControlActivityRecords-1),
    controlActivityRecords            SET SIZE (NoOfControlActivityRecords) OF
        controlActivityRecord        SEQUENCE {
            controlType               ControlType,
            controlTime               TimeReal,
            controlledCardNumber       FullCardNumber,
            controlledVehicleRegistration VehicleRegistrationIdentification,
            controlDownloadPeriodBegin TimeReal,
            controlDownloadPeriodEnd   TimeReal
        }
}
```

controlPointerNewestRecord — Index des zuletzt aktualisierten Kontrolltätigkeitsdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Kontrolltätigkeitsdatensatzes entspricht, beginnend mit ,0' für das erste Auftreten des Kontrolltätigkeitsdatensatzes in der Struktur.

controlActivityRecords — sämtliche Kontrolltätigkeitsdatensätze.

controlActivityRecord — Folge von Informationen zu einer Kontrolle.

controlType — Art der Kontrolle.

controlTime — Datum und Uhrzeit der Kontrolle.

controlledCardNumber — Kartenummer und ausstellender Mitgliedstaat der kontrollierten Karte.

controlledVehicleRegistration — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs, in dem die Kontrolle stattfand.

controlDownloadPeriodBegin und **controlDownloadPeriodEnd** — heruntergeladener Zeitraum.

2.43. **ControlCardHolderIdentification**

Auf einer Kontrollkarte gespeicherte Information zur Identifizierung des Karteninhabers (Randnummer 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
    controlBodyName          Name,
    controlBodyAddress       Address,
    cardHolderName           HolderName,
    cardHolderPreferredLanguage Language
}
```

controlBodyName — Name der Kontrollstelle des Karteninhabers.

controlBodyAddress — Anschrift der Kontrollstelle des Karteninhabers.

cardHolderName — Name und Vorname(n) des Inhabers der Kontrollkarte.

cardHolderPreferredLanguage — Muttersprache des Karteninhabers.

2.44. ControlType

Code zur Angabe der bei einer Kontrolle ausgeführten Aktivitäten. Dieser Datentyp bezieht sich auf die Randnummern 102, 210 and 225.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Wertzuweisung — Oktettanordnung: ,cvpdx' (8 Bit)

,c'B Herunterladen Karte:
 ,0'B: Karte bei dieser Kontrollaktivität nicht heruntergeladen,
 ,1'B: Karte bei dieser Kontrollaktivität heruntergeladen
 ,v'B Herunterladen FE:
 ,0'B: FE bei dieser Kontrollaktivität nicht heruntergeladen,
 ,1'B: FE bei dieser Kontrollaktivität heruntergeladen
 ,p'B Drucken:
 ,0'B: kein Drucken bei dieser Kontrollaktivität,
 ,1'B: Drucken bei dieser Kontrollaktivität
 ,d'B Anzeige:
 ,0'B: keine Anzeige bei dieser Kontrollaktivität verwendet,
 ,1'B: Anzeige bei dieser Kontrollaktivität verwendet
 ,xxx'B Nicht verwendet.

2.45. CurrentDateTime

Aktuelles Datum und aktuelle Uhrzeit des Kontrollgeräts.

```
CurrentDateTime ::= TimeReal
```

Wertzuweisung: nicht näher spezifiziert.

2.46. DailyPresenceCounter

Auf einer Fahrer- oder Werkstattkarte gespeicherter Zähler, der für jeden Kalendertag, an dem die Karte in eine FE eingesteckt wurde, um eins erhöht wird. Dieser Datentyp bezieht sich auf die Randnummern 199 and 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Wertzuweisung: Laufende Nummer mit Höchstwert = 9999, danach wieder bei 0 beginnend. Zum Zeitpunkt des ersten Einsteckens der Karte ist die Zahl auf 0 gesetzt.

2.47. Datef

Datum in einem leicht ausdrückbaren numerischen Format.

```
Datef ::= SEQUENCE {
    year      BCDString(SIZE(2)),
    month     BCDString(SIZE(1)),
    day       BCDString(SIZE(1))
}
```

Wertzuweisung:

```
yyyy      Jahr
mm        Monat
dd        Tag
```

,00000000'H bezeichnet explizit kein Datum.

2.48. Distance

Eine zurückgelegte Wegstrecke (Ergebnis der Differenz von zwei Kilometerständen des Fahrzeugs).

```
Distance ::= INTEGER(0..216-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in km im Betriebsbereich 0 bis 9999 km.

2.49. DriverCardApplicationIdentification

Auf einer Fahrerkarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Randnummer 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType            NoOfEventsPerType,
    noOfFaultsPerType            NoOfFaultsPerType,
    activityStructureLength       CardActivityLengthRange,
    noOfCardVehicleRecords       NoOfCardVehicleRecords,
    noOfCardPlaceRecords         NoOfCardPlaceRecords
}
```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion gibt die Version der auf der Karte implementierten Version der Struktur an.

noOfEventsPerType — Anzahl der Ereignisse je Ereignisart, die die Karte speichern kann.

noOfFaultsPerType — Anzahl der Störungen je Störungsart, die die Karte speichern kann.

activityStructureLength gibt die Zahl der Bytes an, die für die Speicherung von Tätigkeitsdatensätzen zur Verfügung stehen.

noOfCardVehicleRecords — Anzahl der Fahrzeugdatensätze, die die Karte enthalten kann.

noOfCardPlaceRecords — Anzahl der Orte, die die Karte aufzeichnen kann.

2.50. DriverCardHolderIdentification

Auf einer Fahrerkarte gespeicherte Information zur Identifizierung des Karteninhabers (Randnummer 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
    cardHolderName      HolderName,
    cardHolderBirthDate Datef,
    cardHolderPreferredLanguage Language
}
```

cardHolderName — Name und Vorname(n) des Inhabers der Fahrerkarte.

cardHolderBirthDate — Geburtsdatum des Inhabers der Fahrerkarte.

cardHolderPreferredLanguage — Muttersprache des Karteninhabers.

2.51. EntryTypeDailyWorkPeriod

Code zur Unterscheidung zwischen Beginn und Ende des Eintrags eines Arbeitstages und Eingabebedingung.

EntryTypeDailyWorkPeriod ::= INTEGER

Begin,	related time = card insertion time or time of entry	(0),
End,	related time = card withdrawal time or time of entry	(1),
Begin,	related time manually entered (start time)	(2),
End,	related time manually entered (end of work period)	(3),
Begin,	related time assumed by VU	(4),
End,	related time assumed by VU	(5)

}

Wertzuweisung: gemäß ISO/IEC8824-1.

2.52. EquipmentType

Code zur Unterscheidung verschiedener Gerätetypen für die Kontrollgerätenwendung.

EquipmentType ::= INTEGER(0..255)

-- Reserved	(0),
-- Driver Card	(1),
-- Workshop Card	(2),
-- Control Card	(3),
-- Company Card	(4),
-- Manufacturing Card	(5),
-- Vehicle Unit	(6),
-- Motion Sensor	(7),
-- RFU	(8..255)

Wertzuweisung: gemäß ISO/IEC 8824-1.

Der Wert 0 ist für die Angabe des Mitgliedstaats oder Europas im CHA-Feld der Zertifikate reserviert.

2.53. EuropeanPublicKey

Der europäische öffentliche Schlüssel.

EuropeanPublicKey ::= PublicKey

2.54. EventFaultType

Code zur näheren Beschreibung eines Ereignisses oder einer Störung.

EventFaultType ::= OCTET STRING (SIZE(1))

Wertzuweisung:

'0x'H	Allgemeine Ereignisse
'00'H	Keine weiteren Angaben
'01'H	Einstecken einer ungültigen Karte
'02'H	Kartenkonflikt
'03'H	Zeitüberlappung
'04'H	Lenken ohne geeignete Karte
'05'H	Einstecken der Karte während des Lenkens
'06'H	Letzter Vorgang nicht korrekt abgeschlossen
'07'H	Geschwindigkeitsüberschreitung

'08'H	Unterbrechung der Stromversorgung
'09'H	Datenfehler Weg und Geschwindigkeit
'0A'H .. '0F'H	RFU (für zukünftige Funktionen reserviert)
'1x'H	Sicherheitsverletzende Versuche an der Fahrzeugeinheit
'10'H	Keine weiteren Angaben
'11'H	Fehlgeschlagene Authentisierung des Weg- und/oder Geschwindigkeitsgebers
'12'H	Authentisierungsfehler der Kontrollgerätkarte
'13'H	Unbefugte Veränderung des Weg- und/oder Geschwindigkeitsgebers
'14'H	Integritätsfehler der Kartendateneingabedaten
'15'H	Integritätsfehler der gespeicherten Benutzerdaten
'16'H	Interner Datenübertragungsfehler
'17'H	Unberechtigtes Öffnen des Gehäuses
'18'H	Hardwaremanipulation
'19'H .. '1F'H	RFU
'2x'H	Sicherheitsverletzende Versuche Weg- und/oder Geschwindigkeitsgeber
'20'H	Keine weiteren Angaben
'21'H	Fehlgeschlagene Authentisierung
'22'H	Integritätsfehler der Speicherdaten
'23'H	Interner Datenübertragungsfehler
'24'H	Unberechtigtes Öffnen des Gehäuses
'25'H	Hardwaremanipulation
'26'H .. '2F'H	RFU
'3x'H	Störungen Kontrollgerät
'30'H	Keine weiteren Angaben
'31'H	FE-interne Störung
'32'H	Druckerstörung
'33'H	Anzeigestörung
'34'H	Störung beim Herunterladen
'35'H	Sensorstörung
'36'H .. '3F'H	RFU
'4x'H	Kartenstörungen
'40'H	Keine weiteren Angaben
'41'H .. '4F'H	RFU
'50'H .. '7F'H	RFU
'80'H .. 'FF'H	Herstellerspezifisch.

2.55. EventFaultRecordPurpose

Code, der erläutert, warum ein Ereignis oder eine Störung aufgezeichnet wurde.

EventFaultRecordPurpose ::= OCTET STRING (SIZE (1))

Wertzuweisung:

'00'H	eines der 10 jüngsten Ereignisse oder Störungen
'01'H	das längste Ereignis an einem der letzten 10 Tage des Auftretens
'02'H	eines der 5 längsten Ereignisse in den letzten 365 Tagen
'03'H	das letzte Ereignis an einem der letzten 10 Tage des Auftretens
'04'H	das schwerwiegendste Ereignis an einen der letzten 10 Tage des Auftretens
'05'H	eines der 5 schwerwiegendsten Ereignisse in den letzten 365 Tagen
'06'H	das erste Ereignis oder die erste Störung nach der letzten Kalibrierung
'07'H	ein aktives Ereignis oder eine andauernde Störung
'08'H .. '7F'H	RFU
'80'H .. 'FF'H	herstellerspezifisch

2.56. ExtendedSerialNumber

Eindeutige Kennung eines Geräts. Kann auch als Bezeichner des öffentlichen Schlüssels eines Geräts verwendet werden.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber          INTEGER(0..232-1)
    monthYear             BCDString(SIZE(2))
    type                  OCTET STRING(SIZE(1))
    manufacturerCode      ManufacturerCode
}
```

serialNumber — einmalige Seriennummer des Geräts in Bezug auf den Hersteller, den Gerätetyp und den im Folgenden angegebenen Monat.

monthYear — Kennung für den Monat und das Jahr der Herstellung (oder der Zuweisung der Seriennummer).

Wertzuweisung: BCD-Kodierung des Monats (zwei Stellen) und des Jahres (die beiden letzten Stellen).

type — Bezeichner des Gerätetyps.

Wertzuweisung: herstellerspezifisch, mit reserviertem Wert ‚FFh‘.

manufacturerCode — numerischer Code des Geräteherstellers.

2.57. FullCardNumber

Code zur vollständigen Identifizierung einer Karte.

```
FullCardNumber ::= SEQUENCE {
    cardType              EquipmentType,
    cardIssuingMemberState NationNumeric,
    cardNumber            CardNumber
}
```

cardType — Art der Kontrollgerätkarte.

cardIssuingMemberState — Code des Mitgliedstaates, der die Karte ausgegeben hat.

cardNumber — Kartenummer.

2.58. HighResOdometer

Kilometerstand des Fahrzeugs: Vom Fahrzeug während des Betriebs insgesamt zurückgelegte Wegstrecke.

```
HighResOdometer ::= INTEGER(0..232-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in 1/200 km im Betriebsbereich 0 bis 21 055 406 km.

2.59. HighResTripDistance

Während einer Fahrt oder eines Teils einer Fahrt zurückgelegte Wegstrecke.

```
HighResTripDistance ::= INTEGER(0..232-1)
```

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in 1/200 km im Betriebsbereich 0 bis 21 055 406 km.

2.60. HolderName

Familiennamen und Vorname(n) eines Karteninhabers.

```
HolderName ::= SEQUENCE {
    holderSurname          Name,
    holderFirstNames       Name
}
```


holderSurname — Familienname des Inhabers ohne Titel.

Wertzuweisung: Handelt es sich nicht um eine auf eine bestimmte Person ausgestellte Karte, enthält holderSurname die gleichen Informationen wie companyName oder workshopName oder controlBodyName.

holderFirstNames — Vorname(n) und Initialen des Inhabers.

2.61. **K-ConstantOfRecordingEquipment**

Kontrollgerätkonstante (Begriffsbestimmung m)).

`K-ConstantOfRecordingEquipment ::= INTEGER(0..216-1)`

Wertzuweisung: Impulse je Kilometer im Betriebsbereich 0 bis 64 255 Imp/km.

2.62. **KeyIdentifier**

Eindeutiger Bezeichner eines öffentlichen Schlüssels zur Herstellung eines Verweises auf den Schlüssel und für dessen Auswahl. Identifiziert zugleich den Inhaber des Schlüssels.

```
KeyIdentifier ::= CHOICE {
    extendedSerialNumber          ExtendedSerialNumber,
    certificateRequestID           CertificateRequestID,
    certificationAuthorityKID      CertificationAuthorityKID
}
```

Die erste Auswahlmöglichkeit eignet sich zum Verweis auf den öffentlichen Schlüssel einer Fahrzeugeinheit oder einer Kontrollgerätkarte.

Die zweite Auswahlmöglichkeit eignet sich zum Verweis auf den öffentlichen Schlüssel einer Fahrzeugeinheit (falls die Seriennummer der Fahrzeugeinheit zum Zeitpunkt der Generierung des Zertifikats nicht bekannt ist).

Die dritte Auswahlmöglichkeit eignet sich zum Verweis auf den öffentlichen Schlüssel eines Mitgliedstaates.

2.63. **L-TyreCircumference**

Tatsächlicher Umfang der Fahrzeugreifen (Begriffsbestimmung u)).

`L-TyreCircumference ::= INTEGER(0..216-1)`

Wertzuweisung: Vorzeichenlose Binärzahl, Wert in 1/8 mm im Betriebsbereich 0 bis 8 031 mm.

2.64. **Language**

Code zur Identifizierung einer Sprache.

`Language ::= IA5String(SIZE(2))`

Wertzuweisung: Kodierung aus zwei Kleinbuchstaben gemäß ISO 639.

2.65. **LastCardDownload**

Auf der Fahrerkarte gespeicherte(s) Datum und Uhrzeit des letzten Herunterladens der Daten von der Karte (zu anderen als Kontrollzwecken). Diese Datumsangabe kann mit einer beliebigen FE oder einem Kartenlesegerät geändert werden.

`LastCardDownload ::= TimeReal`

Wertzuweisung: nicht näher spezifiziert.

2.66. **ManualInputFlag**

Code, der angibt, ob ein Karteninhaber beim Einstecken der Karte Fahrtätigkeiten manuell eingegeben hat oder nicht (Randnummer 081).

```
ManualInputFlag ::= INTEGER {
    noEntry                (0)
    manualEntries          (1)
}
```

Wertzuweisung: nicht näher spezifiziert.

2.67. ManufacturerCode

Code zur Identifizierung des Herstellers.

```
ManufacturerCode ::= INTEGER(0..255)
```

Wertzuweisung:

'00'H	Keine Informationen verfügbar
'01'H	Reservierter Wert
'02'H .. '0F'H	Zur künftigen Verwendung reserviert
'10'H	ACTIA
'11'H .. '17'H	Reserviert für Hersteller, deren Name mit ‚A‘ beginnt
'18'H .. '1F'H	Reserviert für Hersteller, deren Name mit ‚B‘ beginnt
'20'H .. '27'H	Reserviert für Hersteller, deren Name mit ‚C‘ beginnt
'28'H .. '2F'H	Reserviert für Hersteller, deren Name mit ‚D‘ beginnt
'30'H .. '37'H	Reserviert für Hersteller, deren Name mit ‚E‘ beginnt
'38'H .. '3F'H	Reserviert für Hersteller, deren Name mit ‚F‘ beginnt
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Reserviert für Hersteller, deren Name mit ‚G‘ beginnt
'48'H .. '4F'H	Reserviert für Hersteller, deren Name mit ‚H‘ beginnt
'50'H .. '57'H	Reserviert für Hersteller, deren Name mit ‚I‘ beginnt
'58'H .. '5F'H	Reserviert für Hersteller, deren Name mit ‚J‘ beginnt
'60'H .. '67'H	Reserviert für Hersteller, deren Name mit ‚K‘ beginnt
'68'H .. '6F'H	Reserviert für Hersteller, deren Name mit ‚L‘ beginnt
'70'H .. '77'H	Reserviert für Hersteller, deren Name mit ‚M‘ beginnt
'78'H .. '7F'H	Reserviert für Hersteller, deren Name mit ‚N‘ beginnt
'80'H	OSCARD
'81'H .. '87'H	Reserviert für Hersteller, deren Name mit ‚O‘ beginnt
'88'H .. '8F'H	Reserviert für Hersteller, deren Name mit ‚P‘ beginnt
'90'H .. '97'H	Reserviert für Hersteller, deren Name mit ‚Q‘ beginnt
'98'H .. '9F'H	Reserviert für Hersteller, deren Name mit ‚R‘ beginnt
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Reserviert für Hersteller, deren Name mit ‚S‘ beginnt
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Reserviert für Hersteller, deren Name mit ‚T‘ beginnt
'B0'H .. 'B7'H	Reserviert für Hersteller, deren Name mit ‚U‘ beginnt
'B8'H .. 'BF'H	Reserviert für Hersteller, deren Name mit ‚V‘ beginnt
'C0'H .. 'C7'H	Reserviert für Hersteller, deren Name mit ‚W‘ beginnt
'C8'H .. 'CF'H	Reserviert für Hersteller, deren Name mit ‚X‘ beginnt
'D0'H .. 'D7'H	Reserviert für Hersteller, deren Name mit ‚Y‘ beginnt
'D8'H .. 'DF'H	Reserviert für Hersteller, deren Name mit ‚Z‘ beginnt

2.68. MemberStateCertificate

Zertifikat des öffentlichen Schlüssels eines Mitgliedstaates, ausgestellt von der europäischen Zertifizierungsstelle.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Der öffentliche Schlüssel eines Mitgliedstaates.

`MemberStatePublicKey ::= PublicKey`

2.70. Name

Ein Name.

```
Name ::= SEQUENCE {
    codePage                INTEGER (0..255),
    name                    OCTET STRING (SIZE (35))
}
```

codePage gibt den Teil der ISO/IEC 8859 an, der zur Kodierung des Namens verwendet wurde.

name — ein entsprechend der ISO/IEC 8859-Codepage kodierter Name.

2.71. NationAlpha

Alphabetische Bezeichnung eines Landes entsprechend der üblichen Landeskennzeichen an Kraftfahrzeugen und/oder entsprechend der Verwendung in den international einheitlichen Fahrzeugversicherungspapieren (grüne Versicherungskarte).

`NationAlpha ::= IA5String(SIZE(3))`

Wertzuweisung:

' '	Keine Information verfügbar
'A'	Österreich
'AL'	Albanien
'AND'	Andorra
'ARM'	Armenien
'AZ'	Aserbaidschan
'B'	Belgien
'BG'	Bulgarien
'BIH'	Bosnien und Herzegowina
'BY'	Weißrussland
'CH'	Schweiz
'CY'	Zypern
'CZ'	Tschechische Republik
'D'	Deutschland
'DK'	Dänemark
'E'	Spanien
'EST'	Estland
'F'	Frankreich
'FIN'	Finnland
'FL'	Liechtenstein
'FR'	Färöer
'UK'	Vereinigtes Königreich, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar
'GE'	Georgien
'GR'	Griechenland
'H'	Ungarn
'HR'	Kroatien
'I'	Italien
'IRL'	Irland
'IS'	Island
'KZ'	Kasachstan
'L'	Luxemburg
'LT'	Litauen
'LV'	Lettland
'M'	Malta
'MC'	Monaco

'MD'	Republik Moldau
'MK'	Mazedonien
'N'	Norwegen
'NL'	Niederlande
'P'	Portugal
'PL'	Polen
'RO'	Rumänien
'RSM'	San Marino
'RUS'	Russische Föderation
'S'	Schweden
'SK'	Slowakei
'SLO'	Slowenien
'TM'	Turkmenistan
'TR'	Türkei
'UA'	Ukraine
'V'	Vatikanstadt
'YU'	Jugoslawien
'UNK'	Unbekannt
'EC'	Europäische Gemeinschaft
'EUR'	Übriges Europa
'WLD'	Übrige Welt.

2.72. NationNumeric

Numerische Bezeichnung eines Landes.

NationNumeric ::= INTEGER(0..255)

Wertzuweisung:

-- Keine Informationen verfügbar	(00) H,
-- Österreich	(01) H,
-- Albanien	(02) H,
-- Andorra	(03) H,
-- Armenien	(04) H,
-- Aserbaidshan	(05) H,
-- Belgien	(06) H,
-- Bulgarien	(07) H,
-- Bosnien und Herzegowina	(08) H,
-- Weißrussland	(09) H,
-- Schweiz	(0A) H,
-- Zypern	(0B) H,
-- Tschechische Republik	(0C) H,
-- Deutschland	(0D) H,
-- Dänemark	(0E) H,
-- Spanien	(0F) H,
-- Estland	(10) H,
-- Frankreich	(11) H,
-- Finnland	(12) H,
-- Liechtenstein	(13) H,
-- Färöer	(14) H,
-- Vereinigtes Königreich	(15) H,
-- Georgien	(16) H,
-- Griechenland	(17) H,
-- Ungarn	(18) H,
-- Kroatien	(19) H,
-- Italien	(1A) H,
-- Irland	(1B) H,
-- Island	(1C) H,

- - Kasachstan	(1D) H,
- - Luxemburg	(1E) H,
- - Litauen	(1F) H,
- - Lettland	(20) H,
- - Malta	(21) H,
- - Monaco	(22) H,
- - Republik Moldau	(23) H,
- - Mazedonien	(24) H,
- - Norwegen	(25) H,
- - Niederlande	(26) H,
- - Portugal	(27) H,
- - Polen	(28) H,
- - Rumänien	(29) H,
- - San Marino	(2A) H,
- - Russische Föderation	(2B) H,
- - Schweden	(2C) H,
- - Slowakei	(2D) H,
- - Slowenien	(2E) H,
- - Turkmenistan	(2F) H,
- - Türkei	(30) H,
- - Ukraine	(31) H,
- - Vatikanstadt	(32) H,
- - Jugoslawien	(33) H,
- - RFU	(34 . . FC) H,
- - Europäische Gemeinschaft	(FD) H,
- - Übriges Europa	(FE) H,
- - Übrige Welt	(FF) H

2.73. NoOfCalibrationRecords

Anzahl der Kalibrierungsdatensätze, die eine Werkstattkarte speichern kann.

NoOfCalibrationRecords ::= INTEGER(0..255)

Wertzuweisung: siehe Abschnitt 3.

2.74. NoOfCalibrationsSinceDownload

Zähler zur Angabe der mit einer Werkstattkarte seit dem letzten Herunterladen durchgeführten Kalibrierungen (Randnummer 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2¹⁶-1),

Wertzuweisung: nicht näher spezifiziert.

2.75. NoOfCardPlaceRecords

Anzahl der Ortsdatensätze, die eine Fahrer- oder Werkstattkarte speichern kann.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Wertzuweisung: siehe Abschnitt 3.

2.76. NoOfCardVehicleRecords

Anzahl der Angaben zu den gefahrenen Fahrzeugen enthaltenden Datensätze, die eine Fahrer- oder Werkstattkarte speichern kann.

NoOfCardVehicleRecords ::= INTEGER(0..2¹⁶-1)

Wertzuweisung: siehe Abschnitt 3.

2.77. NoOfCompanyActivityRecords

Anzahl der Unternehmenstätigkeitsdatensätze, die eine Unternehmenskarte speichern kann.

NoOfCompanyActivityRecords ::= INTEGER(0..2¹⁶-1)

Wertzuweisung: siehe Abschnitt 3.

2.78. NoOfControlActivityRecords

Anzahl der Kontrollaktivitätsdatensätze, die eine Kontrollkarte speichern kann.

NoOfControlActivityRecords ::= INTEGER(0..2¹⁶-1)

Wertzuweisung: siehe Abschnitt 3.

2.79. NoOfEventsPerType

Anzahl der Ereignisse je Ereignisart, die eine Karte speichern kann.

NoOfEventsPerType ::= INTEGER(0..255)

Wertzuweisung: siehe Abschnitt 3.

2.80. NoOfFaultsPerType

Anzahl der Störungen je Störungsart, die eine Karte speichern kann.

NoOfFaultsPerType ::= INTEGER(0..255)

Wertzuweisung: siehe Abschnitt 3.

2.81. OdometerValueMidnight

Kilometerstand des Fahrzeugs um Mitternacht am jeweiligen Tag (Randnummer 090).

OdometerValueMidnight ::= OdometerShort

Wertzuweisung: nicht näher spezifiziert.

2.82. OdometerShort

Kilometerstand des Fahrzeugs in Kurzform.

OdometerShort ::= INTEGER(0..2²⁴-1)

Wertzuweisung: Vorzeichenlose Binärzahl. Wert in km im Betriebsbereich 0 bis 9 999 999 km.

2.83. OverspeedNumber

Anzahl der Geschwindigkeitsüberschreitungen seit der letzten Kontrolle Geschwindigkeitsüberschreitung.

OverspeedNumber ::= INTEGER(0..255)

Wertzuweisung: 0 bedeutet, dass seit der letzten Kontrolle Geschwindigkeitsüberschreitung kein Ereignis Geschwindigkeitsüberschreitung aufgetreten ist, 1 bedeutet, dass 1 derartiges Ereignis seit der letzten entsprechenden Kontrolle aufgetreten ist, ... 255 bedeutet, dass 255 oder mehr derartige Ereignisse seit der letzten entsprechenden Kontrolle aufgetreten sind.

2.84. PlaceRecord

Informationen zum Ort des Beginns oder Endes des Arbeitstages (Randnummer 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
    entryTime                TimeReal,
    entryTypeDailyWorkPeriod EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry   NationNumeric,
    dailyWorkPeriodRegion    RegionNumeric,
    vehicleOdometerValue     OdometerShort
}
```

entryTime — auf die Eingabe bezogene Datums- und Zeitangabe.

entryTypeDailyWorkPeriod — Art der Eingabe.

dailyWorkPeriodCountry — eingegebenes Land.

dailyWorkPeriodRegion — eingegebene Region.

vehicleOdometerValue — Kilometerstand zum Zeitpunkt und am Ort der Eingabe.

2.85. PreviousVehicleInfo

Information zum zuvor von einem Fahrer gefahrenen Fahrzeug beim Einstecken seiner Karte in eine Fahrzeugeinheit (Randnummer 081).

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification      VehicleRegistrationIdentification,
    cardWithdrawalTime                    TimeReal
}
```

vehicleRegistrationIdentification — amtliches Kennzeichen und zulassender Mitgliedstaat des Fahrzeugs.

cardWithdrawalTime — Datum und Uhrzeit der Kartenentnahme.

2.86. PublicKey

Ein öffentlicher RSA-Schlüssel.

```
PublicKey ::= SEQUENCE {
    rsaKeyModulus                      RSAKeyModulus,
    rsaKeyPublicExponent               RSAKeyPublicExponent
}
```

rsaKeyModulus — Modulus des Schlüsselpaares.

rsaKeyPublicExponent — öffentlicher Exponent des Schlüsselpaares.

2.87. RegionAlpha

Alphabetische Angabe einer Region innerhalb eines bestimmten Landes.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Wertzuweisung:

' ' Keine Informationen verfügbar

Spanien:

'AN'	Andalucía
'AR'	Aragón
'AST'	Asturias
'C'	Cantabria
'CAT'	Cataluña
'CL'	Castilla-León
'CM'	Castilla-La-Mancha
'CV'	Valencia
'EXT'	Extremadura
'G'	Galicia
'IB'	Baleares
'IC'	Canarias
'LR'	La Rioja
'M'	Madrid
'MU'	Murcia
'NA'	Navarra
'PV'	País Vasco

2.88. RegionNumeric

Numerische Angabe einer Region innerhalb eines bestimmten Landes.

```
RegionNumeric ::= OCTET STRING(SIZE(1))
```

Wertzuweisung:

'00'H Keine Informationen verfügbar

Spanien:

'01'H Andalusía
 '02'H Aragón
 '03'H Asturias
 '04'H Cantabria
 '05'H Cataluña
 '06'H Castilla-León
 '07'H Castilla-La-Mancha
 '08'H Valencia
 '09'H Extremadura
 '0A'H Galicia
 '0B'H Baleares
 '0C'H Canarias
 '0D'H La Rioja
 '0E'H Madrid
 '0F'H Murcia
 '10'H Navarra
 '11'H País Vasco

2.89. RSAKeyModulus

Der Modulus eines RSA-Schlüsselpaares.

`RSAKeyModulus ::= OCTET STRING (SIZE(128))`

Wertzuweisung: nicht spezifiziert.

2.90. RSAKeyPrivateExponent

Privater Exponent eines RSA-Schlüsselpaares.

`RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))`

Wertzuweisung: nicht spezifiziert.

2.91. RSAKeyPublicExponent

Öffentlicher Exponent eines RSA-Schlüsselpaares.

`RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))`

Wertzuweisung: nicht spezifiziert.

2.92. SensorApprovalNumber

Bauartgenehmigungsnummer des Weg- und/oder Geschwindigkeitsgebers.

`SensorApprovalNumber ::= IA5String(SIZE(8))`

Wertzuweisung: nicht spezifiziert.

2.93. SensorIdentification

In einem Weg- und/oder Geschwindigkeitsgeber gespeicherte Information zur Identifizierung des Weg- und/oder Geschwindigkeitsgebers (Randnummer 077).

```
SensorIdentification ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorSCIdentifier           SensorSCIdentifier,
    sensorOSIdentifier           SensorOSIdentifier
}
```


sensorSerialNumber — erweiterte Seriennummer des Weg- und/oder Geschwindigkeitsgebers (umfasst Teilnummer und Herstellercode).

sensorApprovalNumber — Bauartgenehmigungsnummer des Weg- und/oder Geschwindigkeitsgebers.

sensorSCIdentifier — Bezeichner der Sicherheitskomponente des Weg- und/oder Geschwindigkeitsgebers.

sensorOSIdentifier — Bezeichner des Betriebssystems des Weg- und/oder Geschwindigkeitsgebers.

2.94. SensorInstallation

In einem Weg- und/oder Geschwindigkeitsgeber gespeicherte Information zur Installation des Weg- und/oder Geschwindigkeitsgebers (Randnummer 099).

```
SensorInstallation ::= SEQUENCE {
    sensorPairingDateFirst          SensorPairingDate,
    firstVuApprovalNumber          VuApprovalNumber,
    firstVuSerialNumber            VuSerialNumber,
    sensorPairingDateCurrent       SensorPairingDate,
    currentVuApprovalNumber        VuApprovalNumber,
    currentVUSerialNumber          VuSerialNumber
}
```

sensorPairingDateFirst — Datum der ersten Koppelung des Weg- und/oder Geschwindigkeitsgebers mit einer Fahrzeugeinheit.

firstVuApprovalNumber — Bauartgenehmigungsnummer der ersten mit dem Weg- und/oder Geschwindigkeitsgeber gekoppelten Fahrzeugeinheit.

firstVuSerialNumber — Seriennummer der ersten mit dem Weg- und/oder Geschwindigkeitsgeber gekoppelten Fahrzeugeinheit.

sensorPairingDateCurrent — Datum der derzeitigen Koppelung des Weg- und/oder Geschwindigkeitsgebers mit der Fahrzeugeinheit.

currentVuApprovalNumber — Bauartgenehmigungsnummer der derzeit mit dem Weg- und/oder Geschwindigkeitsgeber gekoppelten Fahrzeugeinheit.

currentVUSerialNumber — Seriennummer der derzeit mit dem Weg- und/oder Geschwindigkeitsgeber gekoppelten Fahrzeugeinheit.

2.95. SensorInstallationSecData

Auf einer Werkstatkarte gespeicherte Information zu den für die Koppelung von Weg- und/oder Geschwindigkeitsgebern und Fahrzeugeinheiten benötigten Sicherheitsdaten (Randnummer 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Wertzuweisung: gemäß ISO 16844-3.

2.96. SensorOSIdentifier

Bezeichner des Betriebssystems des Weg- und/oder Geschwindigkeitsgebers.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Wertzuweisung: herstellerspezifisch.

2.97. SensorPaired

In einer Fahrzeugeinheit gespeicherte Information zur Identifizierung des mit der Fahrzeugeinheit gekoppelten Weg- und/oder Geschwindigkeitsgebers (Randnummer 079).

```
SensorPaired ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorPairingDateFirst      SensorPairingDate
}
```

sensorSerialNumber — Seriennummer des derzeit mit der Fahrzeugeinheit gekoppelten Weg- und/oder Geschwindigkeitsgebers.

sensorApprovalNumber — Bauartgenehmigungsnummer des derzeit mit der Fahrzeugeinheit gekoppelten Weg- und/oder Geschwindigkeitsgebers.

sensorPairingDateFirst — Datum der ersten Koppelung des derzeit mit der Fahrzeugeinheit gekoppelten Weg- und/oder Geschwindigkeitsgebers mit einer Fahrzeugeinheit.

2.98. **SensorPairingDate**

Datum einer Koppelung des Weg- und/oder Geschwindigkeitsgebers mit einer Fahrzeugeinheit.

`SensorPairingDate ::= TimeReal`

Wertzuweisung: nicht spezifiziert.

2.99. **SensorSerialNumber**

Seriennummer des Weg- und/oder Geschwindigkeitsgebers.

`SensorSerialNumber ::= ExtendedSerialNumber`

2.100. **SensorSCIdentifier**

Bezeichner der Sicherheitskomponente des Weg- und/oder Geschwindigkeitsgebers.

`SensorSCIdentifier ::= IA5String(SIZE(8))`

Wertzuweisung: Komponente herstellerspezifisch.

2.101. **Signature**

Eine digitale Signatur.

`Signature ::= OCTET STRING (SIZE(128))`

Wertzuweisung: gemäß Anlage 11, 'Gemeinsame Sicherheitsmechanismen'.

2.102. **SimilarEventsNumber**

Anzahl ähnlicher Ereignisse an einem bestimmten Tag (Randnummer 094).

`SimilarEventsNumber ::= INTEGER(0..255)`

Wertzuweisung: 0 wird nicht verwendet, 1 bedeutet, dass an diesem Tag nur ein Ereignis dieser Art aufgetreten und gespeichert wurde, 2 bedeutet, dass 2 Ereignisse dieser Art an diesem Tag aufgetreten sind (nur eines wurde gespeichert), ... 255 bedeutet, dass 255 oder mehr Ereignisse dieser Art an diesem Tag aufgetreten sind.

2.103. **SpecificConditionType**

Code zur Identifizierung einer spezifischen Bedingung (Randnummer 050b, 105a, 212a und 230a).

`SpecificConditionType ::= INTEGER(0..255)`

Wertzuweisung:

'00'H	RFU
'01'H	Kontrollgerät nicht erforderlich — Anfang
'02'H	Kontrollgerät nicht erforderlich — Ende
'03'H	Fährüberfahrt/Zugfahrt
'04'H .. 'FF'H	RFU

2.104. **SpecificConditionRecord**

Auf einer Fahrerkarte, einer Werkstattkarte oder in einer Fahrzeugeinheit gespeicherte Information zu einer spezifischen Bedingung (Randnummer 105a, 212a und 230a).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                TimeReal,
    specificConditionType    SpecificConditionType
}
```

entryTime — Datum und Uhrzeit der Eingabe.

specificConditionType — Code zur Identifizierung der spezifischen Bedingung.

2.105. Speed

Fahrzeuggeschwindigkeit (km/h).

```
Speed ::= INTEGER(0..255)
```

Wertzuweisung: Kilometer pro Stunde im Betriebsbereich 0 bis 220 km/h.

2.106. SpeedAuthorised

Zulässige Höchstgeschwindigkeit des Fahrzeugs (Begriffsbestimmung bb)).

```
SpeedAuthorised ::= Speed
```

2.107. SpeedAverage

Durchschnittsgeschwindigkeit in einem vorher festgelegten Zeitraum (km/h).

```
SpeedAverage ::= Speed
```

2.108. SpeedMax

Höchstgeschwindigkeit in einem vorher festgelegten Zeitraum.

```
SpeedMax ::= Speed
```

2.109. TDesSessionKey

Ein Triple-DES-Sitzungsschlüssel.

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA                OCTET STRING (SIZE(8))
    tDesKeyB                OCTET STRING (SIZE(8))
}
```

Wertzuweisung: nicht näher spezifiziert.

2.110. TimeReal

Code für ein kombiniertes Datum/Uhrzeit-Feld, in dem Datum und Uhrzeit als Sekunden nach dem 1. Januar 1970 00h.00m.00s. GMT ausgedrückt sind.

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

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

Höchst mögliche(s) Datum/Uhrzeit ist im Jahr 2106.

2.111. TyreSize

Bezeichnung der Reifenabmessungen.

```
TyreSize ::= IA5String(SIZE(15))
```

Wertzuweisung: gemäß Richtlinie 92/23/EWG.

noOfVuCalibrationRecords — Anzahl der in der vuCalibrationRecords-Menge enthaltenen Datensätze.

vuCalibrationRecords — Menge der Kalibrierungsdatensätze.

2.118. VuCalibrationRecord

In einer Fahrzeugeinheit gespeicherte Information zu einer Kalibrierung des Kontrollgeräts (Randnummer 098).

```
VuCalibrationRecord ::= SEQUENCE {
    calibrationPurpose          CalibrationPurpose,
    workshopName                Name,
    workshopAddress             Address,
    workshopCardNumber          FullCardNumber,
    workshopCardExpiryDate      TimeReal,
    vehicleIdentificationNumber VehicleIdentificationNumber,
    vehicleRegistrationIdentification VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment K-ConstantOfRecordingEquipment,
    lTyreCircumference          L-TyreCircumference,
    tyreSize                    TyreSize,
    authorisedSpeed              SpeedAuthorised,
    oldOdometerValue            OdometerShort,
    newOdometerValue            OdometerShort,
    oldTimeValue                 TimeReal,
    newTimeValue                 TimeReal,
    nextCalibrationDate          TimeReal
}
```

calibrationPurpose — Zweck der Kalibrierung.

workshopName, workshopAddress — Name und Anschrift der Werkstatt.

workshopCardNumber dient der Identifizierung der zur Kalibrierung verwendeten Werkstattkarte.

workshopCardExpiryDate — Ablaufdatum der Karte.

vehicleIdentificationNumber — Fahrzeugidentifizierungsnummer (VIN).

vehicleRegistrationIdentification enthält das amtliche Kennzeichen und den zulassenden Mitgliedstaat.

wVehicleCharacteristicConstant — Wegdrehzahl des Fahrzeugs.

kConstantOfRecordingEquipment — Kontrollgerätkonstante.

lTyreCircumference — tatsächlicher Reifenumfang.

tyreSize — Bezeichnung der Größe der am Fahrzeug montierten Reifen.

authorisedSpeed — zulässige Geschwindigkeit des Fahrzeugs.

oldOdometerValue, newOdometerValue — alter und neuer Kilometerstand.

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

nextCalibrationDate — Datum der nächsten von der zugelassenen Prüfstelle durchzuführenden Kalibrierung der in CalibrationPurpose angegebenen Art.

2.119. VuCardIWDData

In einer Fahrzeugeinheit gespeicherte Information zu Einsteck- und Entnahmevorgängen von Fahrerkarten oder Werkstattkarten in der Fahrzeugeinheit (Randnummer 081).

```
VuCardIWDData ::= SEQUENCE {
    noOfIWRecords              INTEGER(0..216-1),
    vuCardIWRecords SET        SIZE(noOfIWRecords) OF
                                VuCardIWRecord
}
```

noOfIWRecords — Anzahl der Datensätze in der Menge vuCardIWRecords.

vuCardIWRecords — Datensätze zu Einsteck- und Entnahmevorgängen von Karten.

2.120. VuCardIWRecord

In einer Fahrzeugeinheit gespeicherte Information zu einem Einsteck- und Entnahmevorgang einer Fahrerkarte oder Werkstattkarte in der Fahrzeugeinheit (Randnummer 081).

```
VuCardIWRecord ::= SEQUENCE {
    cardHolderName                HolderName,
    fullCardNumber                FullCardNumber,
    cardExpiryDate                TimeReal,
    cardInsertionTime              TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber                CardSlotNumber,
    cardWithdrawalTime            TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo            PreviousVehicleInfo
    manualInputFlag                ManualInputFlag
}
```

cardHolderName — Name und Vorname(n) des Inhabers der Fahrer- oder Werkstattkarte in der auf der Karte gespeicherten Form.

fullCardNumber — Art der Karte, ausstellender Mitgliedstaat und Kartenummer in der auf der Karte gespeicherten Form.

cardExpiryDate — Ablaufdatum der Karte in der auf der Karte gespeicherten Form.

cardInsertionTime — Datum und Uhrzeit des Einsteckens.

vehicleOdometerValueAtInsertion — Kilometerstand des Fahrzeugs beim Einstecken der Karte.

cardSlotNumber — Steckplatz, in dem die Karte eingesteckt ist.

cardWithdrawalTime — Datum und Uhrzeit der Entnahme der Karte.

vehicleOdometerValueAtWithdrawal — Kilometerstand des Fahrzeugs bei Kartenentnahme.

previousVehicleInfo enthält Informationen zum zuvor vom Fahrer gefahrenen Fahrzeug in der auf der Karte gespeicherten Form.

manualInputFlag — Merker, der angibt, ob der Karteninhaber beim Einstecken der Karte Fahrtätigkeiten manuell eingegeben hat.

2.121. VuCertificate

Zertifikat des öffentlichen Schlüssels einer Fahrzeugeinheit.

```
VuCertificate ::= Certificate
```

2.122. VuCompanyLocksData

In einer Fahrzeugeinheit gespeicherte Information zu Unternehmenssperrern (Randnummer 104).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks                    INTEGER(0..20),
    vuCompanyLocksRecords        SET SIZE(noOfLocks) OF
                                VuCompanyLocksRecord
}
```

noOfLocks — Anzahl der in vuCompanyLocksRecords aufgeführten Sperren.

vuCompanyLocksRecords — Datensätze mit Informationen zur Unternehmenssperrern.

2.123. VuCompanyLocksRecord

In einer Fahrzeugeinheit gespeicherte Information zu einer Unternehmenssperrung (Randnummer 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime                TimeReal,
    lockOutTime               TimeReal,
    companyName               Name,
    companyAddress            Address,
    companyCardNumber         FullCardNumber
}
```

lockInTime, lockOutTime — Datum und Uhrzeit der Sperrung und Entsperrung.

companyName, companyAddress — Name und Anschrift des Unternehmens, auf das sich die Sperrung bezieht.

companyCardNumber — Identifizierung der bei der Sperrung verwendeten Karte.

2.124. VuControlActivityData

In einer Fahrzeugeinheit gespeicherte Information zu unter Verwendung dieser FE ausgeführten Kontrollen (Randnummer 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls               INTEGER(0..20),
    vuControlActivityRecords   SET SIZE(noOfControls) OF
                               VuControlActivityRecord
}
```

noOfControls — Anzahl der in vuControlActivityRecords aufgeführten Kontrollen.

vuControlActivityRecords — Kontrollaktivitätsdatensätze.

2.125. VuControlActivityRecord

In einer Fahrzeugeinheit gespeicherte Information zu einer unter Verwendung dieser FE ausgeführten Kontrolle (Randnummer 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType               ControlType,
    controlTime               TimeReal,
    controlCardNumber         FullCardNumber,
    downloadPeriodBeginTime   TimeReal,
    downloadPeriodEndTime     TimeReal
}
```

controlType — Art der Kontrolle.

controlTime — Datum und Uhrzeit der Kontrolle.

ControlCardNumber — Identifizierung der für die Kontrolle verwendeten Kontrollkarte.

downloadPeriodBeginTime — Anfangszeit des heruntergeladenen Zeitraums beim Herunterladen.

downloadPeriodEndTime — Endzeit des heruntergeladenen Zeitraums beim Herunterladen.

2.126. VuDataBlockCounter

Auf einer Karte gespeicherter Zähler, der sequentiell die Einsteck- und Entnahmevergänge der Karte in Fahrzeugeinheiten angibt.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Wertzuweisung: Laufende Nummer mit Höchstwert 9 999, danach wieder Beginn bei 0.

2.127. VuDetailedSpeedBlock

In einer Fahrzeugeinheit gespeicherte Information zur genauen Geschwindigkeit des Fahrzeugs während einer Minute, in der sich das Fahrzeug bewegt hat (Randnummer 093).

```

VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate          TimeReal,
    speedsPerSecond              SEQUENCE SIZE (60) OF Speed
}

```

speedBlockBeginDate — Datum und Uhrzeit des ersten Geschwindigkeitswertes innerhalb des Blocks.

speedsPerSecond — chronologische Reihenfolge der gemessenen Geschwindigkeiten zu jeder Sekunde der Minute, beginnend mit speedBlockBeginDate.

2.128. VuDetailedSpeedData

In einer Fahrzeugeinheit gespeicherte Information zur genauen Geschwindigkeit des Fahrzeugs.

```

VuDetailedSpeedData ::= SEQUENCE {
    noOfSpeedBlocks              INTEGER (0..216-1),
    vuDetailedSpeedBlocks        SET SIZE (noOfSpeedBlocks) OF
                                VuDetailedSpeedBlock
}

```

noOfSpeedBlocks — Anzahl der Geschwindigkeitsblöcke in der Menge vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks — Menge der genauen Geschwindigkeitsblöcke.

2.129. VuDownloadablePeriod

Ältestes und jüngstes Datum, für das eine Fahrzeugeinheit Daten zu Fahrtätigkeiten enthält (Randnummer 081, 084 oder 087).

```

VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime          TimeReal
    maxDownloadableTime          TimeReal
}

```

minDownloadableTime — ältestes in der FE gespeichertes Datum des Einsteckens der Karte, einer Tätigkeitsänderung oder einer Ortseingabe und Angabe der entsprechenden Uhrzeit.

maxDownloadableTime — jüngstes in der FE gespeichertes Datum des Einsteckens der Karte, einer Tätigkeitsänderung oder einer Ortseingabe und Angabe der entsprechenden Uhrzeit.

2.130. VuDownloadActivityData

In einer Fahrzeugeinheit gespeicherte Information zu ihrem letzten Herunterladen (Randnummer 105).

```

VuDownloadActivityData ::= SEQUENCE {
    downloadingTime              TimeReal,
    fullCardNumber                FullCardNumber,
    companyOrWorkshopName         Name
}

```

downloadingTime — Datum und Uhrzeit des Herunterladens

fullCardNumber identifiziert die zur Genehmigung des Herunterladens verwendete Karte.

companyOrWorkshopName — Name des Unternehmens oder der Werkstatt.

2.131. VuEventData

In einer Fahrzeugeinheit gespeicherte Information zu Ereignissen (Randnummer 094, mit Ausnahme Ereignis Geschwindigkeitsüberschreitung).

```

VuEventData ::= SEQUENCE {
    noOfVuEvents                 INTEGER (0..255),
    vuEventRecords               SET SIZE (noOfVuEvents) OF VuEventRecord
}

```

noOfVuEvents — Anzahl der in den vuEventRecords aufgeführten Ereignisse.

vuEventRecords — Ereignisdatensätze.

2.132. VuEventRecord

In einer Fahrzeugeinheit gespeicherte Information zu einem Ereignis (Randnummer 094, mit Ausnahme Ereignis Geschwindigkeitsüberschreitung).

```
VuEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose       EventFaultRecordPurpose,
    eventBeginTime           TimeReal,
    eventEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd  FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber,
    similarEventsNumber     SimilarEventsNumber
}
```

eventType — Art des Ereignisses.

eventRecordPurpose — Zweck der Aufzeichnung dieses Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

cardNumberDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesetzte Karte.

cardNumberCodriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz 2. Fahrer eingesetzte Karte.

cardNumberDriverSlotEnd identifiziert die am Ende des Ereignisses im Steckplatz Fahrer eingesetzte Karte.

cardNumberCodriverSlotEnd identifiziert die am Ende des Ereignisses im Steckplatz 2. Fahrer eingesetzte Karte.

similarEventsNumber — Anzahl ähnlicher Ereignisse an diesem Tag.

Diese Folge kann für alle Ereignisse mit Ausnahme von Geschwindigkeitsüberschreitungen verwendet werden.

2.133. VuFaultData

In einer Fahrzeugeinheit gespeicherte Information zu Störungen (Randnummer 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults                INTEGER(0..255),
    vuFaultRecords SET          SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults — Anzahl der in der Menge vuFaultRecords aufgeführten Störungen.

vuFaultRecords — Störungsdatensätze.

2.134. VuFaultRecord

In einer Fahrzeugeinheit gespeicherte Information zu einer Störung (Randnummer 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                EventFaultType,
    faultRecordPurpose       EventFaultRecordPurpose,
    faultBeginTime           TimeReal,
    faultEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd  FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber
}
```

faultType — Art der Kontrollgerätstörung.

faultRecordPurpose — Zweck der Aufzeichnung dieser Störung.

faultBeginTime — Datum und Uhrzeit des Störungsbeginns.

faultEndTime — Datum und Uhrzeit des Störungsendes.

cardNumberDriverSlotBegin identifiziert die zu Beginn der Störung im Steckplatz Fahrer eingesetzte Karte.

cardNumberCodriverSlotBegin identifiziert die zu Beginn der Störung im Steckplatz 2. Fahrer eingesetzte Karte.

cardNumberDriverSlotEnd identifiziert die zum Zeitpunkt des Endes der Störung im Steckplatz Fahrer eingesetzte Karte.

cardNumberCodriverSlotEnd identifiziert die zum Zeitpunkt des Endes der Störung im Steckplatz 2. Fahrer eingesetzte Karte.

2.135. VuIdentification

In einer Fahrzeugeinheit gespeicherte Information zur Identifizierung der Fahrzeugeinheit (Randnummer 075).

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName          VuManufacturerName,
    vuManufacturerAddress      VuManufacturerAddress,
    vuPartNumber               VuPartNumber,
    vuSerialNumber             VuSerialNumber,
    vuSoftwareIdentification    VuSoftwareIdentification,
    vuManufacturingDate        VuManufacturingDate,
    vuApprovalNumber           VuApprovalNumber
}
```

vuManufacturerName — Name des Herstellers der Fahrzeugeinheit.

vuManufacturerAddress — Anschrift des Herstellers der Fahrzeugeinheit.

vuPartNumber — Teilnummer der Fahrzeugeinheit.

vuSerialNumber — Seriennummer der Fahrzeugeinheit.

vuSoftwareIdentification identifiziert die in der Fahrzeugeinheit implementierte Software.

vuManufacturingDate — Herstellungsdatum der Fahrzeugeinheit.

vuApprovalNumber — Bauartgenehmigungsnummer der Fahrzeugeinheit.

2.136. VuManufacturerAddress

Anschrift des Herstellers der Fahrzeugeinheit.

```
VuManufacturerAddress ::= Address
```

Wertzuweisung: nicht spezifiziert.

2.137. VuManufacturerName

Name des Herstellers der Fahrzeugeinheit.

```
VuManufacturerName ::= Name
```

Wertzuweisung: nicht spezifiziert.

2.138. VuManufacturingDate

Herstellungsdatum der Fahrzeugeinheit.

```
VuManufacturingDate ::= TimeReal
```

Wertzuweisung: nicht spezifiziert.

2.139. VuOverSpeedingControlData

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Geschwindigkeitsüberschreitung seit der letzten Kontrolle Geschwindigkeitsüberschreitung (Randnummer 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince        OverspeedNumber
}
```

lastOverspeedControlTime — Datum und Uhrzeit der letzten Kontrolle Geschwindigkeitsüberschreitung.

firstOverspeedSince — Datum und Uhrzeit der ersten Geschwindigkeitsüberschreitung nach dieser Kontrolle Geschwindigkeitsüberschreitung.

numberOfOverspeedSince — Anzahl der Ereignisse Geschwindigkeitsüberschreitung seit der letzten Kontrolle Geschwindigkeitsüberschreitung.

2.140. VuOverSpeedingEventData

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Geschwindigkeitsüberschreitung (Randnummer 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents      INTEGER(0..255),
    vuOverSpeedingEventRecords    SET SIZE(noOfVuOverSpeedingEvents) OF
                                   VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents — Anzahl der in der Menge vuOverSpeedingEventRecords aufgeführten Ereignisse.

vuOverSpeedingEventRecords — Ereignisdatensätze Geschwindigkeitsüberschreitung.

2.141. VuOverSpeedingEventRecord

In einer Fahrzeugeinheit gespeicherte Information zum Ereignis Geschwindigkeitsüberschreitung (Randnummer 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                     EventFaultType,
    eventRecordPurpose            EventFaultRecordPurpose,
    eventBeginTime                TimeReal,
    eventEndTime                  TimeReal,
    maxSpeedValue                 SpeedMax,
    averageSpeedValue             SpeedAverage,
    cardNumberDriverSlotBegin     FullCardNumber,
    similarEventsNumber           SimilarEventsNumber
}
```

eventType — Art des Ereignisses.

eventRecordPurpose — Zweck der Aufzeichnung dieses Ereignisses.

eventBeginTime — Datum und Uhrzeit des Ereignisbeginns.

eventEndTime — Datum und Uhrzeit des Ereignisendes.

maxSpeedValue — die während des Ereignisses gemessene Höchstgeschwindigkeit.

averageSpeedValue — die während des Ereignis gemessene arithmetische Durchschnittsgeschwindigkeit.

cardNumberDriverSlotBegin identifiziert die zu Beginn des Ereignisses im Steckplatz Fahrer eingesetzte Karte.

similarEventsNumber — Anzahl ähnlicher Ereignisse an diesem Tag.

2.142. VuPartNumber

Teilnummer der Fahrzeugeinheit.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Wertzuweisung: Herstellerspezifisch.

2.143. VuPlaceDailyWorkPeriodData

In einer Fahrzeugeinheit gespeicherte Information zum Ort des Beginns und/oder Endes des Arbeitstages (Randnummer 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
    noOfPlaceRecords                INTEGER(0..255),
    vuPlaceDailyWorkPeriodRecords   SET SIZE(noOfPlaceRecords) OF
                                    VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords — Anzahl der in der Menge vuPlaceDailyWorkPeriodRecords aufgeführten Datensätze.

vuPlaceDailyWorkPeriodRecords — ortsbezogene Datensätze.

2.144. VuPlaceDailyWorkPeriodRecord

In einer Fahrzeugeinheit gespeicherte Information zu einem Ort des Beginns oder Endes des Arbeitstages eines Fahrers (Randnummer 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumber                  FullCardNumber,
    placeRecord                     PlaceRecord
}
```

fullCardNumber — Art der Karte des Fahrers, ausstellender Mitgliedstaat und Kartenummer.

placeRecord enthält die Informationen zum eingegebenen Ort.

2.145. VuPrivateKey

Der private Schlüssel einer Fahrzeugeinheit.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Der öffentliche Schlüssel einer Fahrzeugeinheit.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Seriennummer der Fahrzeugeinheit (Randnummer 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Installationsdatum der FE-Softwareversion.

```
VuSoftInstallationDate ::= TimeReal
```

Wertzuweisung: nicht spezifiziert.

2.149. VuSoftwareIdentification

In einer Fahrzeugeinheit gespeicherte Information zur installierten Software.

```
VuSoftwareIdentification ::= SEQUENCE {
    vuSoftwareVersion                VuSoftwareVersion,
    vuSoftInstallationDate            VuSoftInstallationDate
}
```

vuSoftwareVersion — Softwareversionsnummer der Fahrzeugeinheit.

vuSoftInstallationDate — Installationsdatum der Softwareversion.

2.150. VuSoftwareVersion

Softwareversionsnummer der Fahrzeugeinheit.

VuSoftwareVersion ::= IA5String(SIZE(4))

Wertzuweisung: nicht spezifiziert.

2.151. VuSpecificConditionData

In einer Fahrzeugeinheit gespeicherte Information zu spezifischen Bedingungen.

```
VuSpecificConditionData ::= SEQUENCE {
    noOfSpecificConditionRecords          INTEGER(0..216-1)
    specificConditionRecords              SET SIZE (noOfSpecificConditionRecords) OF
                                          SpecificConditionRecord
}
```

noOfSpecificConditionRecords — Anzahl der in der Menge specificConditionRecords aufgeführten Datensätze.

specificConditionRecords — Datensätze mit Bezug auf spezifische Bedingungen.

2.152. VuTimeAdjustmentData

In einer Fahrzeugeinheit gespeicherte Information zu Zeiteinstellungen außerhalb einer normalen Kalibrierung (Randnummer 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords                 INTEGER(0..6),
    vuTimeAdjustmentRecords              SET SIZE (noOfVuTimeAdjRecords) OF
                                          VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords — Anzahl der in der Menge vuTimeAdjustmentRecords aufgeführten Datensätze.

vuTimeAdjustmentRecords — Zeiteinstellungsdatensätze.

2.153. VuTimeAdjustmentRecord

In einer Fahrzeugeinheit gespeicherte Information zu einer Zeiteinstellung außerhalb einer normalen Kalibrierung (Randnummer 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                         TimeReal,
    oldTimeValue                         TimeReal,
    newTimeValue                         TimeReal,
    workshopName                         Name,
    workshopAddress                      Address,
    workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

workshopName, workshopAddress — Name und Anschrift der Werkstatt.

workshopCardNumber identifiziert die für die Durchführung der Zeiteinstellung verwendete Werkstattkarte.

2.154. W-VehicleCharacteristicConstant

Wegdrehzahl des Fahrzeugs (Begriffsbestimmung k)).

W-VehicleCharacteristicConstant ::= INTEGER(0..2¹⁶-1)

Wertzuweisung: Impulse je Kilometer im Betriebsbereich 0 bis 64 255 Imp/km.

2.155. WorkshopCardApplicationIdentification

Auf einer Werkstattkarte gespeicherte Information zur Identifizierung der Anwendung der Karte (Randnummer 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType            NoOfEventsPerType,
    noOfFaultsPerType           NoOfFaultsPerType,
    activityStructureLength      CardActivityLengthRange,
    noOfCardVehicleRecords      NoOfCardVehicleRecords,
    noOfCardPlaceRecords        NoOfCardPlaceRecords,
    noOfCalibrationRecords      NoOfCalibrationRecords
}
```

typeOfTachographCardId gibt die implementierte Kartenart an.

cardStructureVersion gibt die Version der auf der Karte implementierten Struktur an.

noOfEventsPerType — Anzahl der Ereignisse je Ereignisart, die die Karte speichern kann.

noOfFaultsPerType — Anzahl der Störungen je Störungsart, die die Karte speichern kann.

activityStructureLength gibt die Zahl der Bytes an, die für die Speicherung von Tätigkeitsdatensätzen zur Verfügung stehen.

noOfCardVehicleRecords — Anzahl der Fahrzeugdatensätze, die die Karte enthalten kann.

noOfCardPlaceRecords — Anzahl der Orte, die die Karte aufzeichnen kann.

noOfCalibrationRecords — Anzahl der Kalibrierungsdatensätze, die die Karte speichern kann.

2.156. WorkshopCardCalibrationData

Auf einer Werkstattkarte gespeicherte Information zur mit der Karte durchgeführten Werkstatttätigkeit (Randnummer 227 und 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber      INTEGER(0..216-1),
    calibrationPointerNewestRecord INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords          SET SIZE(NoOfCalibrationRecords) OF
                                WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber — Gesamtzahl der mit der Karte durchgeführten Kalibrierungen.

calibrationPointerNewestRecord — Index des zuletzt aktualisierten Kalibrierungsdatensatzes.

Wertzuweisung: Zahl, die dem Zähler des Kalibrierungsdatensatzes entspricht, beginnend mit ,0' für das erste Auftreten der Kalibrierungsdatensätze in der Struktur.

calibrationRecords — Datensätze mit Informationen zu Kalibrierung und/oder Zeiteinstellung.

2.157. WorkshopCardCalibrationRecord

Auf einer Werkstattkarte gespeicherte Information zu einer mit der Karte durchgeführten Kalibrierung (Randnummer 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    calibrationPurpose          CalibrationPurpose,
    vehicleIdentificationNumber VehicleIdentificationNumber,
    vehicleRegistration         VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment K-ConstantOfRecordingEquipment,
    lTyreCircumference         L-TyreCircumference,
    tyreSize                   TyreSize,
}
```

authorisedSpeed	SpeedAuthorised,
oldOdometerValue	OdometerShort,
newOdometerValue	OdometerShort,
oldTimeValue	TimeReal,
newTimeValue	TimeReal,
nextCalibrationDate	TimeReal,
vuPartNumber	VuPartNumber,
vuSerialNumber	VuSerialNumber,
sensorSerialNumber	SensorSerialNumber

}

calibrationPurpose — Zweck der Kalibrierung.

vehicleIdentificationNumber — Fahrzeugidentifizierungsnummer (VIN).

vehicleRegistration enthält das amtliche Kennzeichen und den zulassenden Mitgliedstaat.

wVehicleCharacteristicConstant — Wegdrehzahl des Fahrzeugs.

kConstantOfRecordingEquipment — Kontrollgerätkonstante.

lTyreCircumference — tatsächlicher Reifenumfang.

tyreSize — Bezeichnung der Größe der am Fahrzeug montierten Reifen.

authorisedSpeed — zulässige Geschwindigkeit des Fahrzeugs.

oldOdometerValue, newOdometerValue — alter und neuer Kilometerstand.

oldTimeValue, newTimeValue — alter und neuer Wert für Datum und Uhrzeit.

nextCalibrationDate — Datum der nächsten von der zugelassenen Prüfstelle durchzuführenden Kalibrierung der in CalibrationPurpose angegebenen Art.

vuPartNumber, vuSerialNumber und **sensorSerialNumber** — Datenelemente zur Identifizierung des Kontrollgeräts.

2.158. WorkshopCardHolderIdentification

Auf einer Werkstattkarte gespeicherte Information zur Identifizierung des Karteninhabers (Randnummer 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName                Name,
    workshopAddress              Address,
    cardHolderName               HolderName,
    cardHolderPreferredLanguage  Language
}
```

workshopName — Name der Werkstatt des Karteninhabers.

workshopAddress — Anschrift der Werkstatt des Karteninhabers.

cardHolderName — Name und Vorname(n) des Inhabers (z. B. Name des Mechanikers).

cardHolderPreferredLanguage — Muttersprache des Karteninhabers.

2.159. WorkshopCardPIN

PIN-Code (Personal Identification Number) der Werkstattkarte (Randnummer 213).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Wertzuweisung: Der dem Karteninhaber bekannte PIN-Code, nach rechts mit ‚FF‘-Bytes bis zu 8 Bytes aufgefüllt.

3. DEFINITIONEN FÜR WERT- UND GRÖSSENBEREICHE

Definition variabler Werte, die für die Definitionen in Abschnitt 2 verwendet werden.

TimeRealRange ::= $2^{32}-1$

3.1. Definitionen für die Fahrerkarte:

Name des variablen Wertes	Min.	Max.
CardActivityLengthRange	5 544 Bytes (28 Tage 93 Tätigkeitsänderungen pro Tag)	13 776 Bytes (28 Tage 240 Tätigkeitsänderungen pro Tag)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Definitionen für die Werkstattkarte:

Name des variablen Wertes	Min.	Max.
CardActivityLengthRange	198 Bytes (1 Tag 93 Tätigkeitsänderungen pro Tag)	492 Bytes (1 Tag 240 Tätigkeitsänderungen)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Definitionen für die Kontrollkarte:

Name des variablen Wertes	Min.	Max.
NoOfControlActivityRecords	230	520

3.4. Definitionen für die Unternehmenskarte:

Name des variablen Wertes	Min.	Max.
NoOfCompanyActivityRecords	230	520

4. ZEICHENSÄTZE

In den IA5Strings werden die ASCII-Zeichen laut Definition in ISO/IEC 8824-1 verwendet. Aus Gründen der Lesbarkeit und zur Bezugnahme ist die Wertzuweisung nachfolgend angegeben. Bei Diskrepanzen mit dieser zu Informationszwecken aufgeführten Angabe gilt stets die Norm ISO/IEC 8824-1.

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Andere Zeichenfolgen (Anschrift, Name, amtliches Kennzeichen) verwenden darüber hinaus die Zeichen, die in den Codes 192 bis 255 der ISO/IEC 8859-1 (Zeichensatz Lateinisch 1) bzw. ISO/IEC 8859-7 (Zeichensatz Griechisch) definiert sind.

5. KODIERUNG

Bei Kodierung anhand der ASN.1-Kodierungsregeln werden alle Datentypen gemäß ISO/IEC 8825-2 (ausgerichtet) kodiert.

Anlage 2

SPEZIFIKATION DER KONTROLLGERÄTKARTEN

INHALTSVERZEICHNIS

1.	Einleitung	99
1.1.	Abkürzungen	99
1.2.	Referenzdokumente	100
2.	Elektrische und physikalische Eigenschaften	100
2.1.	Versorgungsspannung und Stromverbrauch	100
2.2.	Programmierspannung V_{pp}	101
2.3.	Taktversorgung und -frequenz	101
2.4.	E/A-Kontakt	101
2.5.	Kartenzustände	101
3.	Hardware und Datenaustausch	101
3.1.	Einleitung	101
3.2.	Übertragungsprotokoll	101
3.2.1.	Protokolle	101
3.2.2.	ATR	102
3.2.3.	PTS	103
3.3.	Zugriffsbedingungen (AC)	103
3.4.	Datenverschlüsselung	104
3.5.	Befehle und Fehlercodes — Übersicht	104
3.6.	Beschreibung der Befehle	105
3.6.1.	Select File	105
3.6.1.1.	Auswahl nach Namen (AID)	105
3.6.1.2.	Auswahl einer Elementardatei anhand ihrer Dateikennung	106
3.6.2.	Read Binary	106
3.6.2.1.	Befehl ohne Secure Messaging	107
3.6.2.2.	Befehl mit Secure Messaging	107
3.6.3.	Update Binary	109
3.6.3.1.	Befehl ohne Secure Messaging	109
3.6.3.2.	Befehl mit Secure Messaging	110
3.6.4.	Get Challenge	111
3.6.5.	Verify	111
3.6.6.	Get Response	112
3.6.7.	PSO: Verify Certificate	112
3.6.8.	Internal Authenticate	113

3.6.9.	External Authenticate	114
3.6.10.	Manage Security Environment	115
3.6.11.	PSO: Hash	116
3.6.12.	Perform Hash of File	116
3.6.13.	PSO: Compute Digital Signature	117
3.6.14.	PSO: Verify Digital Signature	118
4.	Struktur der Kontrollgerätarten	118
4.1.	Struktur der Fahrerkarte	119
4.2.	Struktur der Werkstattkarte	121
4.3.	Struktur der Kontrollkarte	123
4.4.	Struktur der Unternehmenskarte	125

1. EINLEITUNG

1.1. Abkürzungen

Im Sinne dieser Anlage gelten folgende Abkürzungen:

AC	Access conditions (Zugriffsbedingungen)
AID	Application Identifier (Anwendungskennung)
ALW	Always (immer)
APDU	Application Protocol Data Unit (Befehlsstruktur)
ATR	Answer To Reset (Antwort auf Zurücksetzen)
AUT	Authenticated (authentisiert)
C6, C7	Kontakte Nr. 6 und 7 der Karte laut Beschreibung in ISO/IEC 7816-2
cc	Taktgeberzyklen
CHV	Card holder Verification Information (Information zur Überprüfung des Karteninhabers)
CLA	Klassenbyte eines APDU-Befehls
DF	Dedicated File (Verzeichnis). Ein DF kann andere Verzeichnisse oder Dateien enthalten (EF oder DF)
EF	Elementary File (Elementardatei)
ENC	Verschlüsselt: Zugriff nur durch Datenkodierung möglich
etu	elementary time unit (Elementarzeiteinheit)
IC	Integrated Circuit (Integrierter Schaltkreis)
ICC	Integrated Circuit Card (Chipkarte)
ID	Identifier (Bezeichner, Kennung)
IFD	Interface Device (Schnittstellengerät, Kartenterminal)
IFS	Information Field Size (Informationsfeldgröße)
IFSC	Informationsfeldgröße der Karte
IFSD	Informationsfeldgröße des Terminals
INS	Befehlsbyte eines APDU-Befehls
Lc	Länge der Eingabedaten für einen APDU-Befehl
Le	Länge der erwarteten Daten (Ausgabedaten für einen Befehl)
MF	Master File (Wurzel-DF)
P1-P2	Parameterbytes
NAD	Knotenadresse, verwendet im Protokoll T=1
NEV	Never (nie)
PIN	Personal Identification Number
PRO SM	Mit Secure Messaging geschützt
PTS	Protocol Transmission Selection (Auswahl der Protokollübertragung)
RFU	Reserved for Future Use (für künftige Anwendungen reserviert)

RST	Zurücksetzen (der Karte)
SM	Secure Messaging
SW1-SW2	Statusbytes
TS	ATR-Anfangszeichen
VPP	Programmierspannung
XXh	Wert XX in Hexadezimalnotation
	Verkettungssymbol 03 04=0304

1.2. Referenzdokumente

In dieser Anlage werden folgende Referenzdokumente herangezogen:

EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Identifikationskartensysteme — Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke — Teil 3: Applikationsunabhängige Anforderungen an die Karte)
ISO/CEI 7816-2	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999. (Informationstechnik — Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 2: Abmessungen und Lokalisierung der Kontakte)
ISO/CEI 7816-3	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997. (Informationstechnik — Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 3: Elektronische Eigenschaften und Übertragungsprotokolle)
ISO/CEI 7816-4	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997. (Informationstechnik — Identifikationskarten — Identifikationskarten mit integrierten Schaltkreisen und Kontakten — Teil 4: Interindustrielle Kommandos)
ISO/CEI 7816-6	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998. (Informationstechnik — Identifikationskarten mit integrierten Schaltkreisen und Kontakten — Teil 6: Interindustrielle Datenelemente)
ISO/CEI 7816-8	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First Edition: 1999. (Informationstechnik — Identifizierungskarten — Chipkarten mit Kontakten — Teil 8: Interindustrielle sicherheitsbezogene Kommandos)
ISO/CEI 9797	Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994. (Informationstechnik — IT-Sicherheitsverfahren — Codes zur Erkennung von Nachrichtenveränderungen (MACs) — Teil 1: Mechanismen auf Basis eines Blockschlüssel-Algorithmus)

2. ELEKTRISCHE UND PHYSIKALISCHE EIGENSCHAFTEN

TCS_200 Sofern nicht anderweitig spezifiziert, erfüllen alle elektronischen Signale die Norm ISO/IEC 7816-3.

TCS_201 Lage und Abmessungen der Kartenkontakte erfüllen die Norm ISO/IEC 7816-2.

2.1. Versorgungsspannung und Stromverbrauch

TCS_202 Die Karte arbeitet gemäß Spezifikation innerhalb der Grenzen für die Leistungsaufnahme nach ISO/IEC 7816-3.

TCS_203 Die Karte arbeitet mit $V_{cc} = 3 \text{ V } (+/- 0,3 \text{ V})$ oder mit $V_{cc} = 5 \text{ V } (+/- 0,5 \text{ V})$.

Die Spannungswahl erfolgt gemäß ISO/IEC 7816-3.

2.2. Programmierspannung V_{pp}

- TCS_204 Die Karte benötigt am Kontakt C6 keine Programmierspannung. Es wird davon ausgegangen, dass Kontakt C6 in einem Schnittstellengerät nicht angeschlossen ist. Der Kontakt C6 kann an V_{cc} auf der Karte angeschlossen sein, aber nicht an Masse. Auf jeden Fall ist diese Spannung nicht zu interpretieren.

2.3. Taktversorgung und -frequenz

- TCS_205 Die Karte arbeitet im Frequenzbereich von 1 bis 5 MHz. Innerhalb eines Kartenvorgangs darf die Taktfrequenz um $\pm 2\%$ schwanken. Die Taktfrequenz wird von der Fahrzeugeinheit und nicht von der Karte selbst erzeugt. Für den Arbeitszyklus ist eine Schwankung zwischen 40 und 60 % zulässig.
- TCS_206 Unter den in der Kartendatei EF_{ICC} enthaltenen Bedingungen kann der externe Taktgeber angehalten werden. Das erste Byte des Hauptteils der EF_{ICC} -Datei kodiert die Bedingungen für den Clockstop-Modus (nähere Einzelheiten siehe EN 726-3):

L-Pegel	H-Pegel		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop zulässig, kein Vorzugspegel
0	1	1	Clockstop zulässig, Vorzugspegel: H
1	0	1	Clockstop zulässig, Vorzugspegel: L
0	0	0	Clockstop nicht zulässig
0	1	0	Clockstop nur bei H-Pegel zulässig
1	0	0	Clockstop nur bei L-Pegel zulässig

Bits 4 bis 8 werden nicht genutzt.

2.4. E/A-Kontakt

- TCS_207 Der E/A-Kontakt C7 wird für den Empfang von Daten vom Schnittstellengerät und das Senden von Daten zum Schnittstellengerät verwendet. Während des Betriebs befindet sich entweder die Karte oder das Schnittstellengerät im Sendemodus. Sollten sich beide Einheiten im Sendemodus befinden, darf die Karte dadurch nicht beschädigt werden. Sofern die Karte nicht sendet, tritt sie in den Empfangsmodus.

2.5. Kartenzustände

- TCS_208 Bei angelegter Versorgungsspannung arbeitet die Karte in zwei Zuständen:

- im Betriebszustand während der Ausführung von Befehlen oder während der Verbindung zur Digitaleinheit,
- im Ruhezustand zu allen anderen Zeiten; in diesem Zustand bleiben alle Daten auf der Karte erhalten.

3. HARDWARE UND DATENAUSTAUSCH

3.1. Einleitung

Dieser Abschnitt beschreibt die für die Kontrollgerätkarten und Fahrzeugeinheit (FE) erforderliche Mindestfunktionalität, mit der ein korrekter Betrieb und Interoperabilität gewährleistet werden.

Kontrollgerätkarten erfüllen so weit wie möglich die geltenden ISO/IEC-Normen (insbesondere ISO/IEC 7816). Befehle und Protokolle werden jedoch vollständig beschrieben, um gegebenenfalls bestimmte eingeschränkte Verwendungen oder Unterschiede herauszustellen. Die spezifizierten Befehle entsprechen, sofern nicht anders angegeben, in vollem Umfang den angeführten Normen.

3.2. Übertragungsprotokoll

- TCS_300 Das Übertragungsprotokoll entspricht den Festlegungen von ISO/IEC 7816-3. Insbesondere erkennt die FE von der Karte gesendete Wartezeitverlängerungen.

3.2.1. Protokolle

- TCS_301 Die Karte unterstützt sowohl Protokoll T=0 als auch Protokoll T=1.

TCS_302 T=0 ist das Standardprotokoll; zum Wechsel auf das Protokoll T=1 ist daher ein PTS-Befehl erforderlich.

TCS_303 Die Geräte unterstützen in beiden Protokollen die ‚direct convention‘, die somit für die Karte obligatorisch ist.

TCS_304 Das Byte für die Informationsfeldgröße der Karte wird im ATR im Zeichen TA3 dargestellt. Dieser Wert beträgt mindestens ‚F0h‘ (= 240 Byte).

Für die Protokolle gelten die folgenden Einschränkungen:

TCS_305 T=0

- Das Schnittstellengerät unterstützt eine Antwort bei E/A nach der ansteigenden Flanke des Signals bei RST von 400 cc.
- Das Schnittstellengerät muss Zeichen im Abstand von 12 etu lesen können.
- Das Schnittstellengerät liest ein fehlerhaftes Zeichen und dessen Wiederholung, wenn der Abstand 13 etu beträgt. Wird ein fehlerhaftes Zeichen festgestellt, kann das Fehlersignal bei E/A zwischen 1 etu und 2 etu auftreten. Das Gerät unterstützt eine Verzögerung von 1 etu.
- Das Schnittstellengerät akzeptiert ein ATR von 33 Byte (TS+32).
- Befindet sich TC1 im ATR, ist für vom Schnittstellengerät gesendete Zeichen die Extra Guard Time vorhanden, obwohl von der Karte gesendete Zeichen weiterhin mit 12 etu getrennt werden können. Dies gilt auch für das von der Karte gesendete ACK-Zeichen nach Aussendung eines P3-Zeichens vom Schnittstellengerät.
- Das Schnittstellengerät berücksichtigt ein von der Karte ausgesendetes NUL-Zeichen.
- Das Schnittstellengerät akzeptiert den Ergänzungsmodus für ACK.
- Der Befehl GET RESPONSE kann im Verkettungsmodus nicht zum Einholen von Daten verwendet werden, deren Länge 255 Byte übersteigen könnte.

TCS_306 T=1

- NAD-Byte: nicht verwendet (NAD ist auf ‚00‘ gesetzt).
- S-Block ABORT: nicht verwendet.
- S-Block VPP-Zustandsfehler: nicht verwendet.
- Die Gesamtverkettungslänge für ein Datenfeld darf 255 Byte (vom Schnittstellengerät abzusichern) nicht übersteigen.
- Die Informationsfeldgröße des Schnittstellengeräts (IFSD) wird vom Schnittstellengerät unmittelbar nach dem ATR angezeigt: Das Schnittstellengerät überträgt die S-Block IFS-Anforderung nach dem ATR, und die Karte sendet S-Block IFS zurück. Der empfohlene Wert für IFSD ist 254 Byte.
- Die Karte fordert keine IFS-Nachkorrektur an.

3.2.2. **ATR**

TCS_307 Das Gerät überprüft ATR-Bytes gemäß ISO/IEC 7816-3. Es erfolgt keine Überprüfung von historischen ATR-Zeichen.

Beispiel für ein Zweiprotokoll-Basis-ATR gemäß ISO/IEC 7816-3

Zeichen	Wert	Bemerkungen
TS	‚3Bh‘	Anzeiger für ‚direct convention‘
T0	‚85h‘	TD1 vorhanden; 5 historische Bytes vorhanden
TD1	‚80h‘	TD2 vorhanden; T=0 verwenden
TD2	‚11h‘	TA3 vorhanden; T=1 verwenden
TA3	‚XXh‘ (mind. ‚F0h‘)	Informationsfeldgröße der Karte (IFSC)
TH1 bis TH5	‚XXh‘	Historische Zeichen
TCK	‚XXh‘	Prüfzeichen (ohne OR)

TCS_308 Nach der Antwort auf das Zurücksetzen (ATR) wird das Wurzelverzeichnis (MF) implizit ausgewählt und zum aktuellen Verzeichnis.

3.2.3. PTS

TCS_309 Das Standardprotokoll ist T=0. Zur Einstellung des Protokolls T=1 muss ein PTS (auch PPS genannt) vom Gerät gesendet werden.

TCS_310 Da für die Karte beide Protokolle, T=0 und T=1, obligatorisch sind, ist das Basis-PTS für die Protokollumschaltung ebenfalls obligatorisch.

Wie in ISO/IEC 7816-3 angegeben, kann das PTS zur Umschaltung auf höhere Übertragungsraten als die von der Karte im ATR vorgeschlagene Geschwindigkeit verwendet werden (TA(1) Byte).

Höhere Übertragungsraten sind für die Karte fakultativ.

TCS_311 Wird keine andere Übertragungsrate als die Standardgeschwindigkeit unterstützt (oder wird die ausgewählte Übertragungsrate nicht unterstützt), antwortet die Karte auf das PTS korrekt gemäß ISO/IEC 7816-3 durch Weglassen des PPS1-Byte.

Beispiele für ein Basis-PTS zur Protokollwahl:

Zeichen	Wert	Bemerkungen
PPSS	,FFh'	Startzeichen
PPS0	,00h' oder ,01h'	PPS1 bis PPS3 nicht vorhanden; ,00h' zur Auswahl von T0, ,01h' zur Auswahl von T1
PK	,XXh'	Prüfzeichen: ,XXh' = ,FFh' wenn PPS0 = ,00h' ,XXh' = ,FEh' wenn PPS0 = ,01h'

3.3. Zugriffsbedingungen (AC)

Für jede Elementardatei sind Zugriffsbedingungen (AC) für die Befehle UPDATE BINARY und READ BINARY festgelegt.

TCS_312 Vor dem Zugriff auf die aktuelle Datei müssen deren AC erfüllt werden.

Die Definitionen der verfügbaren Zugriffsbedingungen lauten wie folgt:

- ALW: Die Aktion ist immer möglich und kann ohne Einschränkung ausgeführt werden.
- NEV: Die Aktion ist nie möglich.
- AUT: Das Zugriffsrecht, das einer erfolgreichen externen Authentisierung entspricht, muss eröffnet werden (durch den Befehl EXTERNAL AUTHENTICATE).
- PRO SM: Befehl muss mit einer kryptografischen Prüfsumme unter Verwendung von Secure Messaging übertragen werden (siehe Anlage 11).
- AUT und PRO SM (kombiniert).

Mit den Verarbeitungsbefehlen (UPDATE BINARY und READ BINARY) können die folgenden Zugriffsbedingungen auf der Karte gesetzt werden:

	UPDATE BINARY	READ BINARY
ALW	Ja	Ja
NEV	Ja	Ja
AUT	Ja	Ja
PRO SM	Ja	Nein
AUT und PRO SM	Ja	Nein

Die Zugriffsbedingung PRO SM steht für den Befehl READ BINARY nicht zur Verfügung. Das bedeutet, dass das Vorhandensein einer kryptografischen Prüfsumme für einen READ-Befehl nie obligatorisch ist. Unter Verwendung des Wertes ,OC' für die Klasse ist es jedoch möglich, wie im Abschnitt 3.6.2 beschrieben wird, den Befehl READ BINARY mit Secure Messaging zu benutzen.

3.4. Datenverschlüsselung

Wenn die Vertraulichkeit von aus einer Datei auszulesenden Daten geschützt werden muss, wird die Datei als ‚verschlüsselt‘ gekennzeichnet. Die Verschlüsselung erfolgt mit Hilfe von Secure Messaging (siehe Anlage 11).

3.5. Befehle und Fehlercodes — Übersicht

Befehle und Dateiorganisation sind von der ISO/IEC 7816-4 abgeleitet und erfüllen diese Norm.

TCS_313 Dieser Abschnitt beschreibt die folgenden APDU-Befehl-Antwort-Paare:

Befehl	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 In jeder Antwortnachricht werden die Statusbytes SW1 SW2 zurückgesendet, die den Verarbeitungszustand des Befehls bezeichnen.

SW1	SW2	Bedeutung
90	00	Normale Verarbeitung
61	XX	Normale Verarbeitung. XX = Zahl der verfügbaren Antwortbytes
62	81	Verarbeitungswarnung. Ein Teil der zurückgesendeten Daten kann beschädigt sein
63	CX	Falsche CHV (PIN). Zähler für verbleibende Versuche ‚X‘
64	00	Ausführungsfehler — Zustand des nichtflüchtigen Speichers unverändert. Integritätsfehler
65	00	Ausführungsfehler — Zustand des nichtflüchtigen Speichers verändert
65	81	Ausführungsfehler — Zustand des nichtflüchtigen Speichers verändert — Speicherfehler
66	88	Sicherheitsfehler: falsche kryptografische Prüfsumme (bei Secure Messaging) oder falsches Zertifikat (bei Zertifikatsverifizierung) oder falsches Kryptogramm (bei externer Authentisierung) oder falsche Signatur (bei Signaturverifizierung)
67	00	Falsche Länge (falsche Lc oder Le)
69	00	Verbotener Befehl (keine Antwort verfügbar in T=0)
69	82	Sicherheitsstatus nicht erfüllt
69	83	Authentisierungsverfahren blockiert
69	85	Nutzungsbedingungen nicht erfüllt
69	86	Befehl nicht zulässig (keine aktuelle EF)
69	87	Erwartete Secure-Messaging-Datenobjekte fehlen
69	88	Inkorrekte Secure-Messaging-Datenobjekte
6A	82	Datei nicht gefunden
6A	86	Falsche Parameter P1-P2
6A	88	Bezugsdaten nicht gefunden
6B	00	Falsche Parameter (Offset außerhalb der EF)

SW1	SW2	Bedeutung
6C	XX	Falsche Länge, SW2 gibt die genaue Länge an. Kein Datenfeld wird zurückgesendet
6D	00	Befehlscode nicht unterstützt oder ungültig
6E	00	Klasse nicht unterstützt
6F	00	Sonstige Prüffehler

3.6. Beschreibung der Befehle

In diesem Kapitel werden die obligatorischen Befehle für die Kontrollgerätkarten beschrieben.

Weitere sachdienliche Einzelheiten zu kryptografischen Operationen sind in Anlage 11, Gemeinsame Sicherheitsmechanismen, aufgeführt.

Alle Befehle werden unabhängig vom verwendeten Protokoll (T=0 oder T=1) beschrieben. Die APDU-Bytes CLA, INS, P1, P2, Lc und Le werden immer angegeben. Wird Lc oder Le für den beschriebenen Befehl nicht benötigt, bleiben die entsprechende Länge, der Wert und die Beschreibung leer.

TCS_315 Werden beide Längenbytes (Lc und Le) angefordert, ist der Befehl in zwei Teile aufzuspalten, wenn das IFD das Protokoll T=0 verwendet: Das IFD sendet den Befehl wie beschrieben mit P3=Lc + Daten und sendet dann einen GET RESPONSE-Befehl (siehe Abschnitt 3.6.6) bei P3=Le.

TCS_316 Wenn beide Längenbytes angefordert werden und wenn Le=0 (Secure Messaging) gilt Folgendes:

- Bei Verwendung von Protokoll T=1 antwortet die Karte auf Le=0 mit dem Senden aller verfügbaren Ausgabedaten.
- Bei Verwendung von Protokoll T=0 sendet das IFD den ersten Befehl mit P3=Lc + Daten und die Karte antwortet auf dieses implizierte Le=0 mit den Statusbytes '61La', wobei La die Anzahl der verfügbaren Antwortbytes ist. Daraufhin generiert das IFD einen GET RESPONSE-Befehl mit P3=La zum Lesen der Daten.

3.6.1. *Select File*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4; seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl SELECT FILE wird verwendet:

- zur Auswahl eines Applikations-DF (Auswahl nach Namen obligatorisch)
- zur Auswahl einer Elementardatei, die der vorgelegten Datei-ID entspricht.

3.6.1.1. *Auswahl nach Namen (AID)*

Dieser Befehl ermöglicht die Auswahl eines Applikations-DF auf der Karte.

TCS_317 Dieser Befehl kann von jeder beliebigen Stelle in der Dateistruktur aus ausgeführt werden (nach dem ATR oder jederzeit).

TCS_318 Bei Auswahl einer Anwendung wird die derzeitige Sicherheitsumgebung zurückgesetzt. Nach Auswahl der Anwendung wird kein aktueller öffentlicher Schlüssel mehr ausgewählt, und der frühere Sitzungsschlüssel steht nicht mehr für das Secure Messaging zur Verfügung. Die Zugriffsbedingung AUT geht ebenfalls verloren.

TCS_319 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Auswahl nach Namen (AID)
P2	1	'0Ch'	Keine Antwort erwartet
Lc	1	'NNh'	Anzahl der an die Karte gesendeten Bytes (Länge der AID): '06h' für die Kontrollgerätanwendung
#6—#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' für die Kontrollgerätanwendung

Es wird keine Antwort auf den Befehl SELECT FILE benötigt (Le fehlt in T=1, oder keine Antwort angefordert in T=0).

TCS_320 Antwortnachricht (keine Antwort angefordert)

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Wird die der AID entsprechende Anwendung nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus ,6A82'.
- Bei Vorhandensein des Bytes Le lautet in T=1 der zurückgesendete Status ,6700'.
- Wenn nach dem Befehl SELECT FILE eine Antwort angefordert wird, lautet in T=0 der zurückgesendete Status ,6900'.
- Wird die ausgewählte Anwendung als verfälscht betrachtet (weil in den Dateiattributen ein Integritätsfehler festgestellt wurde), lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

3.6.1.2. Auswahl einer Elementardatei anhand ihrer Dateikennung

TCS_321 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	
INS	1	,A4h'	
P1	1	,02h'	Auswahl einer EF unter dem aktuellen DF
P2	1	,0Ch'	Keine Antwort erwartet
Lc	1	,02h'	Anzahl der an die Karte gesendeten Bytes
#6—#7	2	,XXXXh'	Dateikennung

Es wird keine Antwort auf den Befehl SELECT FILE benötigt (Le fehlt in T=1, oder keine Antwort angefordert in T=0).

TCS_322 Antwortnachricht (keine Antwort angefordert)

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Wird die der AID entsprechende Anwendung nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus ,6A82'.
- Bei Vorhandensein des Bytes Le lautet in T=1 der zurückgesendete Status ,6700'.
- Wenn nach dem Befehl SELECT FILE eine Antwort angefordert wird, lautet in T=0 der zurückgesendete Status ,6900'.
- Wird die ausgewählte Anwendung als verfälscht betrachtet (weil in den Dateiattributen ein Integritätsfehler festgestellt wurde), lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

3.6.2. **Read Binary**

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4; seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl Read Binary wird zum Auslesen von Daten aus einer transparenten Datei verwendet.

Die Antwort der Karte besteht im Zurücksenden der gelesenen Daten, die optional in einer Secure-Messaging-Struktur eingekapselt werden können.

TCS_323 Der Befehl kann nur ausgeführt werden, wenn der Sicherheitsstatus den für die EF für die READ-Funktion festgelegten Sicherheitsattributen genügt.

3.6.2.1. Befehl ohne Secure Messaging

Dieser Befehl ermöglicht dem IFD das Lesen von Daten aus der zu dem entsprechenden Zeitpunkt ausgewählten EF ohne Secure Messaging.

TCS_324 Das Lesen aus einer als verschlüsselt gekennzeichneten Datei darf mit diesem Befehl nicht möglich sein.

TCS_325 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	Kein Secure Messaging angefordert
INS	1	,B0h'	
P1	1	,XXh'	Offset in Bytes vom Dateianfang: höchstwertiges Byte
P2	1	,XXh'	Offset in Bytes vom Dateianfang: niedrigstwertiges Byte
Le	1	,XXh'	Erwartete Datenlänge. Anzahl der zu lesenden Bytes

Anmerkung: Bit 8 von P1 muss auf 0 gesetzt sein.

TCS_326 Antwortnachricht

Byte	Länge	Wert	Beschreibung
#1—#X	X	,XX..XXh'	Gelesene Daten
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Ist keine EF ausgewählt, lautet der zurückgesendete Verarbeitungsstatus ,6986'.
- Sind die Zugangsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit ,6982' unterbrochen.
- Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus ,6B00'.
- Ist die Größe der auszulesenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe) lautet der zurückgesendete Verarbeitungsstatus ,6700' oder ,6Cxx', wobei ,xx' die genaue Länge angibt.
- Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wieder herstellbar und der zurückgesendete Verarbeitungsstatus lautet ,6400' oder ,6581'.
- Wird in den gespeicherten Daten ein Integritätsfehler festgestellt, so gibt die Karte die angeforderten Daten aus und der zurückgesendete Verarbeitungsstatus lautet ,6281'.

3.6.2.2. Befehl mit Secure Messaging

Dieser Befehl ermöglicht dem IFD das Lesen von Daten aus der zu dem entsprechenden Zeitpunkt ausgewählten EF mit Secure Messaging, um die Integrität der empfangenen Daten zu überprüfen und die Vertraulichkeit der Daten bei als verschlüsselt gekennzeichneten EF zu schützen.

TCS_327 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,0Ch'	Secure Messaging angefordert
INS	1	,B0h'	INS
P1	1	,XXh'	P1 (Offset in Bytes vom Dateianfang): höchstwertiges Byte
P2	1	,XXh'	P2 (Offset in Bytes vom Dateianfang): niedrigstwertiges Byte
Lc	1	,09h'	Länge der Eingabedaten für Secure Messaging
#6	1	,97h'	T _{LE} : Tag zur Spezifikation der erwarteten Länge
#7	1	,01h'	L _{LE} : Erwartete Länge
#8	1	,NNh'	Spezifikation der erwarteten Länge (Original Le): Anzahl der zu lesenden Bytes

Byte	Länge	Wert	Beschreibung
#9	1	,8Eh'	T _{CC} : Tag für die kryptografische Prüfsumme
#10	1	,04h'	L _{CC} : Länge der folgenden kryptografischen Prüfsumme
#11—#14	4	,XX..XXh'	Kryptografische Prüfsumme (4 höchstwertige Bytes)
Le	1	,00h'	Gemäß Spezifikation in ISO/IEC 7816-4

TCS_328 Antwortnachricht, wenn EF nicht als verschlüsselt gekennzeichnet und wenn Secure-Messaging-Eingabeformat korrekt:

Byte	Länge	Wert	Beschreibung
#1	1	,81h'	T _{PV} : Tag für Klarwertdaten
#2	L	,NNh' oder ,81 NNh'	L _{PV} : Länge der zurückgesendeten Daten (= Original Le) L gleich 2 Byte, wenn L _{PV} > 127 Byte
#(2+L)—#(1+L+NN)	NN	,XX..XXh'	Klardenwert
#(2+L+NN)	1	,8Eh'	T _{CC} : Tag für kryptografische Prüfsumme
#(3+L+NN)	1	,04h'	L _{CC} : Länge der folgenden kryptografischen Prüfsumme
#(4+L+NN)—#(7+L+NN)	4	,XX..XXh'	Kryptografische Prüfsumme (4 höchstwertige Bytes)
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

TCS_329 Antwortnachricht, wenn EF als verschlüsselt gekennzeichnet und wenn Secure-Messaging-Eingabeformat korrekt:

Byte	Länge	Wert	Beschreibung
#1	1	,87h'	T _{PI CG} : Tag für verschlüsselte Daten (Kryptogramm)
#2	L	,MMh' oder ,81 MMh'	L _{PI CG} : Länge der zurückgesendeten verschlüsselten Daten (wegen Auffüllung anders als Original-Le des Befehls) L gleich 2 Byte, wenn L _{PI CG} > 127 Byte
#(2+L)—#(1+L+MM)	MM	,01XX..XXh'	Verschlüsselte Daten: Auffüllindikator und Kryptogramm
#(2+L+MM)	1	,8Eh'	T _{CC} : Tag für kryptografische Prüfsumme
#(3+L+MM)	1	,04h'	L _{CC} : Länge der folgenden kryptografischen Prüfsumme
#(4+L+MM)—#(7+L+MM)	4	,XX..XXh'	Kryptografische Prüfsumme (4 höchstwertige Bytes)
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

Die zurückgesendeten verschlüsselten Daten enthalten ein erstes Byte, das den verwendeten Auffüllmodus angibt. Für die Kontrollgerätenwendung nimmt der Auffüllindikator stets den Wert ,01h' an und zeigt damit an, dass der verwendete Auffüllmodus dem Modus in ISO/IEC 7816-4 entspricht (ein Byte mit Wert ,80h', gefolgt von einigen Nullbytes: ISO/IEC 9797 Methode 2).

Die für den Befehl READ BINARY ohne Secure Messaging beschriebenen ,regulären' Verarbeitungszustände (siehe Abschnitt 3.6.2.1), können unter Verwendung der oben aufgeführten Antwortnachrichtstrukturen zurückgesendet werden.

Darüber hinaus können einige Fehler speziell im Zusammenhang mit Secure Messaging auftreten. In diesem Fall wird der Verarbeitungsstatus einfach ohne Secure-Messaging-Struktur zurückgesendet:

TCS_330 Antwortnachricht bei inkorrektem Secure-Messaging-Eingabeformat

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist kein aktueller Sitzungsschlüssel vorhanden, wird der Verarbeitungsstatus ,6A88' zurückgesendet. Dies geschieht entweder, wenn der Sitzungsschlüssel noch nicht erzeugt wurde oder wenn dessen Gültigkeit abgelaufen ist (in diesem Fall muss das IFD erneut eine gegenseitige Authentisierung durchführen, um einen neuen Sitzungsschlüssel zu setzen).
- Wenn im Secure-Messaging-Format einige erwartete Datenobjekte (siehe oben) fehlen, wird der Verarbeitungsstatus ,6987' zurückgesendet. Dieser Fehler tritt auf, wenn ein erwartetes Tag fehlt oder wenn der Befehlskörper nicht den Anforderungen entsprechend aufgebaut ist.

- Sind Datenobjekte nicht korrekt, lautet der zurückgesendete Verarbeitungsstatus ‚6988‘. Dieser Fehler tritt auf, wenn zwar alle benötigten Tags vorhanden sind, einige Längen sich jedoch von den erwarteten unterscheiden.
- Schlägt die Überprüfung der kryptografischen Prüfsumme fehl, lautet der zurückgesendete Verarbeitungsstatus ‚6688‘.

3.6.3. Update Binary

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4; seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Die Befehlsnachricht UPDATE BINARY initiiert die Aktualisierung (erase + write) der bereits in einer EF-Binärzahl vorhandenen Bits mit den im APDU-Befehl gegebenen Bits.

TCS_331 Der Befehl kann nur ausgeführt werden, wenn der Sicherheitsstatus den für die EF für die UPDATE-Funktion festgelegten Sicherheitsattributen genügt (wenn die Zugangskontrolle der UPDATE-Funktion PRO SM enthält, muss im Befehl ein Secure Messaging hinzugefügt werden).

3.6.3.1. Befehl ohne Secure Messaging

Dieser Befehl ermöglicht dem IFD das Schreiben von Daten in die zu dem entsprechenden Zeitpunkt ausgewählte EF, ohne dass die Karte die Integrität der empfangenen Daten überprüft. Dieser Klarmodus ist nur dann zulässig, wenn die entsprechende Datei nicht als verschlüsselt gekennzeichnet ist.

TCS_332 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	‚00h‘	Kein Secure Messaging angefordert
INS	1	‚D6h‘	Offset in Bytes vom Dateianfang: höchstwertiges Byte
P1	1	‚XXh‘	
P2	1	‚XXh‘	
Lc	1	‚NNh‘	Lc Länge der zu aktualisierenden Daten. Anzahl der zu schreibenden Bytes
#6—#(5+NN)	NN	‚XX..XXh‘	Zu schreibende Daten

Anmerkung: Bit 8 von P1 muss auf 0 gesetzt sein.

TCS_333 Antwortnachricht

Byte	Länge	Wert	Beschreibung
SW	2	‚XXXXh‘	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ‚9000‘ zurück.
- Ist keine EF ausgewählt, lautet der zurückgesendete Verarbeitungsstatus ‚6986‘.
- Sind die Zugriffsbedingungen der ausgewählten Dateien nicht erfüllt, wird der Befehl mit ‚6982‘ abgebrochen.
- Ist das Offset nicht mit der Größe der EF kompatibel (Offset > EF-Größe), lautet der zurückgesendete Verarbeitungsstatus ‚6B00‘.
- Ist die Größe der auszulesenden Daten nicht mit der Größe der EF kompatibel (Offset + Le > EF-Größe) lautet der zurückgesendete Verarbeitungsstatus ‚6700‘.
- Wird in den Dateiattributen ein Integritätsfehler festgestellt, so betrachtet die Karte die Datei als beschädigt und nicht wieder herstellbar und der zurückgesendete Verarbeitungsstatus lautet ‚6400‘ oder ‚6500‘.
- Schlägt der Schreibvorgang fehl, so lautet der zurückgesendete Verarbeitungsstatus ‚6581‘.

3.6.3.2. Befehl mit Secure Messaging

Dieser Befehl ermöglicht dem IFD das Schreiben von Daten in die zu dem entsprechenden Zeitpunkt ausgewählte EF, wobei die Karte die Integrität der empfangenen Daten überprüft. Da keine Vertraulichkeit erforderlich ist, werden die Daten nicht verschlüsselt.

TCS_334 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,0Ch'	Secure Messaging angefordert
INS	1	,D6h'	INS
P1	1	,XXh'	Offset in Bytes vom Dateianfang: höchstwertiges Byte
P2	1	,XXh'	Offset in Bytes vom Dateianfang: niedrigstwertiges Byte
Lc	1	,XXh'	Länge des gesicherten Datenfeldes
#6	1	,81h'	T _{PV} : Tag für Klarwertdaten
#7	L	,NNh' oder ,81 NNh'	L _{PV} : Länge der übermittelten Daten L gleich 2 Byte, wenn L _{PV} > 127 Byte
#(7+L)—#(6+L+NN)	NN	,XX.XXh'	Klardenwert (zu schreibende Daten)
#(7+L+NN)	1	,8Eh'	T _{CC} : Tag für die kryptografische Prüfsumme
#(8+L+NN)	1	,04h'	L _{CC} : Länge der folgenden kryptografischen Prüfsumme
#(9+L+NN)—#(12+L+NN)	4	,XX.XXh'	Kryptografische Prüfsumme (4 höchstwertige Bytes)
Le	1	,00h'	Gemäß Spezifikation in ISO/IEC 7816-4

TCS_335 Antwortnachricht bei korrektem Secure-Messaging-Eingabeformat

Byte	Länge	Wert	Beschreibung
#1	1	,99h'	T _{SW} : Tag für Statusbytes (durch CC zu schützen)
#2	1	,02h'	L _{SW} : Länge der zurückgesendeten Statusbytes
#3—#4	2	,XXXXh'	Statusbytes (SW1, SW2)
#5	1	,8Eh'	T _{CC} : Tag für die kryptografische Prüfsumme
#6	1	,04h'	L _{CC} : Länge der folgenden kryptografischen Prüfsumme
#7—#10	4	,XX.XXh'	Kryptografische Prüfsumme (4 höchstwertige Bytes)
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

Die für den Befehl UPDATE BINARY ohne Secure Messaging beschriebenen ‚regulären‘ Verarbeitungszustände (siehe Abschnitt 3.6.3.1) können unter Verwendung der oben aufgeführten Antwortnachrichtstrukturen zurückgesendet werden.

Darüber hinaus können einige Fehler speziell im Zusammenhang mit Secure Messaging auftreten. In diesem Fall wird der Verarbeitungsstatus einfach ohne Secure-Messaging-Struktur zurückgesendet:

TCS_336 Antwortnachricht bei Fehler im Secure Messaging

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist kein aktueller Sitzungsschlüssel vorhanden, wird der Verarbeitungsstatus ‚6A88‘ zurückgesendet.
- Wenn im Secure-Messaging-Format einige erwartete Datenobjekte (siehe oben) fehlen, wird der Verarbeitungsstatus ‚6987‘ zurückgesendet. Dieser Fehler tritt auf, wenn ein erwartetes Tag fehlt oder wenn der Befehlskörper nicht den Anforderungen entsprechend aufgebaut ist.
- Sind Datenobjekte nicht korrekt, so lautet der zurückgesendete Verarbeitungsstatus ‚6988‘. Dieser Fehler tritt auf, wenn zwar alle benötigten Tags vorhanden sind, einige Längen sich jedoch von den erwarteten unterscheiden.
- Schlägt die Überprüfung der kryptografischen Prüfsumme fehl, lautet der zurückgesendete Verarbeitungsstatus ‚6688‘.

3.6.4. *Get Challenge*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4; seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl GET CHALLENGE fordert die Karte zur Ausgabe einer Zufallszahl aus, damit diese in einem sicherheitsbezogenen Verfahren verwendet werden kann, bei dem ein Kryptogramm oder chiffrierte Daten an die Karte gesendet werden.

TCS_337 Die von der Karte ausgegebene Zufallszahl ist nur für den nächsten Befehl gültig, der eine an die Karte gesendete Zufallszahl verwendet.

TCS_338 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,84h'	INS
P1	1	,00h'	P1
P2	1	,00h'	P2
Le	1	,08h'	Le (erwartete Länge der Zufallszahl)

TCS_339 Antwortnachricht

Byte	Länge	Wert	Beschreibung
#1—#8	8	,XX..XXh'	Zufallszahl
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Unterscheidet sich Le von ,08h', ist der Verarbeitungsstatus ,6700'.
- Sind die Parameter P1-P2 inkorrekt, ist der Verarbeitungsstatus ,6A86'.

3.6.5. *Verify*

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl Verify leitet auf der Karte den Vergleich der vom Befehl gesendeten CHV (PIN)-Daten mit der auf der Karte gespeicherten Bezugs-CHV ein.

Anmerkung: Die vom Benutzer eingegebene PIN muss durch das IFD bis zu einer Länge von 8 Byte nach rechts mit ,FFh'-Bytes aufgefüllt sein.

TCS_340 Ist der Befehl erfolgreich, werden die der CHV-Präsentation entsprechenden Rechte freigegeben, und der Zähler für die verbleibenden CHV-Versuche wird reinitialisiert.

TCS_341 Ein erfolgloser Vergleich wird auf der Karte registriert, um die Anzahl weiterer Versuche der Verwendung der Bezugs-CHV zu beschränken.

TCS_342 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,20h'	INS
P1	1	,00h'	P1
P2	1	,00h'	P2 (die überprüfte CHV ist implizit bekannt)
Lc	1	,08h'	Länge des übertragenen CHV-Codes
#6—#13	8	,XX..XXh'	CHV

TCS_343 Antwortnachricht

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Wird die Bezugs-CHV nicht gefunden, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Ist die CHV blockiert (der Zähler für verbleibende Versuche steht auf Null), lautet der zurückgesendete Verarbeitungsstatus ,6983'. Wenn dieser Zustand erreicht ist, kann die CHV nie wieder erfolgreich präsentiert werden.
- Ist der Vergleich erfolglos, wird der Zähler für die verbleibenden Versuche herabgesetzt und der Status ,63CX' zurückgesendet ($X > 0$, und X ist gleich dem Zähler für verbleibende CHV-Versuche. Wenn $X = ,F'$, ist der Zähler für CHV-Versuche größer als ,F').
- Wird die Bezugs-CHV als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

3.6.6. **Get Response**

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4.

Dieser (nur für das Protokoll T=0 notwendige und verfügbare) Befehl wird zur Übertragung vorbereiteter Daten von der Karte zum Schnittstellengerät verwendet (wenn ein Befehl sowohl Lc als auch Le enthalten hat).

Der Befehl GET RESPONSE muss sofort nach dem Befehl zur Vorbereitung der Daten ausgegeben werden, sonst gehen die Daten verloren. Nach der Ausführung des Befehls GET RESPONSE (außer bei Auftreten der Fehler ,61xx' oder ,6Cxx', siehe unten) stehen die zuvor vorbereiteten Daten nicht mehr zur Verfügung.

TCS_344 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	
INS	1	,C0h'	
P1	1	,00h'	
P2	1	,00h'	
Le	1	,XXh'	Anzahl der erwarteten Bytes

TCS_345 Antwortnachricht

Byte	Länge	Wert	Beschreibung
#1—#X	X	,XX..XXh'	Daten
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Wurden von der Karte keine Daten vorbereitet, lautet der zurückgesendete Verarbeitungsstatus ,6900' oder ,6F00'.
- Übersteigt Le die Anzahl der verfügbaren Bytes oder ist Le gleich null, lautet der zurückgesendete Verarbeitungsstatus ,6Cxx', wobei ,xx' die genaue Anzahl der verfügbaren Bytes bezeichnet. In diesem Fall stehen die vorbereiteten Daten für einen weiteren Befehl GET RESPONSE zur Verfügung.
- Ist Le nicht null und kleiner als die Anzahl der verfügbaren Bytes, werden die angeforderten Daten normal von der Karte gesendet. Der zurückgesendete Verarbeitungsstatus lautet ,61xx', wobei ,xx' die Anzahl der zusätzlichen Bytes angibt, die noch für einen nachfolgenden Befehl GET RESPONSE zur Verfügung stehen.
- Wird der Befehl nicht unterstützt (Protokoll T=1), sendet die Karte ,6D00' zurück.

3.6.7. **PSO: Verify Certificate**

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-8, seine Verwendung ist jedoch im Vergleich zu dem in der Norm definierten Befehl eingeschränkt.

Der Befehl VERIFY CERTIFICATE wird von der Karte zur Einholung eines öffentlichen Schlüssels von außen und zur Prüfung seiner Gültigkeit verwendet.

TCS_346 Ist der Befehl VERIFY CERTIFICATE erfolgreich, wird der öffentliche Schlüssel zur künftigen Verwendung in der Sicherheitsumgebung gespeichert. Dieser Schlüssel wird explizit zur Verwendung in sicherheitsbezogenen Befehlen (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE oder VERIFY CERTIFICATE) durch den Befehl MSE (siehe Abschnitt 3.6.10) unter Verwendung seines Schlüsselbezeichners gesetzt.

TCS_347 Auf jeden Fall verwendet der Befehl VERIFY CERTIFICATE den zuvor vom Befehl MSE zur Eröffnung des Zertifikats ausgewählten öffentlichen Schlüssel. Dabei muss es sich um den öffentlichen Schlüssel eines Mitgliedstaates oder Europas handeln.

TCS_348 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,2Ah'	Perform Security Operation
P1	1	,00h'	P1
P2	1	,AEh'	P2: nicht BER-TLV-kodierte Daten (Verkettung von Datenelementen)
Lc	1	,CEh'	Lc: Länge des Zertifikats, 194 Byte
#6—#199	194	,XX..XXh'	Zertifikat: Verkettung von Datenelementen (entsprechend Beschreibung in Anlage 11)

TCS_349 Antwortnachricht

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Schlägt die Zertifikatsverifizierung fehl, lautet der zurückgesendete Verarbeitungsstatus ,6688'. Das Prüfungs- und Entpackungsverfahren für das Zertifikat wird in Anlage 11 beschrieben.
- Ist in der Sicherheitsumgebung kein öffentlicher Schlüssel vorhanden, wird ,6A88' zurückgesendet.
- Wird der (zum Entpacken des Zertifikats verwendete) ausgewählte öffentliche Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.
- Weist der (zum Entpacken des Zertifikats verwendete) öffentliche Schlüssel ein CHA.LSB (CertificateHolderAuthorisation.equipmentType) mit einem anderen Wert als ,00' auf (d. h. es ist der Schlüssel eines Mitgliedstaates oder Europas), so lautet der zurückgesendete Verarbeitungsstatus ,6985'.

3.6.8. Internal Authenticate

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4.

Mit Hilfe des Befehls INTERNAL AUTHENTICATE kann das IFD die Karte authentisieren.

Der Authentisierungsvorgang wird in Anlage 11 beschrieben. Er beinhaltet folgende Aussagen:

TCS_350 Der Befehl INTERNAL AUTHENTICATE verwendet den (implizit ausgewählten) privaten Kartenschlüssel zum Signieren von Authentisierungsdaten einschließlich K1 (erstes Element für die Sitzungsschlüsselvereinbarung) und RND1 und verwendet den aktuell (durch den letzten MSE-Befehl) ausgewählten öffentlichen Schlüssel zur Verschlüsselung der Signatur und zur Bildung des Authentisierungstokens (nähere Angaben in Anlage 11).

TCS_351 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,88h'	INS
P1	1	,00h'	P1
P2	1	,00h'	P2
Lc	1	,10h'	Länge der an die Karte gesendeten Daten
#6—#13	8	,XX..XXh'	Zufallszahl zur Authentisierung der Karte
#14—#21	8	,XX..XXh'	VU.CHR (siehe Anlage 11)
Le	1	,80h'	Länge der von der Karte erwarteten Daten

TCS_352 Antwortnachricht

Byte	Länge	Wert	Beschreibung
#1—#128	128	,XX..XXh'	Kartenauthentisierungstoken (siehe Anlage 11)
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Ist in der Sicherheitsumgebung kein öffentlicher Schlüssel vorhanden, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Ist in der Sicherheitsumgebung kein privater Schlüssel vorhanden, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Stimmt VU.CHR nicht mit dem aktuellen Bezeichner des öffentlichen Schlüssels überein, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Wird der ausgewählte private Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

TCS_353 Ist der Befehl INTERNAL AUTHENTICATE erfolgreich, wird der aktuelle Sitzungsschlüssel, sofern vorhanden, gelöscht und ist nicht mehr verfügbar. Um einen neuen Sitzungsschlüssel zur Verfügung zu haben, muss der Befehl EXTERNAL AUTHENTICATE erfolgreich ausgeführt werden.

3.6.9. **External Authenticate**

Dieser Befehl entspricht den Festlegungen von ISO/IEC 7816-4.

Mit Hilfe des Befehls EXTERNAL AUTHENTICATE kann die Karte das IFD authentisieren.

Der Authentisierungsvorgang wird in Anlage 11 beschrieben. Er beinhaltet folgende Aussagen:

TCS_354 Ein GET CHALLENGE-Befehl muss dem Befehl EXTERNAL AUTHENTICATE unmittelbar vorausgehen. Die Karte gibt eine Zufallszahl (RND3) nach außen aus.

TCS_355 Die Verifizierung des Kryptogramms verwendet RND3 (von der Karte ausgegebene Zufallszahl), den (implizit ausgewählten) privaten Kartenschlüssel und den zuvor durch den MSE-Befehl ausgewählten öffentlichen Schlüssel.

TCS_356 Die Karte prüft das Kryptogramm, und wenn es korrekt ist, wird die Zugriffsbedingung AUT eröffnet.

TCS_357 Das Eingabekryptogramm trägt das zweite Element für die Sitzungsschlüsselvereinbarung K2.

TCS_358 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,82h'	INS
P1	1	,00h'	P1
P2	1	,00h'	P2 (der zu verwendende öffentliche Schlüssel ist implizit bekannt und wurde vorher durch den MSE-Befehl gesetzt)
Lc	1	,80h'	Lc (Länge der an die Karte gesendeten Daten)
#6—#133	128	,XX..XXh'	Kryptogramm (siehe Anlage 11)

TCS_359 Antwortnachricht

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (Statusbytes (SW1, SW2))

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Ist kein öffentlicher Schlüssel in der Sicherheitsumgebung vorhanden, wird ,6A88' zurückgesendet.
- Ist die CHA des derzeit gesetzten Schlüssels nicht die Verkettung der AID der Kontrollgerätanwendung und eines FE-Gerätetyps, lautet der zurückgesendete Verarbeitungsstatus ,6F00' (siehe Anlage 11).
- Ist kein privater Schlüssel in der Sicherheitsumgebung vorhanden, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Ist die Prüfung des Kryptogramms falsch, lautet der zurückgesendete Verarbeitungsstatus ,6688'.
- Geht dem Befehl nicht unmittelbar ein GET CHALLENGE-Befehl voraus, lautet der zurückgesendete Verarbeitungsstatus ,6985'.
- Wird der ausgewählte private Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

TCS_360 Ist der Befehl EXTERNAL AUTHENTICATE erfolgreich und ist der erste Teil des Sitzungsschlüssels eines kurz zuvor erfolgreich ausgeführten INTERNAL AUTHENTICATE verfügbar, wird der Sitzungsschlüssel für künftige Befehle unter Verwendung von Secure Messaging gesetzt.

TCS_361 Ist der erste Teil des Sitzungsschlüssels nicht aus einem vorhergehenden INTERNAL AUTHENTICATE-Befehl verfügbar, wird der vom IFD gesendete zweite Teil des Sitzungsschlüssels nicht auf der Karte gespeichert. Mit diesem Mechanismus wird sichergestellt, dass der Vorgang der gegenseitigen Authentisierung in der in Anlage 11 spezifizierten Reihenfolge abläuft.

3.6.10. Manage Security Environment

Dieser Befehl wird zum Setzen eines öffentlichen Schlüssels zu Authentisierungszwecken verwendet.

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

TCS_362 Der Schlüssel, auf den im MSE-Datenfeld verwiesen wird, ist für jede Datei des DF Tachograph gültig.

TCS_363 Der Schlüssel, auf den im MSE-Datenfeld verwiesen wird, bleibt bis zum nächsten korrekten MSE-Befehl der aktuelle öffentliche Schlüssel.

TCS_364 Ist der Schlüssel, auf den verwiesen wird, (noch) nicht in der Karte vorhanden, bleibt die Sicherheitsumgebung unverändert.

TCS_365 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,22h'	INS
P1	1	,C1h'	P1: Schlüssel, auf den verwiesen wird, gültig für alle kryptografischen Operationen
P2	1	,B6h'	P2 (mit Verweis versehene Daten zur digitalen Signatur)
Lc	1	,0Ah'	Lc: Länge des folgenden Datenfelds
#6	1	,83h'	Tag zum Verweis auf einen öffentlichen Schlüssel in asymmetrischen Fällen
#7	1	,08h'	Länge des Schlüsselverweises (Schlüsselbezeichner)
#8—#15	08h	,XX..XXh'	Schlüsselbezeichner laut Anlage 11

TCS_366 Antwortnachricht

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Ist der Schlüssel, auf den verwiesen wird, auf der Karte nicht vorhanden, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Fehlen einige erwartete Datenobjekte im Secure-Messaging-Format, wird ,6987' zurückgesendet. Dies kann der Fall sein, wenn der Tag ,83h' fehlt.
- Sind einige Datenobjekte inkorrekt, lautet der zurückgesendete Verarbeitungsstatus ,6988'. Dies kann der Fall sein, wenn der Schlüsselbezeichner nicht ,08h' ist.
- Wird der ausgewählte Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

3.6.11. **PSO: Hash**

Dieser Befehl dient dazu, Ergebnisse der Hashwertberechnung für bestimmte Daten an die Karte zu übertragen. Der Hashwert wird im EEPROM für den folgenden Befehl zur Prüfung der digitalen Signatur gespeichert.

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

TCS_367 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,2Ah'	Perform Security Operation
P1	1	,90h'	Hash-Code zurücksenden
P2	1	,A0h'	Tag: Datenfeld enthält relevante DO für Hash-Code-Anwendung
Lc	1	,16h'	Länge Lc des folgenden Datenfelds
#6	1	,90h'	Tag für den Hash-Code
#7	1	,14h'	Länge des Hash-Codes
#8—#27	20	,XX..XXh'	Hash-Code

TCS_368 Antwortnachricht

Byte	Longitud	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Fehlen einige der erwarteten Datenobjekte (siehe oben), wird der Verarbeitungsstatus ,6987' zurückgesendet. Dies kann der Fall sein, wenn der Tag ,90h' fehlt.
- Sind einige Datenobjekte inkorrekt, lautet der zurückgesendete Verarbeitungsstatus ,6988'. Dieser Fehler tritt auf, wenn der erforderliche Tag zwar vorhanden ist, aber eine andere Länge als ,14h' aufweist.

3.6.12. **Perform Hash of File**

Dieser Befehl entspricht nicht den Festlegungen von ISO/IEC 7816-8. Das CLA-Byte dieses Befehls gibt daher an, dass eine proprietäre Verwendung von PERFORM SECURITY OPERATION / HASH erfolgt.

TCS_369 Der Befehl PERFORM HASH OF FILE wird zur Hash-Berechnung des Datenbereichs der zu dem entsprechenden Zeitpunkt ausgewählten transparenten EF verwendet.

TCS_370 Das Ergebnis der Hash-Operation wird auf der Karte gespeichert. Es kann dann zur Einholung einer digitalen Signatur der Datei mit Hilfe des Befehls PSO: COMPUTE DIGITAL SIGNATURE verwendet werden. Dieses Ergebnis bleibt bis zum nächsten erfolgreichen Befehl Perform Hash of File für den Befehl COMPUTE DIGITAL SIGNATURE verfügbar.

TCS_371 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,80h'	CLA
INS	1	,2Ah'	Perform Security Operation
P1	1	,90h'	Tag: Hash
P2	1	,00h'	P2: Hash-Berechnung der Daten der zu dem entsprechenden Zeitpunkt ausgewählten transparenten Datei

TCS_372 Antwortnachricht

Byte	Länge	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Ist keine Anwendung ausgewählt, wird der Verarbeitungsstatus ,6985' zurückgesendet.
- Wird die ausgewählte EF als verfälscht betrachtet (wegen Integritätsfehlern in den Dateiattributen oder den gespeicherten Daten), lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.
- Ist die ausgewählte Datei keine transparente Datei, lautet der zurückgesendete Verarbeitungsstatus ,6986'.

3.6.13. PSO: Compute Digital Signature

Dieser Befehl wird zur Berechnung der digitalen Signatur des zuvor berechneten Hash-Codes (siehe Perform Hash of File, 3.6.12) verwendet.

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

TCS_373 Zur Berechnung der digitalen Signatur wird der private Schlüssel der Karte, der der Karte implizit bekannt ist, herangezogen.

TCS_374 Die Karte führt eine digitale Signatur mit Hilfe einer Auffüllmethode gemäß PKCS1 aus (Einzelheiten siehe Anlage 11).

TCS_375 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,2Ah'	Perform Security Operation
P1	1	,9Eh'	Zurückzusendende digitale Signatur
P2	1	,9Ah'	Tag: Datenfeld enthält zu signierende Daten. Da kein Datenfeld enthalten ist, wird davon ausgegangen, dass die Daten bereits auf der Karte vorhanden sind (hash of file)
Le	1	,80h'	Länge der erwarteten Signatur

TCS_376 Antwortnachricht

Byte	Länge	Wert	Beschreibung
#1—#128	128	,XX..XXh'	Signatur des zuvor berechneten Hash
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Wird der implizit ausgewählte private Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

3.6.14. PSO: Verify Digital Signature

Dieser Befehl wird zur Verifizierung der als Eingabe gemäß PKCS1 bereitgestellten digitalen Signatur einer Nachricht verwendet, deren Hash der Karte bekannt ist. Der Signaturalgorithmus ist der Karte implizit bekannt.

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

TCS_377 Der Befehl VERIFY DIGITAL SIGNATURE verwendet stets den vom vorhergehenden Befehl MANAGE SECURITY ENVIRONMENT ausgewählten öffentlichen Schlüssel sowie den von einem PSO: Hash-Befehl eingegebenen Hash-Code.

TCS_378 Befehlsnachricht

Byte	Länge	Wert	Beschreibung
CLA	1	,00h'	CLA
INS	1	,2Ah'	Perform Security Operation
P1	1	,00h'	Tag: Datenfeld enthält verifizierungsrelevante DO
P2	1	,A8h'	
Lc	1	,83h'	Länge Lc des folgenden Datenfelds
#28	1	,9Eh'	Tag für digitale Signatur
#29—#30	2	,8180h'	Länge der digitalen Signatur (128 Byte, kodiert gemäß ISO/IEC 7816-6)
#31—#158	128	,XX..XXh'	Inhalt der digitalen Signatur

TCS_379 Antwortnachricht

Byte	Longitud	Wert	Beschreibung
SW	2	,XXXXh'	Statusbytes (SW1, SW2)

- Ist der Befehl erfolgreich, sendet die Karte ,9000' zurück.
- Schlägt die Verifizierung der Signatur fehl, lautet der zurückgesendete Verarbeitungsstatus ,6688'. Der Verifizierungsvorgang wird in Anlage 11 beschrieben.
- Ist kein öffentlicher Schlüssel ausgewählt, lautet der zurückgesendete Verarbeitungsstatus ,6A88'.
- Fehlen einige der erwarteten Datenobjekte (siehe oben), wird der Verarbeitungsstatus ,6987' zurückgesendet. Das kann der Fall sein, wenn der erforderliche Tag fehlt.
- Ist kein Hash-Code zur Verarbeitung des Befehls verfügbar (im Ergebnis eines PSO: Hash-Befehls), lautet der zurückgesendete Verarbeitungsstatus ,6985'.
- Sind einige Datenobjekte inkorrekt, lautet der zurückgesendete Verarbeitungsstatus ,6988'. Dies kann der Fall sein, wenn eine Länge der erforderlichen Datenobjekte inkorrekt ist.
- Wird der ausgewählte öffentliche Schlüssel als verfälscht betrachtet, lautet der zurückgesendete Verarbeitungsstatus ,6400' oder ,6581'.

4. STRUKTUR DER KONTROLLGERÄTKARTEN

In diesem Abschnitt werden die Dateistrukturen, die auf den Kontrollgerätkarten der Speicherung zugänglicher Daten dienen, spezifiziert.

Nicht spezifiziert werden vom Kartenhersteller abhängige interne Strukturen, wie z. B. Dateianfangskennsätze oder die Speicherung und Verarbeitung von Datenelementen, die nur für den internen Gebrauch benötigt werden, z. B. EuropeanPublicKey, CardPrivateKey, TDesSessionKey oder WorkshopCardPin.

Die nutzbare Speicherkapazität von Kontrollgerätkarten beträgt mindestens 11 KB, doch sind höhere Kapazitäten zulässig. In einem derartigen Fall bleibt die Struktur der Karte gleich, während sich die Anzahl der Datensätze einiger Elemente der Struktur erhöht. Dieser Abschnitt spezifiziert die Mindest- und die Höchstwerte dieser Datensatzzahlen.

4.1. Struktur der Fahrerkarte

TCS_400 Nach der Personalisierung weist die Fahrerkarte folgende permanente Dateistruktur und Dateizugriffsbedingungen auf:

File	File ID	Zugriffsbedingungen		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	Nein
EF IC	0005	ALW	NEV	Nein
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Nein
EF Card_Certificate	C100	ALW	NEV	Nein
EF CA_Certificate	C108	ALW	NEV	Nein
EF Identification	0520	ALW	NEV	Nein
EF Card_Download	050E	ALW	ALW	Nein
EF Driving_Licence_Info	0521	ALW	NEV	Nein
EF Events_Data	0502	ALW	PRO SM / AUT	Nein
EF Faults_Data	0503	ALW	PRO SM / AUT	Nein
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Nein
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Nein
EF Places	0506	ALW	PRO SM / AUT	Nein
EF Current_Usage	0507	ALW	PRO SM / AUT	Nein
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Nein
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Nein

TCS_401 Die Strukturen aller EF sind transparent.

TCS_402 Lesen mit Secure Messaging muss für alle Dateien unter dem DF Tachograph möglich sein.

TCS_403 Die Fahrerkarte hat folgende Datenstruktur:

Datei/Datenelement	Anzahl der Datensätze	Größe (in Byte)		Standardwerte
		Min.	Max.	
MF	11411	24959		
EF ICC	25	25		
CardIccIdentification	25	25		
clockStop	1	1		{00}
cardExtendedSerialNumber	8	8		{00..00}
cardApprovalNumber	8	8		{20..20}
cardPersonaliserID	1	1		{00}
embedderIcAssemblerId	5	5		{00..00}
icIdentifier	2	2		{00 00}
EF IC	8	8		
CardChipIdentification	8	8		
icSerialNumber	4	4		{00..00}
icManufacturingReferences	4	4		{00..00}
DF Tachograph	11378	24926		
EF Application_Identification	10	10		
DriverCardApplicationIdentification	10	10		
typeOfTachographCardId	1	1		{00}
cardStructureVersion	2	2		{00 00}
noOfEventsPerType	1	1		{00}
noOfFaultsPerType	1	1		{00}
activityStructureLength	2	2		{00 00}
noOfCardVehicleRecords	2	2		{00 00}
noOfCardPlaceRecords	1	1		{00}
EF Card_Certificate	194	194		
CardCertificate	194	194		{00..00}
EF CA_Certificate	194	194		
MemberStateCertificate	194	194		{00..00}
EF Identification	143	143		
CardIdentification	65	65		
cardIssuingMemberState	1	1		{00}
cardNumber	16	16		{20..20}
cardIssuingAuthorityName	36	36		{20..20}
cardIssueDate	4	4		{00..00}
cardValidityBegin	4	4		{00..00}
cardExpiryDate	4	4		{00..00}
DriverCardHolderIdentification	78	78		
cardHolderName	72	72		
holderSurname	36	36		{00, 20..20}
holderFirstNames	36	36		{00, 20..20}
cardHolderBirthDate	4	4		{00..00}
cardHolderPreferredLanguage	2	2		{20 20}

EF Card_Download		4	4	
└ LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
└ CardDrivingLicenceInformation		53	53	
└ drivingLicenceIssuingAuthority		36	36	{00, 20..20}
└ drivingLicenceIssuingNation		1	1	{00}
└ drivingLicenceNumber		16	16	{20..20}
EF Events_Data		864	1728	
└ CardEventData		864	1728	
└ cardEventRecords	6	144	288	
└ CardEventRecord	n ₁	24	24	
└ eventType		1	1	{00}
└ eventBeginTime		4	4	{00..00}
└ eventEndTime		4	4	{00..00}
└ eventVehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		576	1152	
└ CardFaultData		576	1152	
└ cardFaultRecords	2	288	576	
└ CardFaultRecord	n ₂	24	24	
└ faultType		1	1	{00}
└ faultBeginTime		4	4	{00..00}
└ faultEndTime		4	4	{00..00}
└ faultVehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		5548	13780	
└ CardDriverActivity		5548	13780	
└ activityPointerOldestDayRecord		2	2	{00 00}
└ activityPointerNewestRecord		2	2	{00 00}
└ activityDailyRecords	n ₆	5544	13776	{00..00}
EF Vehicles_Used		2606	6202	
└ CardVehiclesUsed		2606	6202	
└ vehiclePointerNewestRecord		2	2	{00 00}
└ cardVehicleRecords		2604	6200	
└ CardVehicleRecord	n ₃	31	31	
└ vehicleOdometerBegin		3	3	{00..00}
└ vehicleOdometerEnd		3	3	{00..00}
└ vehicleFirstUse		4	4	{00..00}
└ vehicleLastUse		4	4	{00..00}
└ vehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
└ vuDataBlockCounter		2	2	{00 00}
EF Places		841	1121	
└ CardPlaceDailyWorkPeriod		841	1121	
└ placePointerNewestRecord		1	1	{00}
└ placeRecords		840	1120	
└ PlaceRecord	n ₄	10	10	
└ entryTime		4	4	{00..00}
└ entryTypeDailyWorkPeriod		1	1	{00}
└ dailyWorkPeriodCountry		1	1	{00}
└ dailyWorkPeriodRegion		1	1	{00}
└ vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
└ CardCurrentUse		19	19	
└ sessionOpenTime		4	4	{00..00}
└ sessionOpenVehicle				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
└ CardControlActivityDataRecord		46	46	
└ controlType		1	1	{00}
└ controlTime		4	4	{00..00}
└ controlCardNumber				
└ cardType		1	1	{00}
└ cardIssuingMemberState		1	1	{00}
└ cardNumber		16	16	{20..20}
└ controlVehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
└ controlDownloadPeriodBegin		4	4	{00..00}
└ controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		280	280	
└ SpecificConditionRecord	56	5	5	
└ entryTime		4	4	{00..00}
└ SpecificConditionType		1	1	{00}

TCS_404 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Fahrerkarte verwenden muss:

		Min.	Max.
n ₁	NoOfEventsPerType	6	12
n ₂	NoOfFaultsPerType	12	24
n ₃	NoOfCardVehicleRecords	84	200
n ₄	NoOfCardPlaceRecords	84	112
n ₆	CardActivityLengthRange	5544 Byte (28 Tage * 93 Tätigkeitsänderungen)	13776 Byte (28 Tage * 240 Tätigkeitsänderungen)

4.2. Struktur der Werkstattkarte

TCS_405 Nach der Personalisierung weist die Werkstattkarte folgende permanente Dateistruktur und Dateizugriffsbedingungen auf:

File	File ID	Zugriffsbedingungen		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	Nein
EF IC	0005	ALW	NEV	Nein
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Nein
EF Card_Certificate	C100	ALW	NEV	Nein
EF CA_Certificate	C108	ALW	NEV	Nein
EF Identification	0520	ALW	NEV	Nein
EF Card_Download	0509	ALW	ALW	Nein
EF Calibration	050A	ALW	PRO SM / AUT	Nein
EF Sensor_Installation_Data	050B	ALW	NEV	Ja
EF Events_Data	0502	ALW	PRO SM / AUT	Nein
EF Faults_Data	0503	ALW	PRO SM / AUT	Nein
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Nein
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Nein
EF Places	0506	ALW	PRO SM / AUT	Nein
EF Current_Usage	0507	ALW	PRO SM / AUT	Nein
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Nein
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Nein

TCS_406 Die Strukturen aller EF sind transparent.

TCS_407 Lesen mit Secure Messaging muss für alle Dateien unter dem DF Tachograph möglich sein.

TCS_408 Die Werkstattkarte hat folgende Datenstruktur:

Datei/Datenelement	Anzahl der Datensätze	Größe (in Byte)		Standardwerte
		Min.	Max.	
MF		11088	29061	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11055	29028	
EF Application_Identification		11	11	
WorkshopCardApplicationIdentification		11	11	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}

EF Card_Certificate	194	194	
CardCertificate	194	194	{00..00}
EF CA_Certificate	194	194	
MemberStateCertificate	194	194	{00..00}
EF Identification	211	211	
CardIdentification	65	65	
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
cardIssuingAuthorityName	36	36	{00, 20..20}
cardIssueDate	4	4	{00..00}
cardValidityBegin	4	4	{00..00}
cardExpiryDate	4	4	{00..00}
WorkshopCardHolderIdentification	146	146	
workshopName	36	36	{00, 20..20}
workshopAddress	36	36	{00, 20..20}
cardHolderName			
holderSurname	36	36	{00, 20..20}
holderFirstNames	36	36	{00, 20..20}
cardHolderPreferredLanguage	2	2	{20 20}
EF Card_Download	2	2	
NoOfCalibrationsSinceDownload	2	2	{00 00}
EF Calibration	9243	26778	
WorkshopCardCalibrationData	9243	26778	
calibrationTotalNumber	2	2	{00 00}
calibrationPointerNewestRecord	1	1	{00}
calibrationRecords	9240	26775	
WorkshopCardCalibrationRecord	n ₅	105	105
calibrationPurpose	1	1	{00}
vehicleIdentificationNumber	17	17	{20..20}
vehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
wVehicleCharacteristicConstant	2	2	{00 00}
kConstantOfRecordingEquipment	2	2	{00 00}
lTyreCircumference	2	2	{00 00}
tyreSize	15	15	{20..20}
authorisedSpeed	1	1	{00}
oldOdometerValue	3	3	{00..00}
newOdometerValue	3	3	{00..00}
oldTimeValue	4	4	{00..00}
newTimeValue	4	4	{00..00}
nextCalibrationDate	4	4	{00..00}
vuPartNumber	16	16	{20..20}
vuSerialNumber	8	8	{00..00}
sensorSerialNumber	8	8	{00..00}
EF Sensor_Installation_Data	16	16	
SensorInstallationSecData	16	16	{00..00}
EF Events_Data	432	432	
CardEventData	432	432	
cardEventRecords	6	72	72
CardEventRecord	n ₁	24	24
eventType	1	1	{00}
eventBeginTime	4	4	{00..00}
eventEndTime	4	4	{00..00}
eventVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Faults_Data	288	288	
CardFaultData	288	288	
cardFaultRecords	2	144	144
CardFaultRecord	n ₂	24	24
faultType	1	1	{00}
faultBeginTime	4	4	{00..00}
faultEndTime	4	4	{00..00}
faultVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Driver_Activity_Data	202	496	
CardDriverActivity	202	496	
activityPointerOldestDayRecord	2	2	{00 00}
activityPointerNewestRecord	2	2	{00 00}
activityDailyRecords	n ₆	198	492
EF Vehicles_Used	126	250	
CardVehiclesUsed	126	250	
vehiclePointerNewestRecord	2	2	{00 00}
cardVehicleRecords	124	248	
CardVehicleRecord	n ₃	31	31
vehicleOdometerBegin	3	3	{00..00}

vehicleOdometerEnd	3	3	{00..00}
vehicleFirstUse	4	4	{00..00}
vehicleLastUse	4	4	{00..00}
vehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
vuDataBlockCounter	2	2	{00 00}
EF Places	61	81	
CardPlaceDailyWorkPeriod	61	81	
placePointerNewestRecord	1	1	{00}
placeRecords	60	80	
PlaceRecord	n ₄ 10	10	
entryTime	4	4	{00..00}
entryTypeDailyWorkPeriod	1	1	{00}
dailyWorkPeriodCountry	1	1	{00}
dailyWorkPeriodRegion	1	1	{00}
vehicleOdometerValue	3	3	{00..00}
EF Current_Usage	19	19	
CardCurrentUse	19	19	
sessionOpenTime	4	4	{00..00}
sessionOpenVehicle			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Control_Activity_Data	46	46	
CardControlActivityDataRecord	46	46	
controlType	1	1	{00}
controlTime	4	4	{00..00}
controlCardNumber			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
controlVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
controlDownloadPeriodBegin	4	4	{00..00}
controlDownloadPeriodEnd	4	4	{00..00}
EF Specific_Conditions	10	10	
SpecificConditionRecord	2	5	
entryTime	4	4	{00..00}
SpecificConditionType	1	1	{00}

TCS_409 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Werkstattkarte verwenden muss:

		Min.	Max.
n ₁	NoOfEventsPerType	3	3
n ₂	NoOfFaultsPerType	6	6
n ₃	NoOfCardVehicleRecords	4	8
n ₄	NoOfCardPlaceRecords	6	8
n ₆	CardActivityLengthRange	88	255
n ₅	NoOfCalibrationRecords	198 Byte (1 Tag * 93 Tätigkeits- veränderungen)	492 Byte (1 Tag * 240 Tätigkeits- veränderungen)

4.3. Struktur der Kontrollkarte

TCS_410 Nach der Personalisierung weist die Kontrollkarte folgende permanente Dateistruktur und Dateizugriffsbedingungen auf:

File	File ID	Zugriffsbedingungen		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	Nein
EF IC	0005	ALW	NEV	Nein
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Nein
EF Card_Certificate	C100	ALW	NEV	Nein
EF CA_Certificate	C108	ALW	NEV	Nein
EF Identification	0520	AUT	NEV	Nein
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Nein

TCS_411 Die Strukturen aller EF sind transparent.

TCS_412 Lesen mit Secure Messaging muss für alle Dateien unter dem DF Tachograph möglich sein.

TCS_413 Die Kontrollkarte hat folgende Datenstruktur:

Datei/Datenelement	Anzahl der Datensätze	Größe (in Byte)		Standardwerte
		Min.	Max.	
MF		11219	24559	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11186	24526	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		10580	23920	
controlActivityRecord	n ₇	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Kontrollkarte verwenden muss:

		Min.	Max.
n ₇	NoOfControlActivityRecords	230	520

4.4. Struktur der Unternehmenskarte

TCS_415 Nach der Personalisierung weist die Unternehmenskarte folgende permanente Dateistruktur und Dateizugriffsbedingungen auf:

File	File ID	Zugriffsbedingungen		
		Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	Nein
EF IC	0005	ALW	NEV	Nein
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Nein
EF Card_Certificate	C100	ALW	NEV	Nein
EF CA_Certificate	C108	ALW	NEV	Nein
EF Identification	0520	AUT	NEV	Nein
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Nein

TCS_416 Die Strukturen aller EF sind transparent.

TCS_417 Lesen mit Secure Messaging muss für alle Dateien unter dem DF Tachograph möglich sein.

TCS_418 Die Unternehmenskarte hat folgende Datenstruktur:

Datei/Datenelement	Anzahl der Datensätze	Größe (in Byte)		Standardwerte
		Min.	Max.	
MF		11147	24487	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11114	24454	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n ₈	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

└─cardNumberInformation			
└─┬─cardType	1	1	{00}
└─┬─cardIssuingMemberState	1	1	{00}
└─┬─cardNumber	16	16	{20..20}
└─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

TCS_419 Die folgenden, in der vorstehenden Tabelle zur Größenangabe herangezogenen Werte sind die Mindest- und die Höchstwerte für die Anzahl der Datensätze, die die Datenstruktur der Unternehmenskarte verwenden muss:

		Min.	Max.
ng	NoOfCompanyActivityRecords	230	520

Anlage 3

PIKTOGRAMME

PIC_001 Vom Kontrollgerät können folgende Piktogramme und Piktogrammkombinationen verwendet werden:

1. EINZELPIKTOGRAMME

	Personen	Maßnahmen	Betriebsarten
	Unternehmen		Unternehmen
	Kontrolleur	Kontrolle	Kontrolle
	Fahrer	Lenken	Betrieb
	Werkstatt/Prüfstelle	Überprüfung/Kalibrierung	Kalibrierung
	Hersteller		

	Tätigkeiten	Dauer
	Bereitschaft	Laufende Bereitschaftszeit
	Lenken	Kontinuierliche Lenkzeit
	Ruhe	Laufende Ruhezeit
	Arbeit	Laufende Arbeitszeit
	Unterbrechung	Kumulative Pausenzeit
	Unbekannt	

	Geräte	Funktionen
	Steckplatz Fahrer	
	Steckplatz 2. Fahrer	
	Karte	
	Uhr	
	Anzeige	Anzeigen
	Externe Speicherung	Herunterladen
	Stromversorgung	
	Drucker/Ausdruck	Drucken
	Sensor	
	Reifengröße	
	Fahrzeug/Fahrzeugeinheit	

	Spezifische Bedingungen
	Kontrollgerät nicht erforderlich
	Fährüberfahrt/Zugfahrt

	Verschiedenes		
	Ereignisse		Störungen
	Beginn des Arbeitstages		Ende des Arbeitstages
	Ort		Manuelle Eingabe von Fahrttätigkeiten
	Sicherheit		Geschwindigkeit
	Zeit		Gesamt/Zusammenfassung

	Qualifikatoren
	täglich
	wöchentlich
	zwei Wochen
	von oder bis

2. PIKTOGRAMMKOMBINATIONEN

	Verschiedenes		
	Kontrollort		Ort des Endes des Arbeitstages
	Ort des Beginns des Arbeitstages		Endzeit
	Anfangszeit		
	von Fahrzeug		
	Kontrollgerät nicht erforderlich — Beginn		Kontrollgerät nicht erforderlich — Ende

Karten

	Fahrerkarte
	Unternehmenskarte
	Kontrollkarte
	Werkstattkarte
	Keine Karte

Lenken

	Team
	Lenkzeit für eine Woche
	Lenkzeit für zwei Wochen

Ausdrucke

24h	Täglicher Ausdruck Fahrttätigkeiten von der Karte
24h	Täglicher Ausdruck Fahrttätigkeiten von der FE
	Ausdruck Ereignisse und Störungen von der Karte
	Ausdruck Ereignisse und Störungen von der FE
	Ausdruck Technische Daten
	Ausdruck Geschwindigkeitsüberschreitung

Ereignisse

	Einstecken einer ungültigen Karte
	Kartenkonflikt
	Zeitüberlappung
	Lenken ohne geeignete Karte
	Einstecken der Karte während des Lenkens
	Letzter Kartenvorgang nicht korrekt abgeschlossen
	Geschwindigkeitsüberschreitung
	Unterbrechung der Stromversorgung
	Datenfehler Weg und Geschwindigkeit
	Sicherheitsverletzung
	Zeiteinstellung (durch Werkstatt)
	Kontrolle Geschwindigkeitsüberschreitung

Störungen

	Kartenfehlfunktion (Steckplatz Fahrer)
	Kartenfehlfunktion (Steckplatz 2. Fahrer)
	Anzeigestörung
	Herunterladestörung
	Druckerstörung
	Sensorstörung
	Interne FE-Störung

Manueller Eingabevorgang

	Weiterhin derselbe Arbeitstag?
	Ende des vorherigen Arbeitstages?
	Bestätigung oder Eingabe Ort des Arbeitstages
	Eingabe Anfangszeit
	Eingabe Ort des Arbeitstagbeginns

Anmerkung: Weitere Piktogrammkombinationen als Block- oder Datensatzbezeichner bei Ausdrucken sind in Anlage 4 festgelegt.

*Anlage 4***AUSDRUCKE**

INHALTSVERZEICHNIS

1.	Allgemeines	131
2.	Spezifikationen der Datenblöcke	131
3.	Spezifikationen der Ausdrücke	137
3.1.	Ausdruck Fahrtätigkeiten von der Karte	138
3.2.	Tagesausdruck Fahrtätigkeiten von der FE	138
3.3.	Ausdruck Ereignisse und Störungen von der Karte	139
3.4.	Ausdruck Ereignisse und Störungen von der FE	139
3.5.	Ausdruck Technische Daten	140
3.6.	Ausdruck Geschwindigkeitsüberschreitung	140

TT/MM/JJJJ hh:mm (UTC)

2 Art des Ausdrucks

Blockbezeichner

Ausdruck Piktogrammkombination (siehe Anlage 3), Einstellung des Geschwindigkeitsbegrenzers (nur bei Ausdruck Geschwindigkeitsüberschreitung)

-----  -----
Pikto xxx km/h

3 Angaben zum Karteninhaber

Blockbezeichner. P = Piktogramm Personen

Name des Karteninhabers

Vorname(n) des Karteninhabers (wenn zutreffend)

Kartenkennung

Karte gültig bis (wenn zutreffend)

Handelt es sich um eine nicht personengebundene Karte ohne Namen des Karteninhabers, ist statt dessen der Name des Unternehmens, der Werkstatt oder der Kontrollstelle zu drucken

-----P-----
P Zuname _____
Vorname _____
Kartenkennung _____
TT/MM/JJJJ

4 Fahrzeugkennung

Blockbezeichner

Fahrzeugidentifizierungsnummer (VIN)

Zulassender Mitgliedstaat und amtliches Kennzeichen

-----  -----
 VIN _____
Nat/Kennzeichen _____

5 FE-Kennung

Blockbezeichner

Name des FE-Herstellers

FE-Teilnummer

-----  -----
 FE-Hersteller _____
FE-Teilnummer _____

6 Letzte Kalibrierung des Kontrollgeräts

Blockbezeichner

Name der Werkstatt

Werkstattkartenkennung

Datum der Kalibrierung

-----  -----
 Name _____
Kartenkennung _____
 TT/MM/JJJJ

7 Letzte Kontrolle (durch einen Kontrolleur)

Blockbezeichner

Kontrollkartenkennung

Datum, Uhrzeit und Art der Kontrolle

Art der Kontrolle: bis zu vier Piktogramme. Die Art der Kontrolle kann sein (auch in Kombination):

: Herunterladen von der Karte, : Herunterladen von der FE, : Drucken, : Anzeigen

-----  -----
Kartenkennung _____
 TT/MM/JJJJ hh:mm pppp

8 Fahrertätigkeiten, auf einer Karte in der Reihenfolge des Auftretens gespeichert

Blockbezeichner

Abfragedatum (Kalendertag des Ausdrucks) + Tagesanwesenheitszähler

-----  -----
TT/MM/JJJJ xxx

8.1 Zeitraum, in dem die Karte nicht eingesteckt war

8.1a Datensatzbezeichner (Beginn des Zeitraums)

8.1b Unbekannter Zeitraum. Uhrzeit Beginn und Ende, Dauer

8.1c Manuell eingegebene Tätigkeit

Piktogramm Tätigkeit (A), Uhrzeit Beginn und Ende, Dauer, Ruhezeiten von mindestens einer Stunde sind mit einem Stern gekennzeichnet

-----  -----
? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2 *Einstecken der Karte in Steckplatz S*
 Datensatzbezeichner; S = Piktogramm Steckplatz
 Zulassender Mitgliedstaat und amtliches Kennzeichen
 Kilometerstand beim Einstecken der Karte
- 8.3 *Tätigkeit (bei eingesteckter Karte)*
 Piktogramm Tätigkeit (A), Uhrzeit Beginn und Ende, Dauer, Status der Fahrzeugführung (Piktogramm Team bei TEAM, Leerstellen bei EINMANNBETRIEB), Ruhezeiten von mindestens einer Stunde sind mit einem Stern gekennzeichnet.
- 8.3a *Spezifische Bedingung. Eingabezeit, Piktogramm Spezifische Bedingung (oder Piktogrammkombination).*
- 8.4 *Entnahme der Karte*
 Kilometerstand und zurückgelegte Wegstrecke seit dem letzten Einstecken, für das der Kilometerstand bekannt ist
- 9 **Fahrtstätigkeiten, in einer FE je Steckplatz in chronologischer Reihenfolge gespeichert**
 Blockbezeichner
 Anfragedatum (Kalendertag des Ausdrucks)
 Kilometerstand um 00:00 Uhr und 24:00 Uhr
- 10 **Tätigkeiten in Steckplatz S**
 Blockbezeichner
- 10.1 *Zeitraum, in dem keine Karte in Steckplatz S eingesetzt ist*
 Datensatzbezeichner
 Keine Karte eingesetzt
 Kilometerstand zu Beginn des Zeitraums
- 10.2 *Einstecken der Karte*
 Datensatzbezeichner Einstecken der Karte
 Name des Fahrers
 Vorname(n) des Fahrers
 Fahrerkartenkennung
 Fahrerkarte gültig bis
 Zulassender Mitgliedstaat und amtliches Kennzeichen des vorherigen Fahrzeuges
 Datum und Uhrzeit der Kartenentnahme aus vorherigem Fahrzeug
 Leerzeile
 Kilometerstand beim Einstecken der Karte, manuelle Eingabe der Fahrtstätigkeits-Flags (M = ja, leer = nein)
- 10.3 *Tätigkeit*
 Piktogramm Tätigkeit (A), Uhrzeit Beginn und Ende, Dauer, Status der Fahrzeugführung (Piktogramm Team bei TEAM, Leerstellen bei EINMANNBETRIEB), Ruhezeiten von mindestens einer Stunde sind mit einem Stern gekennzeichnet.

```

-----S-----
A Nat/Kennzeichen _____
x xxx xxx km

```

```

A hh:mm hh:mm hh:mm 00 *

```

```

hh:mm ----- pppp -----

```

```

x xxx xxx km; x xxx km

```

```

-----0-----
TT/MM/JJJJ
x xxx xxx - x xxx xxx km

```

```

----- S -----

```

```

-----
00 ---
x xxx xxx km

```

```

-----
0 Zuname _____
Vorname _____
Kartenkennung _____
TT/MM/JJJJ
A + Nat/VRN _____
TT/MM/JJJJ hh:mm
x xxx xxx km M

```

```

A hh:mm hh:mm hh:mm 00 *

```

- | | | |
|-------|--|---|
| 10.3a | <i>Spezifische Bedingung.</i> Eingabezeit, Piktogramm Spezifische Bedingung (oder Piktogrammkombination) | hh:mm ----- pppp ----- |
| 10.4 | <i>Kartenentnahme oder Ende des Zeitraums ‚keine Karte‘</i>
Kilometerstand bei Kartenentnahme oder Ende des Zeitraums ‚keine Karte‘ und zurückgelegte Wegstrecke seit Einstecken der Karte oder seit Beginn des Zeitraums ‚keine Karte‘ | x xxx xxx km; x xxx km |
| 11 | Tageszusammenfassung
Blockbezeichner | ----- Σ ----- |
| 11.1 | <i>FE-Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Fahrer</i>
Blockbezeichner | 1 @ - - - |
| 11.2 | <i>FE-Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz 2. Fahrer</i>
Blockbezeichner | 2 @ - - - |
| 11.3 | <i>FE-Tageszusammenfassung je Fahrer</i>
Datensatzbezeichner
Name des Fahrers
Vorname(n) des Fahrers
Fahrerkartenkennung | -----
@ Zuname _____
Vorname _____
Kartenkennung _____ |
| 11.4 | <i>Eingabe Ort des Beginns oder Endes des Arbeitstages</i>
pi = Piktogramm Ort Beginn/Ende, Uhrzeit, Land, Region
Kilometerstand | pihh:mm Lnd Reg
x xxx xxx km |
| 11.5 | <i>Gesamtwerte Tätigkeiten (von einer Karte)</i>
Gesamtlenkzeit, zurückgelegte Wegstrecke
Gesamte Arbeits- und Bereitschaftszeit
Gesamte Ruhezeit und unbekannte Zeiten
Gesamtzeit Teamtätigkeiten | @ hhhmm x xxx km
✱ hhhmm @ hhhmm
└─ hhhmm ? hhhmm
@@ hhhmm |
| 11.6 | <i>Gesamtwerte Tätigkeiten (Zeitabschnitte ohne Steckplatz Fahrer)</i>
Gesamtlenkzeit, zurückgelegte Wegstrecke
Gesamte Arbeits- und Bereitschaftszeit
Gesamtruhezeit | @ hhhmm x xxx km
✱ hhhmm @ hhhmm
└─ hhhmm |
| 11.7 | <i>Gesamtwerte Tätigkeiten (Zeitabschnitte ohne Steckplatz 2. Fahrer)</i>
Gesamte Arbeits- und Bereitschaftszeit
Gesamtruhezeit | ✱ hhhmm @ hhhmm
└─ hhhmm |

11.8 Gesamtwerte Tätigkeiten (je Fahrer, beide Steckplätze)

Gesamtlenkzeit, zurückgelegte Wegstrecke

Gesamte Arbeits- und Bereitschaftszeit

Gesamtruhezeit

Gesamtzeit Teamtätigkeiten

Wird ein Tagesausdruck für den aktuellen Tag benötigt, erfolgt die Berechnung der Angaben für die Tageszusammenfassung anhand der zum Zeitpunkt des Ausdrucks vorhandenen Daten

```

⊙ hh:mm x xxx km
✱ hh:mm ☐ hh:mm
┌ hh:mm
⊙⊙ hh:mm

```

12 Auf einer Karte gespeicherte Ereignisse und/oder Störungen

12.1 Blockbezeichner für die letzten 5 Ereignisse und Störungen auf der Karte

```

----- ! ✱ ☐ -----

```

12.2 Blockbezeichner für alle aufgezeichneten Ereignisse auf der Karte

```

----- ! ☐ -----

```

12.3 Blockbezeichner für alle aufgezeichneten Störungen auf der Karte

```

----- ✱ ☐ -----

```

12.4 Datensatz Ereignis und/oder Störung

Datensatzbezeichner

Piktogramm Ereignis/Störung, Datensatzzweck, Datum/Zeit Beginn

(ggf.) weiterer Ereignis-/Störungscode, Dauer

Zulassender Mitgliedstaat und amtliches Kennzeichen des Fahrzeugs, in dem Ereignis oder Störung auftrat

```

-----
Pik          TT/MM/JJJJ hh:mm
!xxx                      hh:mm
☐ Nat/Kennzeichen _____

```

13 In einer FE gespeicherte oder andauernde Ereignisse und Störungen

13.1 Blockbezeichner für die letzten 5 Ereignisse und Störungen in der FE

```

----- ! ✱ ☐ -----

```

13.2 Blockbezeichner für alle aufgezeichneten oder andauernden Ereignisse in der FE

```

----- ! ☐ -----

```

13.3 Blockbezeichner für alle aufgezeichneten oder andauernden Störungen in der FE

```

----- ✱ ☐ -----

```

13.4 Datensatz Ereignis und/oder Störung

Datensatzbezeichner

Pikt. Ereignis/Störung, Datensatzzweck, Datum/Zeit Beginn

(ggf.) weiterer Ereignis-/Störungscode, Anzahl ähnlicher Ereignisse an diesem Tag, Dauer

Kennung der zu Beginn oder am Ende des Ereignisses oder der Störung eingesteckten Karte (bis zu 4 Zeilen ohne Wiederholung derselben Kartennummern)

Bei nicht eingesteckter Karte

Der Datensatzzweck (z) ist ein numerischer Code zur Erläuterung, warum das Ereignis oder die Störung aufgezeichnet wurde; die Codierung erfolgt entsprechend dem Datenelement EventFaultRecordPurpose.

```

-----
Pik (z) TT/MM/JJJJ hh:mm
!xxx (xxx) hh:mm

Kartenkennung _____
Kartenkennung _____
Kartenkennung _____
Kartenkennung _____
☐ ---

```

14 FE-Kennung

Blockbezeichner
 Name des FE-Herstellers
 Anschrift des FE-Herstellers
 FE-Teilnummer
 FE-Bauartgenehmigungsnummer
 FE-Seriennummer
 FE-Baujahr
 Version und Installationsdatum der FE-Software

```

-----B-----
B Name _____
  Anschrift _____
  Teilnummer _____
  Genehmigungsnr. ____
  Seriennr
  JJJJ
  V  xx.xx.xx  TT/MM/JJJJ
  
```

15 Kennnummer des Weg- und/oder Geschwindigkeitsgebers (Sensor)

Blockbezeichner
 Seriennummer des Sensors
 Bauartgenehmigungsnummer des Sensors
 Ersteinbaudatum des Sensors

```

-----L-----
L Seriennr
  Genehmigungsnr. ____
  TT/MM/JJJJ
  
```

16 Kalibrierungsdaten

Blockbezeichner

```

-----T-----
  
```

16.1 Datensatz Kalibrierung

Datensatzbezeichner
 Werkstatt, die die Kalibrierung ausgeführt hat
 Anschrift der Werkstatt
 Werkstattkartenkennung
 Werkstattkarte gültig bis
 Leerzeile
 Datum und Zweck der Kalibrierung
 Fahrzeugidentifizierungsnummer (VIN)
 Zulassender Mitgliedstaat und amtliches Kennzeichen
 Wegdrehzahl des Fahrzeugs
 Konstante des Kontrollgeräts
 Tatsächlicher Reifenumfang
 Reifengröße
 Einstellung des Geschwindigkeitsbegrenzers
 Alter und neuer Kilometerstand
 Der Kalibrierungszweck (z) ist ein numerischer Code zur Erläuterung, warum diese Kalibrierungsparameter aufgezeichnet wurden; die Codierung erfolgt entsprechend dem Datenelement CalibrationPurpose.

```

-----
T Name_Werkstatt _____
  Anschrift_Werkstatt _____
  Kartenkennung _____
  TT/MM/JJJJ

T TT/MM/JJJJ  (z)
A VIN _____
  Nat/Kennzeichen _____
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
o Reifengröße
> xxx km/h
x xxx xxx - x xxx xxx km
  
```

17 Zeiteinstellung

Blockbezeichner

```

-----G-----
  
```

17.1 Datensatz Zeiteinstellung

Datensatzbezeichner
 Datum und Uhrzeit, alt
 Datum und Uhrzeit, neu
 Werkstatt, die die Zeiteinstellung vorgenommen hat
 Anschrift der Werkstatt
 Werkstattkartenkennung
 Werkstattkarte gültig bis

```

-----
! G TT/MM/JJJJ hh:mm
  G TT/MM/JJJJ hh:mm
T Name_Werkstatt _____
  Anschrift_Werkstatt ____
  Kartenkennung _____
  TT/MM/JJJJ
  
```


18 Jüngste(s) in der FE aufgezeichnete(s) Ereignis und Störung

Blockbezeichner

Jüngstes Ereignis, Datum und Uhrzeit

Jüngste Störung, Datum und Uhrzeit

```

----- ! x A -----
! TT/MM/JJJJ hh:mm
x TT/MM/JJJJ hh:mm

```

19 Angaben zur Kontrolle Geschwindigkeitsüberschreitung (GÜ)

Blockbezeichner

Datum/Uhrzeit der letzten KONTROLLE GÜ

Datum/Uhrzeit der ersten Geschwindigkeitsüberschreitung und Anzahl der weiteren Überschreitungen seitdem

```

----- >> -----
> TT/MM/JJJJ hh:mm
>> TT/MM/JJJJ hh:mm (nnn)

```

20 Datensatz Geschwindigkeitsüberschreitung

20.1 Blockbezeichner ‚Erste Geschwindigkeitsüberschreitung nach der letzten Kalibrierung‘

```

----- >>T -----

```

20.2 Blockbezeichner ‚5 schwerste Geschwindigkeitsüberschreitungen in den letzten 365 Tagen‘

```

----- >> (365) -----

```

20.3 Blockbezeichner ‚Schwerste GÜ der letzten 10 Tage mit derartigen Ereignissen‘

```

----- >> (10) -----

```

20.4 Datensatzbezeichner

Datum, Uhrzeit und Dauer

Höchst- und Durchschnittsgeschwindigkeit, Anzahl ähnlicher Ereignisse an diesem Tag

Name des Fahrers

Vorname(n) des Fahrers

Fahrerkartenkennung

```

-----
>> TT/MM/JJJJ hh:mm hh:mm
xxx km/h xxx km/h (xxx)
@ Zuname _____
Vorname
Kartenkennung _____

```

20.5 Wenn in einem Block kein Datensatz für GÜ existiert

```

>> - - -

```

21 Handschriftliche Angaben

Blockbezeichner

21.1 Ort der Kontrolle

21.2 Unterschrift des Kontrolleurs

21.3 Anfangszeit

21.4 Endzeit

21.5 Unterschrift des Fahrers

```

-----
@ * .....
@ .....
@ + .....
+ @ .....
@ .....

```

‚Handschriftliche Angaben‘: Es sind so viele Leerzeilen über einem handschriftlichen Eintrag einzufügen, dass der Platz für die erforderlichen Angaben oder eine Unterschrift ausreicht.

3. SPEZIFIKATION DER AUSDRUCKE

In diesem Kapitel werden die folgenden Konventionen für die Notation verwendet:

N	Nummer N des Druckblocks oder -datensatzes
N	Nummer N des Druckblocks oder -datensatzes, Wiederholung so oft wie nötig
X/Y	Druckblöcke oder Datensätze X und/oder Y nach Bedarf, Wiederholung so oft wie nötig

3.1. Ausdruck Fahrertätigkeiten von der Karte

PRT_007 Der Ausdruck Fahrertätigkeiten von der Karte hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Kontrolleur (bei eingesteckter Kontrollkarte)
3	Angaben zum Fahrer (von der Karte, auf die sich Ausdruck bezieht)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
5	FE-Kennung (FE, mit der Ausdruck erstellt wird)
6	Letzte Kalibrierung dieser FE
7	Letzte Kontrolle des hier kontrollierten Fahrers
8	Begrenzungszeichen Fahrertätigkeiten
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Tätigkeiten des Fahrers in der Reihenfolge ihres Auftretens
11	Begrenzungszeichen Tageszusammenfassung
11.4	Eingegebene Orte in chronologischer Reihenfolge
11.5	Gesamtwerte Tätigkeiten
12.1	Begrenzungszeichen Ereignisse und Störungen von der Karte
12.4	Datensätze Ereignis/Störung (die letzten 5 auf Karte gespeicherten Ereignisse/Störungen)
13.1	Begrenzungszeichen Ereignisse oder Störungen von der FE
13.4	Datensätze Ereignis/Störung (die letzten 5 in der FE gespeicherten oder andauernden Ereignisse/Störungen)
21.1	Ort der Kontrolle
21.2	Unterschrift des Kontrolleurs
21.5	Unterschrift des Fahrers

3.2. Tagesausdruck Fahrertätigkeiten von der FE

PRT_008 Der Tagesausdruck Fahrertätigkeiten von der FE hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die FE eingesteckten Karten)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
5	FE-Kennung (FE, mit der Ausdruck erstellt wird)
6	Letzte Kalibrierung dieser FE
7	Letzte Kontrolle des hier kontrollierten Fahrers
9	Begrenzungszeichen Fahrertätigkeiten
10	Begrenzungszeichen Steckplatz Fahrer (Steckplatz 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Tätigkeiten in chronologischer Reihenfolge (Steckplatz Fahrer)
10	Begrenzungszeichen Steckplatz 2. Fahrer (Steckplatz 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Tätigkeiten in chronologischer Reihenfolge (Steckplatz 2. Fahrer)
11	Begrenzungszeichen Tageszusammenfassung
11.1	Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz Fahrer
11.4	Eingegebene Orte in chronologischer Reihenfolge
11.6	Gesamtwerte Tätigkeiten

11.2	Zusammenfassung der Zeitabschnitte ohne Karte im Steckplatz 2. Fahrer
11.4	Eingegebene Orte in chronologischer Reihenfolge
11.7	Gesamtwerte Tätigkeiten
11.3	Zusammenfassung der Tätigkeiten für einen Fahrer, beide Steckplätze
11.4	Von diesem Fahrer eingegebene Orte in chronologischer Reihenfolge
11.7	Gesamtwerte Tätigkeiten für diesen Fahrer
13.1	Begrenzungszeichen Ereignisse/Störungen
13.4	Datensätze Ereignis/Störung (die letzten 5 in der FE gespeicherten oder andauernden Ereignisse/Störungen)
21.1	Ort der Kontrolle
21.2	Unterschrift des Kontrolleurs
21.3	Anfangszeit (Raum, in dem ein Fahrer die zutreffenden Zeitabschnitte angeben kann)
21.4	Endzeit
21.5	Unterschrift des Fahrers

3.3. Ausdruck Ereignisse und Störungen von der Karte

PRT_009 Der Ausdruck Ereignisse und Störungen von der Karte hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Kontrolleur (bei eingesteckter Kontrollkarte)
3	Angaben zum Fahrer (von der Karte, auf die sich Ausdruck bezieht)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
12.2	Begrenzungszeichen Ereignisse
12.4	Ereignisdatensätze (alle auf der Karte gespeicherten Ereignisse)
12.3	Begrenzungszeichen Störungen
12.4	Störungsdatensätze (alle auf der Karte gespeicherten Ereignisse)
21.1	Ort der Kontrolle
21.2	Unterschrift des Kontrolleurs
21.5	Unterschrift des Fahrers

3.4. Ausdruck Ereignisse und Störungen von der FE

PRT_010 Der Ausdruck Ereignisse und Störungen von der FE hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die FE eingesteckten Karten)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
13.2	Begrenzungszeichen Ereignisse
13.4	Ereignisdatensätze (alle in der FE gespeicherten oder andauernden Ereignisse)
13.3	Begrenzungszeichen Störungen
13.4	Störungsdatensätze (alle in der FE gespeicherten oder andauernden Ereignisse)
21.1	Ort der Kontrolle
21.2	Unterschrift des Kontrolleurs
21.5	Unterschrift des Fahrers

3.5. Ausdruck Technische Daten

PRT_011 Der Ausdruck Technische Daten hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die FE eingesteckten Karten)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
14	FE-Kennung
15	Sensorkennung
16	Begrenzungszeichen Kalibrierungsdaten
16.1	Kalibrierungsdatensätze (alle verfügbaren Datensätze in chronologischer Reihenfolge)
17	Begrenzungszeichen Zeiteinstellung
17.1	Datensätze Zeiteinstellung (alle verfügbaren Datensätze für Zeiteinstellung und Kalibrierung)
18	Jüngste(s) in der FE aufgezeichnete(s) Ereignis und Störung

3.6. Ausdruck Geschwindigkeitsüberschreitung

PRT_012 Der Ausdruck Geschwindigkeitsüberschreitung hat folgendes Format:

1	Datum und Uhrzeit des Ausdrucks
2	Art des Ausdrucks
3	Angaben zum Karteninhaber (für alle in die FE eingesteckten Karten)
4	Fahrzeugkennung (Fahrzeug, von dem der Ausdruck erstellt wird)
19	Information Kontrolle Geschwindigkeitsüberschreitung
20.1	Kennung Daten Geschwindigkeitsüberschreitung
20.4 / 20.5	Erste Geschwindigkeitsüberschreitung nach der letzten Kalibrierung
20.2	Kennung Daten Geschwindigkeitsüberschreitung
20.4 / 20.5	Die 5 schwersten GÜ in den letzten 365 Tagen
20.3	Kennung Daten Geschwindigkeitsüberschreitung
20.4 / 20.5	Die schwersten GÜ der letzten 10 Tage mit derartigen Ereignissen
21.1	Ort der Kontrolle
21.2	Unterschrift des Kontrolleurs
21.5	Unterschrift des Fahrers

Anlage 5

ANZEIGE

In dieser Anlage werden folgende Konventionen für die Notation verwendet:

- Zeichen in **Fettdruck** stehen für anzuzeigenden Klartext (in der Anzeige erscheinen die Zeichen unformatiert).
- Unformatierte Zeichen stehen für Variablen (Piktogramme oder Daten), die in der Anzeige durch ihre Werte ersetzt werden:
 - TT MM JJJJ: Tag, Monat, Jahr,
 - hh: Stunden,
 - mm: Minuten,
 - D: Piktogramm Dauer,
 - EF: Piktogrammkombination Ereignis oder Störung,
 - O: Piktogramm Betriebsart.

DIS_001 Die Anzeige von Daten durch das Kontrollgerät erfolgt in folgendem Format:

Daten	Format
Standardanzeige	
Ortszeit	hh:mm
Betriebsart	O
Information zum Fahrer	1 Dhhmm hhmm
Information zum 2. Fahrer	2 Dhhmm
Betriebsart „Kontrollgerät nicht erforderlich“ eingeschaltet	OUT
Warnanzeige	
Überschreitung der ununterbrochenen Lenkzeit	1 0 hhmm hhmm
Ereignis oder Störung	EF
Sonstige Anzeigen	
UTC-Datum	UTC 0 TT/MM/JJJJ oder UTC 0 TT.MM.JJJJ
Uhrzeit	hh:mm
Ununterbrochene Lenkzeit und kumulative Pausenzeit des Fahrers	1 0 hhmm hhmm
Ununterbrochene Lenkzeit und kumulative Pausenzeit des 2. Fahrers	2 0 hhmm hhmm
Kumulierte Lenkzeit des Fahrers für die Vorwoche und die laufende Woche	1 0 hhhhmm
Kumulierte Lenkzeit des 2. Fahrers für die Vorwoche und die laufende Woche	2 0 hhhhmm

*Anlage 6***EXTERNE SCHNITTSTELLEN**

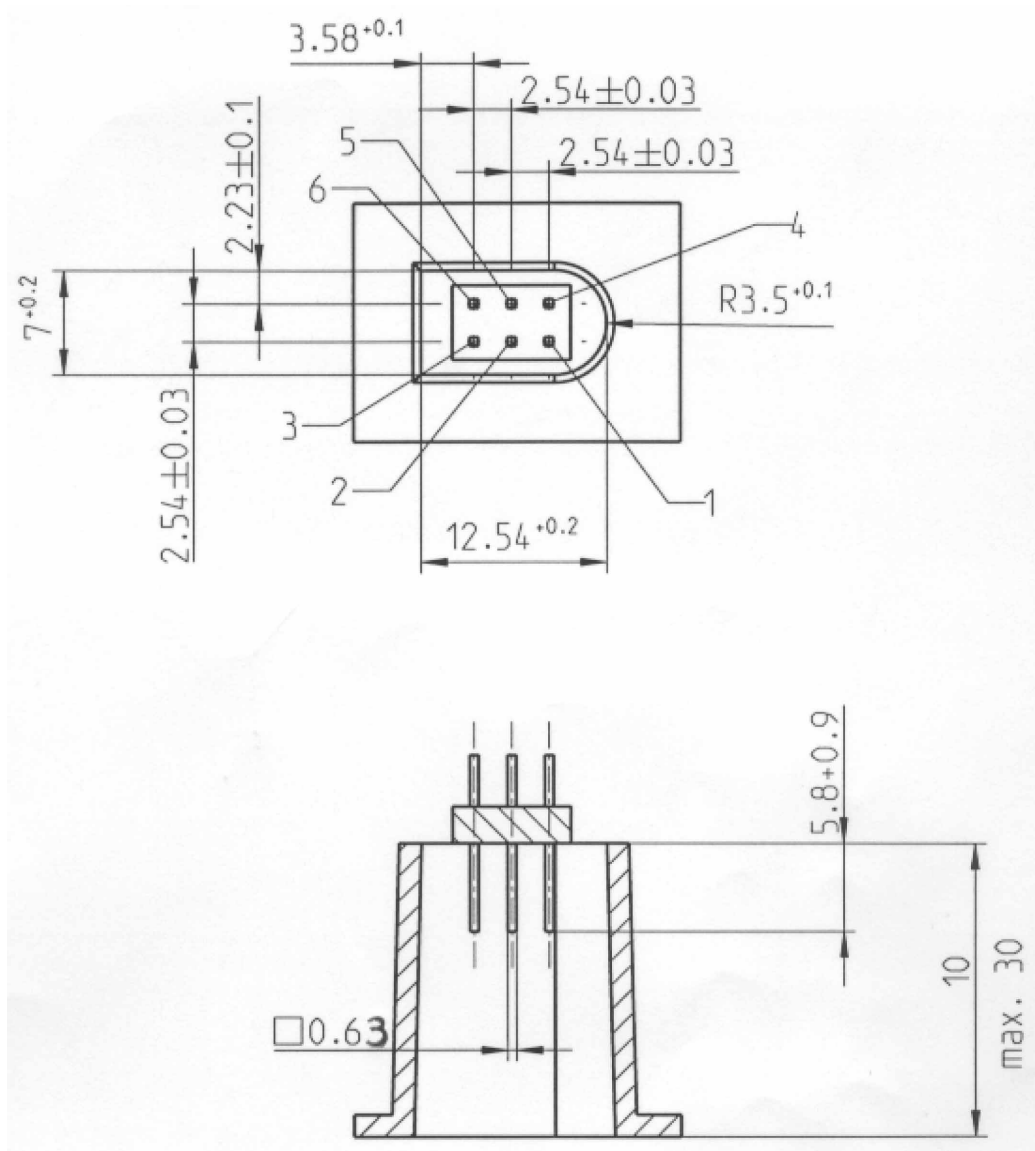
INHALTSVERZEICHNIS

1.	Hardware	144
1.1.	Steckverbinder	144
1.2.	Belegung der Kontakte	146
1.3.	Blockschaltbild	146
2.	Schnittstelle zum Herunterladen	146
3.	Kalibrierungsschnittstelle	147

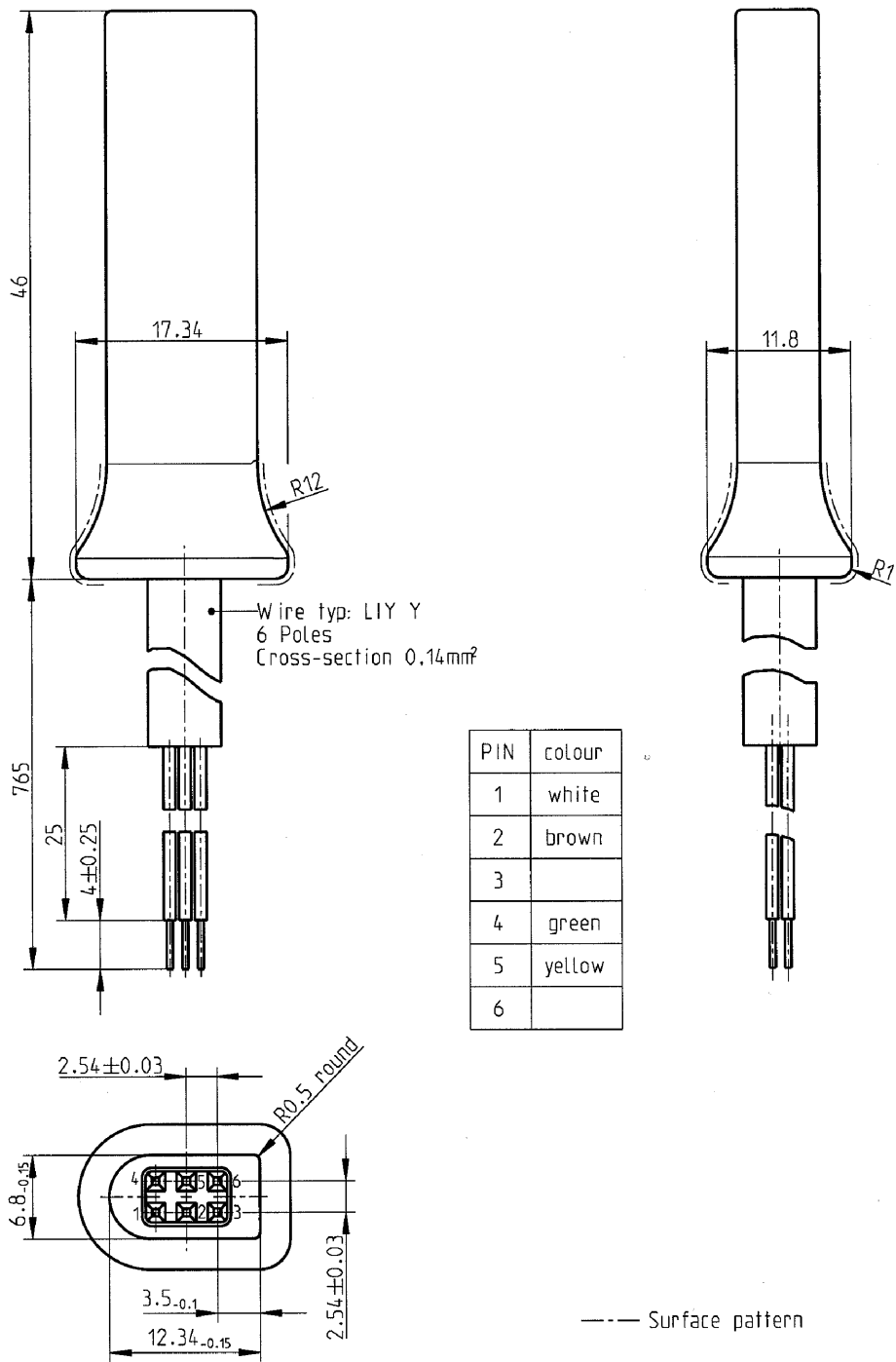
1. HARDWARE

1.1. Steckverbinder

INT_001 Das Herunterladen/Kalibrieren erfolgt über eine sechspolige Steckverbindung, die an der Frontplatte zugänglich ist, ohne dass ein Teil des Kontrollgeräts abgetrennt werden muss. Sie ist entsprechend der folgenden Abbildung auszulegen (sämtliche Maßangaben in mm):



Die folgende Abbildung zeigt einen typischen sechspoligen Stecker:



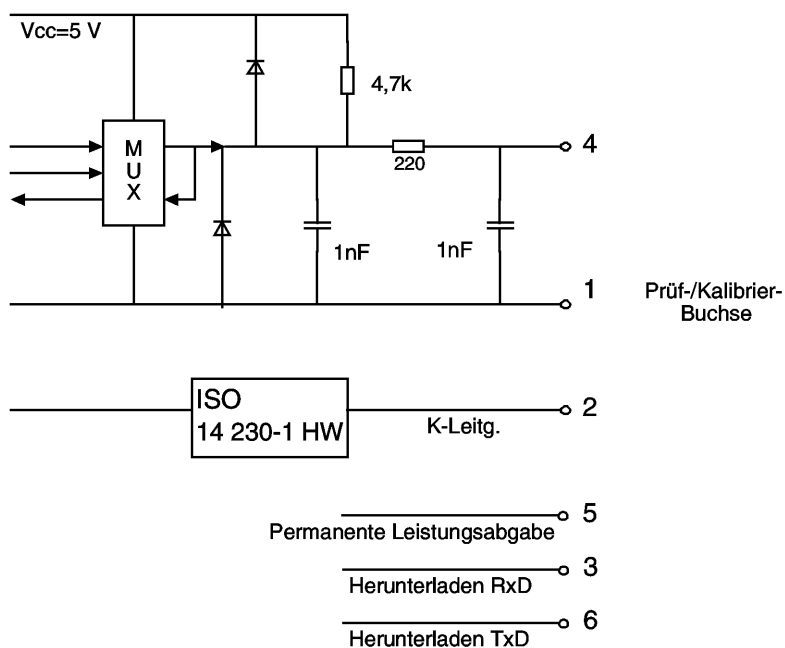
1.2. Belegung der Kontakte

INT_002 Die Kontakte sind entsprechend der nachstehenden Tabelle zu belegen:

Stift	Beschreibung	Anmerkung
1	Batterie minus	Zum Minuspol der Fahrzeugbatterie
2	Datenkommunikation	K-Leitung (ISO 14230-1)
3	RxD — Herunterladen	Dateneingang Kontrollgerät
4	Eingabe-/Ausgabesignal	Kalibrierung
5	Dauerausgangsleistung	Zur Berücksichtigung des Spannungsabfalls am Schutzstromkreis entspricht der Spannungsbereich dem des Fahrzeugs minus 3 V Ausgangsleistung: 40 mA
6	TxD — Herunterladen	Datenausgang Kontrollgerät

1.3. Blockschaltbild

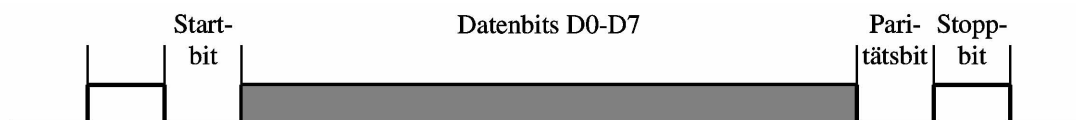
INT_003 Folgendes Blockschaltbild ist vorgegeben:



2. SCHNITTSTELLE ZUM HERUNTERLADEN

INT_004 Die Schnittstelle zum Herunterladen entspricht den RS232-Spezifikationen.

INT_005 Die Schnittstelle zum Herunterladen verwendet ein Startbit, 8 Datenbits mit dem niedrigstwertigen Bit an erster Stelle, ein Bit geradzahlgiger Parität und 1 Stoppbit.



Aufbau der Datenbytes: Startbit Ein Bit mit dem Logikpegel 0

Datenbits: An erster Stelle Übertragung des niedrigstwertigen Bits

Paritätsbit: Gerade Parität

Stoppbit: Ein Bit mit dem Logikpegel 1

Bei der Übermittlung numerischer Daten, die aus mehr als einem Byte bestehen, wird das höchstwertige Byte an erster Stelle und das niedrigstwertige Byte an letzter Stelle übertragen.

INT_006 Die Baudrate bei der Übertragung ist zwischen 9 600 und 11 5200 bit/s einstellbar. Die Übertragung hat mit der höchstmöglichen Übertragungsgeschwindigkeit zu erfolgen, wobei die anfängliche Bitgeschwindigkeit nach dem Aufbau der Verbindung auf 9 600 bit/s gesetzt wird.

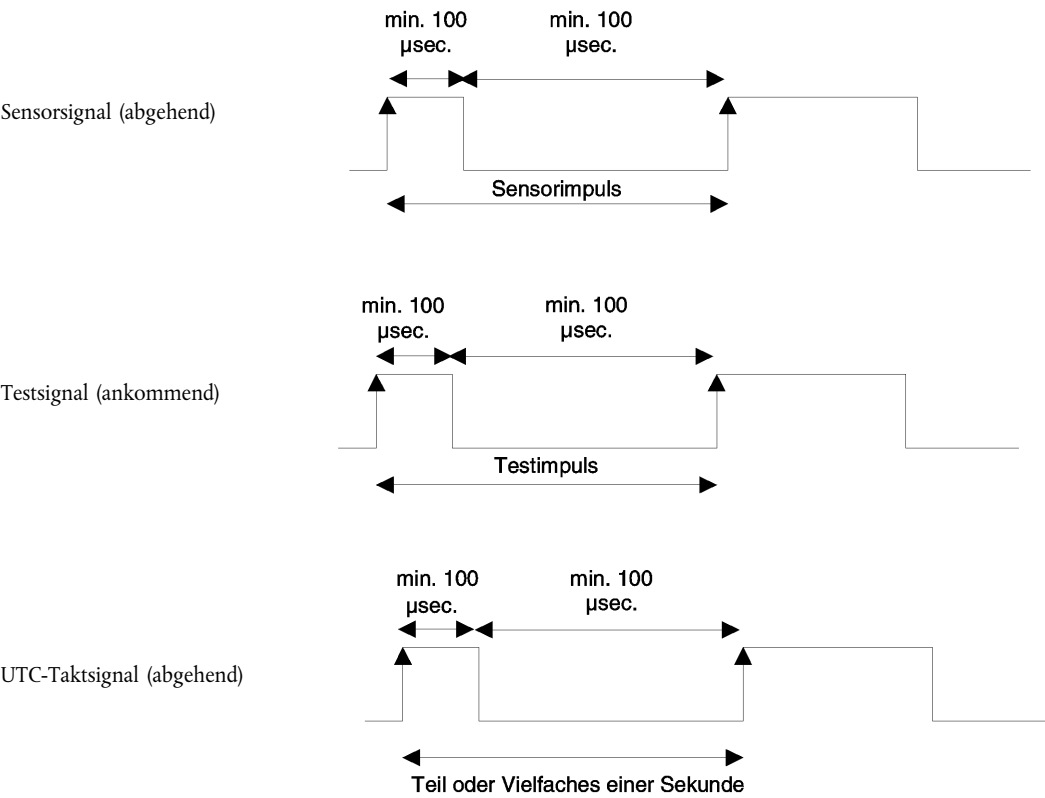
3. KALIBRIERUNGSSCHNITTSTELLE

INT_007 Die Datenkommunikation erfolgt nach ISO 14230-1 Straßenfahrzeuge — Diagnosesysteme — Schlüsselwort 2000 — Teil 1: Bitübertragungsschicht, 1999.

INT_008 Das Eingabe-/Ausgabesignal entspricht den folgenden elektrischen Spezifikationen:

Parameter	Minimum	Typisch	Maximum	Anmerkung
U _L -Pegel (Eingang)			1,0 V	I = 750 µA
U _H -Pegel (Eingang)	4 V			I = 200 µA
Frequenz			4 kHz	
U _L -Pegel (Ausgang)			1,0 V	I = 1 mA
U _H -Pegel (Ausgang)	4 V			I = 1 mA

INT_009 Für das Eingabe-/Ausgabesignal gelten die folgenden Zeitdiagramme:



Anlage 7

PROTOKOLLE ZUM HERUNTERLADEN DER DATEN

INHALTSVERZEICHNIS

1.	Einleitung	150
1.1.	Geltungsbereich	150
1.2.	Akronyme und Notation	150
2.	Herunterladen von Daten von der Fahrzeugeinheit	151
2.1.	Download-Verfahren	151
2.2.	Datendownload-Protokoll	151
2.2.1.	Nachrichtenstruktur	151
2.2.2.	Nachrichtentypen	152
2.2.2.1.	Start Communication Request (SID 81)	154
2.2.2.2.	Positive Response Start Communication (SID C1)	154
2.2.2.3.	Start Diagnostic Session Request (SID 10)	154
2.2.2.4.	Positive Response Start Diagnostic (SID 50)	154
2.2.2.5.	Link Control Service (SID 87)	154
2.2.2.6.	Link Control Positive Response (SID C7)	154
2.2.2.7.	Request Upload (SID 35)	154
2.2.2.8.	Positive Response Request Upload (SID 75)	154
2.2.2.9.	Transfer Data Request (SID 36)	154
2.2.2.10.	Positive Response Transfer Data (SID 76)	155
2.2.2.11.	Request Transfer Exit (SID 37)	155
2.2.2.12.	Positive Response Request Transfer Exit (SID 77)	155
2.2.2.13.	Stop Communication Request (SID 82)	155
2.2.2.14.	Positive Response Stop Communication (SID C2)	155
2.2.2.15.	Acknowledge Sub Message (SID 83)	155
2.2.2.16.	Negative Response (SID 7F)	155
2.2.3.	Nachrichtenfluss	156
2.2.4.	Timing	157
2.2.5.	Fehlerbehandlung	157
2.2.5.1.	Start Communication-Phase	157
2.2.5.2.	Communication-Phase	157
2.2.6.	Inhalt der Antwortnachricht	160
2.2.6.1.	Positive Response Transfer Data Overview	160
2.2.6.2.	Positive Response Transfer Data Activities	161
2.2.6.3.	Positive Response Transfer Data Events and Faults	162

2.2.6.4.	Positive Response Transfer Data Detailed Speed	163
2.2.6.5.	Positive Response Transfer Data Technical Data	163
2.3.	ESM-Datenspeicherung	164
3.	Protokoll für das Herunterladen von Daten von Kontrollgerätkarten	164
3.1.	Geltungsbereich	164
3.2.	Begriffsbestimmungen	164
3.3.	Herunterladen von der Karte	164
3.3.1.	Initialisierungssequenz	165
3.3.2.	Sequenz für unsignierte Dateien	165
3.3.3.	Sequenz für signierte Dateien	165
3.3.4.	Sequenz für das Zurücksetzen des Kalibrierungszählers	166
3.4.	Datenspeicherungsformat	166
3.4.1.	Einleitung	166
3.4.2.	Dateiformat	166
4.	Herunterladen von der Kontrollgerätkarte über eine Fahrzeugeinheit	167

1. EINLEITUNG

Diese Anlage enthält die Spezifizierung der Verfahren für die verschiedenen Arten der Übertragung der Daten von der Karte auf ein externes Speichermedium (ESM) sowie die Protokolle, die zur Sicherung der korrekten Datenübertragung und der vollständigen Kompatibilität des heruntergeladenen Datenformats zu implementieren sind, damit ein Kontrolleur diese Daten inspizieren und vor ihrer Analyse ihre Echtheit und Integrität kontrollieren kann.

1.1. Geltungsbereich

Das Herunterladen von Daten auf ein ESM kann erfolgen:

- von einer Fahrzeugeinheit (FE) durch ein an die FE angeschlossenes Intelligent Dedicated Equipment (IDE),
- von einer Kontrollgerätkarte durch ein mit einem Kartenschnittstellengerät (IFD) ausgestattetes IDE,
- von einer Kontrollgerätkarte über eine Fahrzeugeinheit durch ein an die FE angeschlossenes IDE.

Um eine Prüfung der Echtheit und Integrität der auf einem ESM gespeicherten heruntergeladenen Daten zu ermöglichen, werden die Daten mit einer gemäß Anlage 11 (Gemeinsame Sicherheitsmechanismen) angefügten Signatur heruntergeladen. Ebenfalls heruntergeladen werden die Kennung des Ursprungsgeräts (FE oder Karte) und dessen Sicherheitszertifikat (Mitgliedstaatszertifikat und Gerätezertifikat). Der Prüfer der Daten muss einen zuverlässigen europäischen öffentlichen Schlüssel besitzen.

DDP_001 Die während eines Download-Vorgangs heruntergeladenen Daten müssen auf dem ESM in einer einzigen Datei gespeichert werden.

1.2. Akronyme und Notation

In dieser Anlage werden folgende Akronyme verwendet:

AID	Application Identifier (Anwendungskennung)
ATR	Answer To Reset (Antwort auf Zurücksetzen)
CS	Checksum Byte (Prüfsummenbyte)
DF	Dedicated File (Verzeichnis)
DS_	Diagnostic Session (Diagnosevorgang)
EF	Elementary File (Elementardatei)
ESM	External Storage Medium (externes Speichermedium)
FE	Fahrzeugeinheit
FID	File Identifier (File ID, Dateikennung)
FMT	Formatbyte (erstes Byte eines Nachrichtenkopfes)
ICC	Integrated Circuit Card (Chipkarte)
IDE	Intelligent Dedicated Equipment: Gerät, das zum Herunterladen von Daten auf das ESM verwendet wird (z. B. Personalcomputer)
IFD	Interface Device (Schnittstellengerät, Kartenterminal)
KWP	Keyword Protocol 2000
LEN	Längenbyte (letztes Byte eines Nachrichtenkopfes)
PPS	Protocol Parameter Selection (Auswahl der Protokollparameter)
PSO	Perform Security Operation (Sicherheitsoperation ausführen)
SID	Service Identifier
SRC	Source Byte (Quellbyte)
TGT	Target Byte (Zielbyte)
TLV	Taglängenwert
TREP	Transfer Response Parameter (Antwortübertragungsparameter)
TRTP	Transfer Request Parameter (Anfrageübertragungsparameter)

2. HERUNTERLADEN VON DATEN VON DER FAHRZEUGEINHEIT

2.1. Download-Verfahren

Zur Durchführung eines FE-Datendownloads muss der Bediener folgende Arbeitsschritte ausführen:

- Einführen seiner Kontrollgerätkarte in einen Steckplatz der FE ⁽¹⁾;
- Anschließen des IDE an den FE-Anschluss zum Herunterladen;
- Herstellen der Verbindung zwischen IDE und FE;
- Auswählen der herunterzuladenden Daten auf dem IDE und Senden der Anforderung an die FE;
- Beenden des Download-Vorgangs.

2.2. Datendownload-Protokoll

Das Protokoll ist auf Master/Slave-Basis aufgebaut, wobei das IDE den Master und die FE den Slave bildet.

Nachrichtenstruktur, -typ und -fluss beruhen prinzipiell auf dem Keyword Protocol 2000 (KWP) (ISO 14230-2 Straßenfahrzeuge — Diagnosesysteme — Schlüsselwort 2000 — Teil 2: Sicherungsschicht).

Die Anwendungsschicht beruht grundsätzlich auf dem aktuellen Normentwurf ISO 14229-1 (Straßenfahrzeuge — Diagnosesysteme — Teil 1: Diagnosedienste, Version 6 vom 22. Februar 2001).

2.2.1. Nachrichtenstruktur

DDP_002 Alle zwischen dem IDE und der FE ausgetauschten Nachrichten sind mit einer dreiteiligen Struktur formatiert, die sich zusammensetzt aus

- dem Kopf, bestehend aus einem Formatbyte (FMT), einem Zielbyte (TGT), einem Quellbyte (SRC) und möglicherweise einem Längenbyte (LEN),
- dem Datenfeld, bestehend aus einem Service-Identifizier-Byte (SID) und einer variablen Anzahl von Datenbytes, z. B. ein optionales Diagnostic-Session-Byte (DS_) oder ein optionales Transfer-Parameter-Byte (TRTP oder TREP).
- der Prüfsumme, bestehend aus einem Prüfsummenbyte (CS).

Kopf				Datenfeld					Prüfsumme
FMT	TGT	SRC	LEN	SID	DATA	...	...	...	CS
4 Bytes				Max. 255 Bytes					1 Byte

TGT- und SRC-Byte stellen die physische Adresse des Empfängers und des Absenders der Nachricht dar. Die Werte sind F0 Hex für das IDE und EE Hex für die FE.

Das LEN-Byte ist die Länge des Datenfeldteils.

Das Prüfsummenbyte ist die 8-Bit-Summenreihe modulo 256 aller Bytes der Nachricht außer CS selbst.

Die Bytes FMT, SID, DS_, TRTP und TREP werden an anderer Stelle dieses Dokuments definiert.

⁽¹⁾ Die eingesetzte Karte löst die erforderlichen Zugriffsrechte für die Herunterladefunktion und die Daten aus.

DDP_003 Sind die von der Nachricht aufzunehmenden Daten länger als der im Datenfeldteil zur Verfügung stehende Platz, wird die Nachricht in mehreren Teilnachrichten gesendet. Jede Teilnachricht hat einen Kopf, die gleiche SID, TREP sowie einen 2-Byte-Teilnachrichtenzähler, der die Teilnachrichtnummer innerhalb der Gesamtnachricht angibt. Damit Fehlerprüfung und Abbruch möglich sind, bestätigt das IDE jede Teilnachricht. Das IDE kann die Teilnachricht annehmen, ihre erneute Übertragung anfordern sowie die FE zum Neubeginn oder zum Abbruch der Übertragung auffordern.

DDP_004 Enthält die letzte Teilnachricht genau 255 Bytes im Datenfeld, muss eine abschließende Teilnachricht mit leerem Datenfeld (außer SID, TREP und Teilnachrichtenzähler) angefügt werden, die das Ende der Nachricht anzeigt.

Beispiel:

Kopf	SID	TREP	Nachricht	CS
4 Bytes	Länger als 255 Bytes			

wird übertragen als:

Kopf	SID	TREP	00	01	Teilnachricht 1	CS
4 Bytes	255 Bytes					

Kopf	SID	TREP	00	02	Teilnachricht 2	CS
4 Bytes	255 Bytes					

...

Kopf	SID	TREP	xx	yy	Teilnachricht n	CS
4 Bytes	Weniger als 255 Bytes					

oder als:

Kopf	SID	TREP	00	01	Teilnachricht 1	CS
4 Bytes	255 Bytes					

Kopf	SID	TREP	00	02	Teilnachricht 2	CS
4 Bytes	255 Bytes					

...

Kopf	SID	TREP	xx	yy	Teilnachricht n	CS
4 Bytes	255 Bytes					

Kopf	SID	TREP	xx	yy+1	CS
4 Bytes	4 Bytes				

2.2.2. Nachrichtentypen

Das Kommunikationsprotokoll für das Herunterladen von Daten zwischen der FE und dem IDE verlangt den Austausch von 8 verschiedenen Nachrichtentypen.

In der folgenden Tabelle sind diese Nachrichten zusammengefasst.

Nachrichtenstruktur	Max. 4 Bytes Kopf				Max. 255 Bytes Daten			1 Byte Prüfsumme
	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
IDE ->	<- FE							
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		8F,EA	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Baud	80	EE	F0	04	87		01,01,01	EC
19 200 Baud	80	EE	F0	04	87		01,01,02	ED
38 400 Baud	80	EE	F0	04	87		01,01,03	ED
57 600 Baud	80	EE	F0	04	87		01,01,04	EF
115 200 Baud	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00,00,FF,FF,FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06		9C
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Anmerkungen:

- Sid Req = Sid der entsprechenden Anforderung.
- TREP = der TRTP der entsprechenden Anforderung.
- Geschwärzte Felder zeigen an, dass nichts übertragen wird.
- Der Ausdruck 'Upload' (vom IDE aus gesehen) wird in Anlehnung an die ISO 14229 verwendet. Er bedeutet dasselbe wie 'Download' (von der FE aus gesehen).
- Mögliche 2-Byte-Teilnachrichtenzähler sind in dieser Tabelle nicht aufgeführt.

2.2.2.1. Start Communication Request (SID 81)

- DDP_005 Diese Nachricht wird vom IDE zum Aufbau der Kommunikationsverbindung mit der FE ausgegeben. Der Verbindungsaufbau und die Kommunikation erfolgt anfangs stets mit einer Datenrate von 9 600 Baud (solange die Übertragungsgeschwindigkeit nicht durch einen Link Control Service (Verbindungssteuerungsdienst) geändert wird).

2.2.2.2. Positive Response Start Communication (SID C1)

- DDP_006 Diese Nachricht wird von der FE als positive Antwort auf einen Start Communication Request ausgegeben. Sie enthält die beiden Schlüsselbytes ‚8F‘, ‚EA‘ als Hinweis darauf, dass die Einheit das Protokoll mit Kopf einschließlich Ziel-, Quell- und Längeninformation unterstützt.

2.2.2.3. Start Diagnostic Session Request (SID 10)

- DDP_007 Die Nachricht Start Diagnostic Session Request wird vom IDE ausgegeben, um einen neuen Diagnosevorgang mit der FE zu beginnen. Die Untervariable ‚default session‘ (81 Hex) zeigt an, dass ein Standard-Diagnosevorgang eingeleitet werden soll.

2.2.2.4. Positive Response Start Diagnostic (SID 50)

- DDP_008 Die Nachricht Positive Response Start Diagnostic wird von der FE als positive Antwort auf einen Diagnostic Session Request gesendet.

2.2.2.5. Link Control Service (SID 87)

- DDP_052 Mit Hilfe des Link Control Service (Verbindungssteuerungsdienst) leitet die IDE einen Wechsel der Übertragungsgeschwindigkeit (Baudrate) ein. Dies erfolgt in zwei Schritten. Zunächst schlägt die IDE einen Wechsel vor und gibt dazu die neue Baudrate an. Nach einer positiven Antwort der FE sendet die IDE dann im zweiten Schritt eine Bestätigung des Geschwindigkeitswechsels an die FE und geht danach zur neuen Baudrate über. Nach Erhalt der Bestätigung geht auch die FE zur neuen Baudrate über.

2.2.2.6. Link Control Positive Response (SID C7)

- DDP_053 Die Nachricht Link Control Positive Response wird von der FE als positive Antwort auf einen Link Control Service Request (Schritt 1) gesendet. Die Bestätigungsmeldung (Schritt 2) wird dagegen nicht beantwortet.

2.2.2.7. Request Upload (SID 35)

- DDP_009 Die Nachricht Request Upload wird vom IDE als Mitteilung an die FE ausgegeben, dass eine Download-Operation angefordert wird. In Übereinstimmung mit der ISO 14229 umfasst diese Anforderung stets Angaben zu Adresse, Größe und Format der angeforderten Daten. Da diese Angaben der IDE jedoch vor dem Herunterladen nicht bekannt sind, wird die Speicheradresse auf ‚0‘, das Format auf ‚verschlüsselt und unkomprimiert‘ und die Speichergröße auf den Höchstwert gesetzt.

2.2.2.8. Positive Response Request Upload (SID 75)

- DDP_010 Die Nachricht Positive Response Request Upload wird von der FE gesendet, um dem IDE anzuzeigen, dass die FE zum Herunterladen der Daten bereit ist. In Übereinstimmung mit der ISO 14229 enthält diese Positive-Response-Nachricht auch Daten, mit denen der IDE mitgeteilt wird, dass die spätere Nachrichten Positive Response Transfer Data höchstens 00FF Hex Bytes umfassen werden.

2.2.2.9. Transfer Data Request (SID 36)

- DDP_011 Die Nachricht Transfer Data Request wird vom IDE gesendet und spezifiziert der FE den herunterzuladenden Datentyp. Mit dem Byte Transfer Request Parameter (TRTP) wird die Übertragungsart angegeben.

Es gibt sechs Arten der Datenübertragung:

- Überblick (TRTP 01),
- Tätigkeiten eines bestimmten Tages (TRTP 02),
- Ereignisse und Störungen (TRTP 03),
- Genaue Geschwindigkeitsangaben (TRTP 04),
- Technische Daten (TRTP 05),
- Kartendownload (TRTP 06).

DDP_054 Die IDE muss beim Herunterladen eine Überblicks-Datenübertragung (TRTP 01) anfordern, da nur so die FE-Zertifikate in der heruntergeladenen Datei gespeichert werden (und die digitale Signatur geprüft werden kann).

Im zweiten Fall (TRTP 02) schließt die Nachricht Transfer Data Request die Angabe des herunterzuladenden Kalendertags (Format TimeReal) ein.

2.2.2.10. Positive Response Transfer Data (SID 76)

DDP_012 Die Nachricht Positive Response Transfer Data wird von der FE als Antwort auf die Transfer Data Request gesendet. Sie enthält die angeforderten Daten, wobei die Transfer Response Parameter (TREP) den TRTP der Anforderung entspricht.

DDP_055 Im ersten Fall (TREP 01), sendet die FE Daten, die es dem IDE-Bediener erleichtern, die von ihm herunterzuladenden Daten auszuwählen. Diese Nachricht enthält folgende Informationen:

- Sicherheitszertifikate,
- Fahrzeugkennung,
- aktuelles Datum und Uhrzeit der FE,
- min. und max. herunterladbares Datum (FE-Daten),
- Angabe der in die FE eingesteckten Karten,
- der vorherige Download an ein Unternehmen,
- Unternehmenssperrern,
- bisherige Kontrollen.

2.2.2.11. Request Transfer Exit (SID 37)

DDP_013 Mit der Nachricht Request Transfer Exit teilt das IDE der FE mit, dass der Download-Vorgang beendet ist.

2.2.2.12. Positive Response Request Transfer Exit (SID 77)

DDP_014 Die Nachricht Positive Response Request Transfer Exit wird von der FE zur Quittierung der Request Transfer Exit gesendet.

2.2.2.13. Stop Communication Request (SID 82)

DDP_015 Die Nachricht Stop Communication Request wird vom IDE gesendet, um die Kommunikationsverbindung mit der FE zu trennen.

2.2.2.14. Positive Response Stop Communication (SID C2)

DDP_016 Mit der Nachricht Positive Response Stop Communication quittiert die FE die Nachricht Stop Communication Request.

2.2.2.15. Acknowledge Sub Message (SID 83)

DDP_017 Mit der Nachricht Acknowledge Sub Message bestätigt das IDE den Empfang der einzelnen Teile einer Nachricht, die in mehreren Teilnachrichten gesendet wird. Das Datenfeld enthält die von der FE empfangene SID sowie einen 2-Byte-Code wie folgt:

- MsgC + 1 quittiert den korrekten Empfang der Teilnachricht Nummer MsgC.
Anforderung vom IDE an die FE zur Sendung der nächsten Teilnachricht.
- MsgC zeigt ein Problem beim Empfang der Teilnachricht Nummer MsgC an.
Anforderung von IDE an die FE zur erneuten Sendung der Teilnachricht.
- FFFF fordert zur Beendigung der Nachricht auf.

Kann vom IDE zur Beendigung der Übertragung der FE-Nachricht aus irgendeinem Grund verwendet werden.

Die letzte Teilnachricht einer Nachricht (LEN-Byte < 255) kann unter Verwendung eines dieser Codes oder gar nicht quittiert werden.

Folgende FE-Antwort besteht aus mehreren Teilnachrichten:

- Positive Response Transfer Data (SID 76).

2.2.2.16. Negative Response (SID 7F)

DDP_018 Die Nachricht Negative Response wird von der FE als Antwort auf die obengenannten Anforderungsnachrichten gesendet, wenn sie die Anforderung nicht erfüllen kann. Die Datenfelder der Nachricht enthalten die SID der Antwort (7F), die SID der Anforderung sowie einen Code zur Angabe des Grundes der negativen Antwort. Folgende Codes stehen zur Verfügung:

- 10 general reject
Aktion kann aus einem im Folgenden nicht aufgeführten Grund nicht ausgeführt werden.
- 11 service not supported
Die SID der Anforderung wird nicht verstanden.
- 12 sub function not supported
Die DS_ oder TRTP der Anforderung wird nicht verstanden, oder es sind keine weiteren Teilnachrichten zu übertragen.
- 13 incorrect message length
Die Länge der erhaltenen Nachricht ist nicht korrekt.
- 22 conditions not correct or request sequence error
Der angeforderte Dienst ist nicht aktiv oder die Reihenfolge der Anforderungsnachrichten ist nicht korrekt.
- 31 Request out of range
Der Parameterdatensatz der Anforderung (Datenfeld) ist ungültig.
- 50 upload not accepted
Die Anforderung kann nicht ausgeführt werden (FE in einem nicht geeigneten Modus oder interne Störung der FE).
- 78 response pending
Die angeforderte Aktion kann nicht rechtzeitig abgeschlossen werden, und die FE ist nicht bereit, eine weitere Anforderung anzunehmen.
- FA data not available
Das Datenobjekt einer Datenübertragungsanforderung ist in der FE nicht verfügbar (z. B. keine Karte eingesetzt, ...).

2.2.3. Nachrichtenfluss

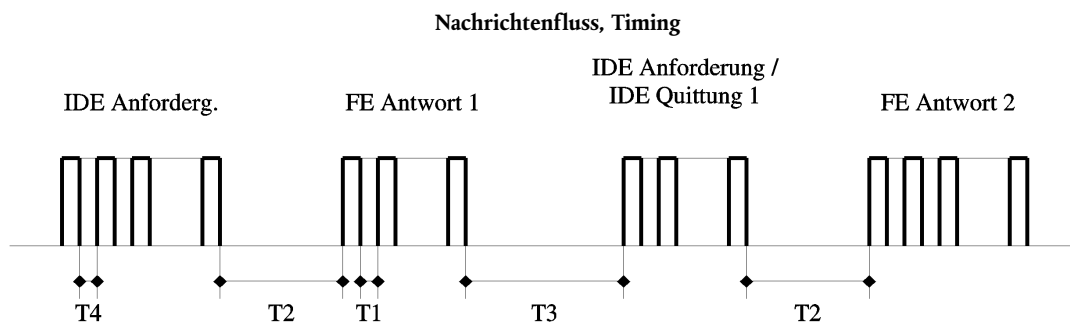
Ein typischer Nachrichtenfluss während einer normalen Datendownload-Prozedur sieht folgendermaßen aus:

IDE		FE
Start Communication Request	⇒ ⇐	Positive Response
Start Diagnostic Service Request	⇒ ⇐	Positive Response
Request Upload	⇒ ⇐	Positive Response
Transfer Data Request Overview	⇒ ⇐	Positive Response
Transfer Data Request #2	⇒ ⇐	Positive Response #1
Acknowledge Sub Message #1	⇒ ⇐	Positive Response #2
Acknowledge Sub Message #2	⇒ ⇐	Positive Response #m
Acknowledge Sub Message #m	⇒ ⇐	Positive Response (Data Field < 255 Bytes)
Acknowledge Sub Message (optional)	⇒	
...		
Transfer Data Request #n	⇒ ⇐	Positive Response
Request Transfer Exit	⇒ ⇐	Positive Response
Stop Communication Request	⇒ ⇐	Positive Response

2.2.4. Timing

DDP_019 Während des normalen Betriebs sind die in der folgenden Abbildung dargestellten Timing-Parameter relevant:

Abbildung 1



Hierbei sind:

- P1 = Zeit zwischen den Bytes bei FE-Antwort.
- P2 = Zeit zwischen dem Ende der IDE-Anforderung und dem Beginn der FE-Antwort bzw. zwischen dem Ende der IDE-Quittung und dem Beginn der nächsten FE-Antwort.
- P3 = Zeit zwischen dem Ende der FE-Antwort und dem Beginn der neuen IDE-Anforderung bzw. zwischen dem Ende der FE-Antwort und dem Beginn der IDE-Quittung bzw. zwischen dem Ende der IDE-Anforderung und dem Beginn der neuen IDE-Anforderung, wenn FE nicht antwortet.
- P4 = Zeit zwischen den Bytes bei IDE-Anforderung.
- P5 = Erweiterter Wert von P3 für das Herunterladen der Karte.

Die zulässigen Werte für die Timing-Parameter sind in der folgenden Tabelle aufgeführt (KWP — erweiterter Timing-Parametersatz, verwendet bei physischer Adressierung zwecks schnellerer Kommunikation).

Timing-Parameter	Unterer Grenzwert (ms)	Oberer Grenzwert (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 Minuten

(*) Wenn die FE mit einer negativen Antwort reagiert, die einen Code mit der Bedeutung „Anforderung korrekt empfangen, Antwort kommt“ enthält, wird dieser Wert auf den gleichen oberen Grenzwert erweitert wie P3.

2.2.5. Fehlerbehandlung

Tritt während des Nachrichtenaustauschs ein Fehler auf, erfolgt eine Modifizierung des Nachrichtenflusses in Abhängigkeit von dem Gerät, das den Fehler erkannt hat, sowie von der Nachricht, die den Fehler hervorgerufen hat.

In Abbildung 2 und 3 sind die Fehlerbehandlungsprozeduren für die FE bzw. für das IDE dargestellt.

2.2.5.1. Start Communication-Phase

DDP_020 Erkennt das IDE einen Fehler während der Start Communication-Phase entweder durch Timing oder durch den Bitstrom, wartet es P3min bis zur erneuten Ausgabe der Anforderung.

DDP_021 Erkennt die FE einen Fehler in der vom IDE eingehenden Folge, sendet sie keine Antwort und wartet innerhalb des Zeitraums P3max auf eine weitere Nachricht Start Communication Request.

2.2.5.2. Communication-Phase

Es lassen sich zwei verschiedene Fehlerbehandlungsbereiche definieren:

1. Die FE erkennt einen IDE-Übertragungsfehler.

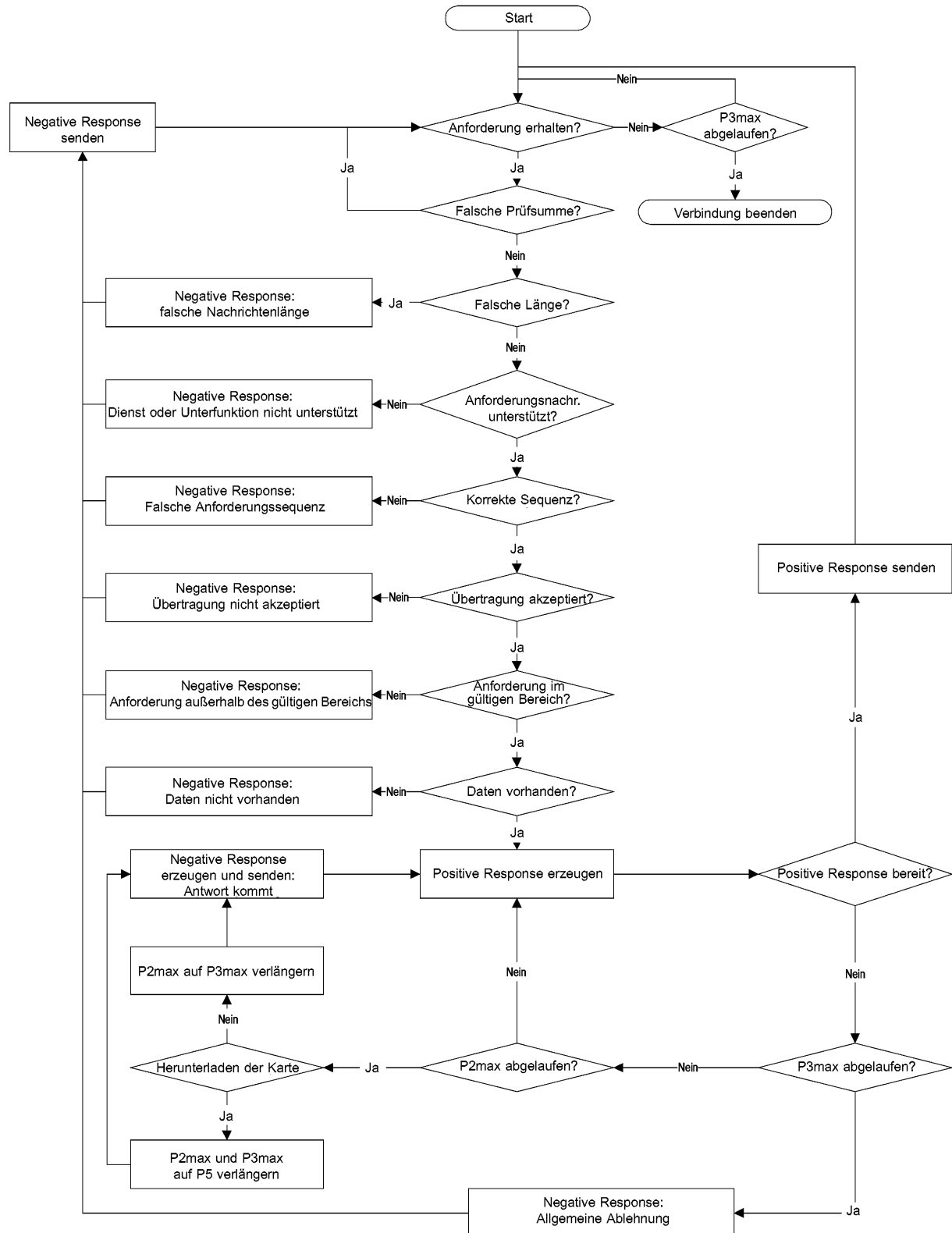
DDP_022 Die FE prüft jede empfangene Nachricht auf Timing-Fehler, Byteformatfehler (z. B. Start- und Stopbitverletzungen) sowie Datenpaketfehler (falsche Byteanzahl empfangen, falsches Prüfsummenbyte).

DDP_023 Erkennt die FE einen der vorstehend genannten Fehler, sendet sie keine Antwort und ignoriert die empfangene Nachricht.

DDP_024 Die FE kann andere Fehler im Format oder Inhalt der empfangenen Nachricht (z. B. Nachricht nicht unterstützt) feststellen, selbst wenn die Nachricht die erforderlichen Längen und Prüfsummen einhält; in diesem Fall antwortet die FE dem IDE mit einer Negative Response-Nachricht unter Angabe der Fehlerart.

Abbildung 2

Fehlerbehandlung durch die FE

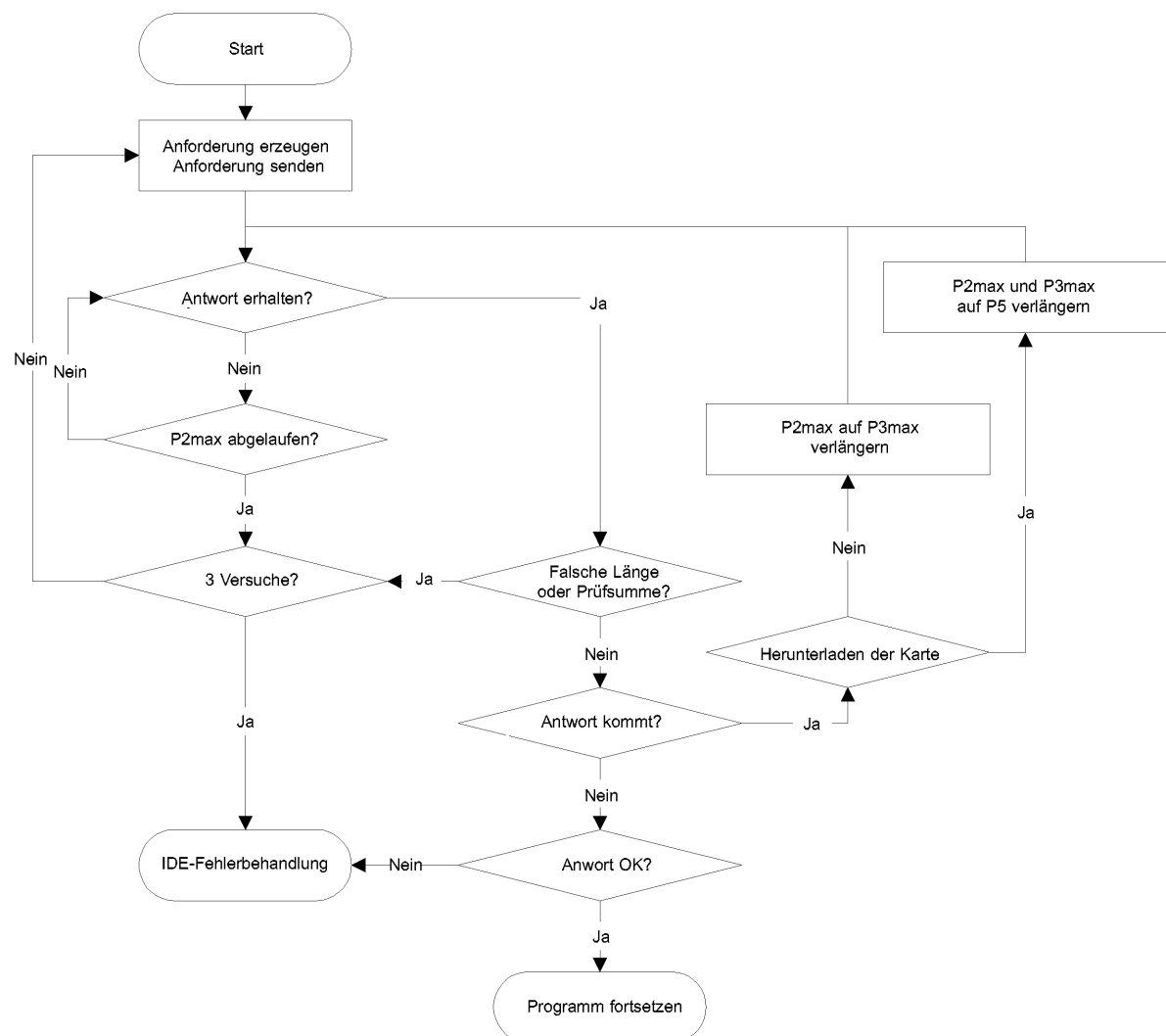


2. Das IDE erkennt einen FE-Übertragungsfehler.

- DDP_025 Das IDE prüft jede empfangene Nachricht auf Timing-Fehler, Byteformatfehler (z. B. Start- und Stopbitverletzungen) sowie Datenpaketfehler (falsche Byteanzahl empfangen, falsches Prüfsummenbyte).
- DDP_026 Das IDE erkennt Sequenzfehler, z. B. die inkorrekte Erhöhung des Teilnachrichtenzählers bei nacheinander empfangenen Nachrichten.
- DDP_027 Erkennt das IDE einen Fehler oder ist innerhalb des Zeitraums T2max keine Antwort von der FE erfolgt, wird die Anforderungsnachricht für insgesamt maximal drei Übertragungen erneut gesendet. Zum Zwecke dieser Fehlererkennung wird eine Teilnachrichtquittung als Anforderung an die FE betrachtet.
- DDP_028 Vor dem Beginn jeder Sendung wartet das IDE mindestens T3min; die Wartezeit wird vom letzten errechneten Auftreten eines Stoppbits nach der Fehlererkennung an gemessen.

Abbildung 3

Fehlerbehandlung durch das IDE



2.2.6. Inhalt der Antwortnachricht

In diesem Abschnitt wird der Inhalt der Datenfelder der verschiedenen positiven Antwortnachrichten spezifiziert.

Die Datenelemente sind in Anlage 1, Datenglossar, definiert.

2.2.6.1. Positive Response Transfer Data Overview

DDP_029 Das Datenfeld der Nachricht Positive Response Transfer Data Overview liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 01 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenelement	Länge (Byte)	Bemerkung
MemberStateCertificate	194	FE-Sicherheitszertifikate
VUCertificate	194	
VehicleIdentificationNumber	17	Fahrzeugkennung
VehicleRegistrationIdentification	1	
vehicleRegistrationNation vehicleRegistrationNumber	14	
CurrentDateTime	4	Aktuelle(s) Datum und Uhrzeit der FE
VuDownloadablePeriod		Herunterladbarer Zeitraum
minDownloadableTime maxDownloadableTime	4 4	
CardSlotsStatus	1	Art der in die FE eingesteckten Karten
VuDownloadActivityData		Vorhergehender FE-Download
downloadingTime	4	
fullCardNumber companyOrWorkshopName	18 36	
VuCompanyLocksData		Alle gespeicherten Unternehmenssperrungen. Ist der Abschnitt leer, wird lediglich noOfLocks = 0 gesendet.
noOfLocks	1	
...	(98)	
Vu Company Locks Record	4	
lockInTime	4	
lockOutTime	36	
companyName companyAddress companyCardNumber	36 18	
...		Alle in der FE gespeicherten Kontrolldatensätze. Ist der Abschnitt leer, wird lediglich noOfControls = 0 gesendet.
VuControlActivityData	1	
noOfControls	(31)	
...		
Vu Control Activity Record	1	
controlType controlTime controlCardNumber downloadPeriodBeginTime downloadPeriodEndTime	4 18 4 4	
...		RSA-Signatur aller Daten (außer Zertifikate), beginnend mit VehicleIdentificationNumber bis hin zum letzten Byte des letzten VuControlActivityRecord.
Signature	128	

2.2.6.2. Positive Response Transfer Data Activities

DDP_030 Das Datenfeld der Nachricht Positive Response Transfer Data Activities liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 02 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenelement	Länge (Bytes)	Bemerkung
TimeReal	4	Datum des heruntergeladenen Tages
OdometerValueMidnight	3	Kilometerstand am Ende des heruntergeladenen Tages
VuCardIWData noOfVuCardIWRecords	2	Daten zu den Einsteck-/Entnahmevorgängen der Karte:
...	(129)	— Enthält dieser Abschnitt keine verfügbaren Daten, wird lediglich noOfVuCardIWRecords = 0 gesendet.
VuCardIWRecord	36	— Geht ein VuCardIWRecord über 00:00 (Einstecken der Karte am Vortag) oder 24:00 (Kartentnahme am Folgetag) hinaus, erscheint er vollständig für beide Tage.
cardHolderName	36	
holderSurname	36	
holderFirstNames	18	
fullCardNumber	4	
cardExpiryDate	4	
cardInsertionTime	3	
vehicleOdometerValueAtInsertion	1	
cardSlotNumber	4	
cardWithdrawalTime	3	
vehicleOdometerValueAtWithdrawal	1	
previousVehicleInfo	14	
vehicleRegistrationIdentification	4	
vehicleRegistrationNation	4	
vehicleRegistrationNumber	1	
cardWithdrawalTime	1	
manualInputFlag	1	
...		
VuActivityDailyData noOfActivityChanges	2	Steckplatzstatus um 00.00 Uhr und aufgezeichnete Tätigkeitsänderungen für den heruntergeladenen Tag.
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData noOfPlaceRecords	1	Aufgezeichnete Ortsdaten für den heruntergeladenen Tag. Ist der Abschnitt leer, wird lediglich noOfPlaceRecords = 0 gesendet.
...	(28)	
VuPlaceDailyWorkPeriodRecord	18	
fullCardNumber	4	
placeRecord	1	
entryTime	1	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData noOfSpecificConditionRecords	2	Aufgezeichnete spezifische Bedingungen für den heruntergeladenen Tag. Ist der Abschnitt leer, wird lediglich noOfSpecificConditionRecords=0 gesendet.
...	(5)	
SpecificConditionRecord	4	
EntryTime	1	
specificConditionType	1	
...		
Signature	128	RSA-Signatur aller Daten, beginnend ab TimeReal bis hin zum letzten Byte des letzten Datensatzes einer spezifischen Bedingung.

2.2.6.3. Positive Response Transfer Data Events and Faults

DDP_031 Das Datenfeld der Nachricht Positive Response Transfer Data Events and Faults liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 03 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenelement		Länge (Bytes)	Bemerkung
VuFaultData			
NoOfVuFaults		1	Alle in der FE gespeicherten oder andauernden Störungen. Ist der Abschnitt leer, wird lediglich noOfVuFaults = 0 gesendet.
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
...			
VuEventData			
NoOfVuEvents		1	Alle in der FE gespeicherten oder andauernden Ereignisse (außer Geschwindigkeitsüberschreitung). Ist der Abschnitt leer, wird lediglich noOfVuEvents = 0 gesendet.
...		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
	SimilarEventsNumber	1	
...			
VuOverSpeedingControlData			
LastOverspeedControlTime		4	Daten zur letzten Kontrolle Geschwindigkeitsüberschreitung (Standardwert, wenn keine Daten vorhanden).
FirstOverspeedSince		4	
NumberOfOverspeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Alle in der FE gespeicherten Ereignisse Geschwindigkeitsüberschreitung. Ist der Abschnitt leer, wird lediglich noOfVuOverSpeedingEvents = 0 gesendet.
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
...			
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Alle in der FE gespeicherten Zeiteinstellungsereignisse (außerhalb des Rahmens einer vollständigen Kalibrierung). Ist der Abschnitt leer, wird lediglich noOfVuTimeAdjRecords = 0 gesendet.
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	RSA-Signatur aller Daten, beginnend ab noOfVuFaults bis hin zum letzten Byte des letzten Zeiteinstellungsdatensatzes.

2.2.6.4. Positive Response Transfer Data Detailed Speed

DDP_032 Das Datenfeld der Nachricht Positive Response Transfer Data Detailed Speed liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 04 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenelement	Länge (Bytes)	Bemerkung
VuDetailedSpeedData		
NoOfSpeedBlocks	2	Alle in der FE gespeicherten detaillierten Geschwindigkeitsdaten (ein Geschwindigkeitsblock pro Minute, in der sich das Fahrzeug bewegt hat) 60 Geschwindigkeitswerte pro Minute (ein Wert pro Sekunde).
...		
VuDetailedSpeedBlock	4	
SpeedBlockBeginDate	60	
speedsPerSecond		
...		
Signature	128	RSA-Signatur aller Daten, beginnend ab noOfSpeedBlocks bis hin zum letzten Byte des letzten Geschwindigkeitsblocks.

2.2.6.5. Positive Response Transfer Data Technical Data

DDP_033 Das Datenfeld der Nachricht Positive Response Transfer Data Technical Data liefert folgende Daten in folgender Reihenfolge unter SID 76 Hex und TREP 05 Hex. Es muss eine geeignete Aufteilung und Zählung der Teilnachrichten erfolgen:

Datenelement	Länge (Bytes)	Bemerkung
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		
noOfVuCalibrationRecords	1	Alle in der FE gespeicherten Kalibrierungsdatensätze.
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	RSA-Signatur aller Daten, beginnend ab vuManufacturerName bis hin zum letzten Byte des letzten VuCalibrationRecord.

2.3. ESM-Datenspeicherung

- DDP_034 War eine FE-Datenübertragung Bestandteil eines Download-Vorgangs, speichert das IDE in einer einzigen physischen Datei alle Daten, die während des Download-Vorgangs von der FE in Positive Response Transfer Data-Nachrichten empfangen wurden. Dabei nicht gespeichert werden Nachrichtenköpfe, Teilnachrichtenzähler, leere Teilnachrichten und Prüfsummen, gespeichert werden jedoch SID und TREP (nur der ersten Teilnachricht bei mehreren Teilnachrichten).

3. PROTOKOLL FÜR DAS HERUNTERLADEN VON DATEN VON KONTROLLGERÄTKARTEN

3.1. Geltungsbereich

Dieser Abschnitt beschreibt das direkte Herunterladen der Kartendaten einer Kontrollgerätkarte auf ein IDE. Da das IDE nicht Bestandteil der Sicherheitsumgebung ist, erfolgt keine Authentisierung zwischen der Karte und dem IDE.

3.2. Begriffsbestimmungen

Download-Vorgang: Die Ausführung eines Download der Chipkartendaten. Der Vorgang umfasst die gesamte Prozedur vom Zurücksetzen der Chipkarte durch ein IFD bis zur Deaktivierung der Chipkarte (Entnahme der Karte oder nächstes Zurücksetzen).

Signierte Datei: Eine Datei von der Chipkarte. Die Datei wird in Klartext zum IFD übertragen. Auf der Chipkarte erfolgt eine Hash-Code-Anwendung für die Datei, sie wird signiert, und die Signatur wird an das IFD übertragen.

3.3. Herunterladen von der Karte

- DDP_035 Das Herunterladen einer Kontrollgerätkarte beinhaltet die folgenden Schritte:

- Herunterladen der gemeinsamen Informationen der Karte in den EF ICC und IC. Diese Informationen sind fakultativ und werden nicht mit einer digitalen Signatur gesichert.
- Herunterladen der EF Card_Certificate und CA_Certificate. Diese Informationen sind nicht mit einer digitalen Signatur gesichert.

Das Herunterladen dieser Dateien ist bei jedem Download-Vorgang obligatorisch.

- Herunterladen der anderen Anwendungsdaten-EF (innerhalb des DF Tachograph) außer EF Card_Download. Diese Informationen sind mit einer digitalen Signatur gesichert.
 - Bei jedem Download-Vorgang ist zumindest das Herunterladen der EF Application_Identification und ID obligatorisch.
 - Beim Herunterladen einer Fahrerkarte ist zudem der Download folgender EF obligatorisch:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions.
- Beim Herunterladen einer Fahrerkarte, wird das Datum LastCard_Download in EF Card_Download aktualisiert.
- Beim Herunterladen einer Werkstattkarte ist der Kalibrierungszähler in der EF Card_Download zurückzusetzen.

3.3.1. Initialisierungssequenz

DDP_036 Das IDE leitet folgende Sequenz ein:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇐	Hardware zurücksetzen	
ATR	⇒		

Mit PPS kann auf eine höhere Baudrate gewechselt werden, sofern die Chipkarte diese Baudrate unterstützt.

3.3.2. Sequenz für unsigned Dateien

DDP_037 Die Sequenz für das Herunterladen der EF ICC, IC, Card_Certificate und CA_Certificate lautet folgendermaßen::

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇐	Select File	Auswahl nach Dateikennung
OK	⇒		
	⇐	Read Binary	Enthält die Datei mehr Daten als der Puffer des Lesers oder der Karte fassen kann, ist der Befehl so lange zu wiederholen, bis die gesamte Datei ausgelesen ist.
File Data OK	⇒	Speicherung der Daten auf ESM	gemäß 3.4, Datenspeicherungsformat

Anmerkung: Vor Auswahl der EF Card_Certificate muss die Kontrollgerätenwendung ausgewählt werden (Auswahl durch AID).

3.3.3. Sequenz für signierte Dateien

DDP_038 Die folgende Sequenz wird für die folgenden Dateien verwendet, die jeweils mit ihrer Signatur herunterzuladen sind:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
	⇐	Select File	
OK	⇒		
	⇐	Perform Hash of File	Berechnet den Hashwert über dem Dateninhalt der ausgewählten Datei mit Hilfe des vorgeschriebenen Hash-Algorithmus gemäß Anlage 11. Dieser Befehl ist kein ISO-Befehl.
Hash of File berechnen und Hashwert temporär speichern			
OK	⇒		
	⇐	Read Binary	Enthält die Datei mehr Daten als der Puffer des Lesers oder der Karte fassen kann, ist der Befehl so lange zu wiederholen, bis die gesamte Datei ausgelesen ist.
File Data OK	⇒	Empfangene Daten auf ESM speichern	gemäß 3.4, Datenspeicherungsformat
	⇐	PSO: Compute Digital Signature	
Perform Security Operation Compute Digital Signature mit Hilfe des temporär gespeicherten Hashwerts			
Signature OK	⇒	Daten an die zuvor auf dem ESM gespeicherten Daten anfügen	gemäß 3.4, Datenspeicherungsformat

3.3.4. Sequenz für das Zurücksetzen des Kalibrierungszählers

DDP_039 Die Sequenz für das Zurücksetzen des Zählers NoOfCalibrationsSinceDownload in der EF Card_Download auf einer Werkstattkarte lautet folgendermaßen:

Karte	Richtung	IDE/IFD	Bedeutung/Bemerkungen
OK	↩	Select File EF Card_Download	Auswahl nach Dateikennung
	⇒		
setzt Kartendownloadzahl zurück	↩	Update Binary NoOfCalibrations SinceDownload = 00 00	
OK	⇒		

3.4. Datenspeicherungsformat

3.4.1. Einleitung

DDP_040 Die heruntergeladenen Daten sind nach folgenden Bedingungen zu speichern:

- Die Daten sind transparent zu speichern, d. h. die Reihenfolge der von der Karte übertragenen Bytes sowie die Reihenfolge der in ihnen enthaltenen Bits muss während der Speicherung erhalten bleiben.
- Alle im Rahmen eines Download-Vorgangs heruntergeladenen Dateien der Karte werden in einer einzigen Datei auf dem ESM gespeichert

3.4.2. Dateiformat

DDP_041 Das Dateiformat ist eine Verkettung mehrerer TLV-Objekte.

DDP_042 Der Tag für eine EF ist die FID sowie der Zusatz ,00'.

DDP_043 Der Tag der Signatur einer EF ist die FID der Datei sowie der Zusatz ,01'.

DDP_044 Die Länge ist ein 2-Byte-Wert. Der Wert legt die Anzahl der Bytes im Wertfeld fest. Der Wert ,FF FF' im Längenfeld ist für eine künftige Verwendung reserviert.

DDP_045 Wird eine Datei nicht heruntergeladen, ist auch nichts zu speichern, was mit der Datei im Zusammenhang steht (also kein Tag und keine Nulllänge).

DDP_046 Eine Signatur wird als nächstes TLV-Objekt unmittelbar nach dem Objekt, das die Daten der Datei enthält, gespeichert.

Definition	Bedeutung	Länge
FID (2 Bytes) ,00'	Tag für EF (FID)	3 Bytes
FID (2 Bytes) ,01'	Tag für Signatur der EF (FID)	3 Bytes
xx xx	Länge des Wertfelds	2 Bytes

Beispiel für Daten in einer Download-Datei auf einem ESM:

Tag	Länge	Wert
00 02 00	00 11	Daten von EF ICC
C1 00 00	00 C2	Daten von EF Card_Certificate
		...
05 05 00	0A 2E	Daten von Vehicles_Used
05 05 01	00 80	Signatur von EF Vehicles_Used

4. HERUNTERLADEN VON DER KONTROLLGERÄTKARTE ÜBER EINE FAHRZEUGEINHEIT

- DDP_047 Die FE muss das Herunterladen des Inhalts einer eingesteckten und an ein IDE angeschlossenen Fahrerkarte zulassen.
- DDP_048 Zum Starten dieses Modus sendet das IDE die Nachricht Transfer Data Request Card Download an die FE (siehe 2.2.2.9).
- DDP_049 Daraufhin lädt die FE die gesamte Karte dateiweise in Übereinstimmung mit dem in Abschnitt 3 definierten Download-Protokoll herunter und leitet alle von der Karte empfangenen Daten im entsprechenden TLV-Dateiformat (siehe 3.4.2) sowie eingekapselt in eine Positive Response Transfer Data-Nachricht an das IDE weiter.
- DDP_050 Das IDE ruft die Kartendaten aus der Nachricht Positive Response Transfer Data ab (unter Fortlassung aller Köpfe, SID, TREP, Teilnachrichtenzähler und Prüfsummen) und speichert sie innerhalb einer in Abschnitt 2.3 beschriebenen physischen Datei.
- DDP_051 Danach aktualisiert die FE gegebenenfalls die Dateien ControlActivityData oder Card_Download der Fahrerkarte.
-

Anlage 8

KALIBRIERUNGSPROTOKOLL

INHALTSVERZEICHNIS

1.	Einleitung	170
2.	Begriffe, Begriffsbestimmungen und Referenzdokumente	170
3.	Diensteübersicht	170
3.1.	Verfügbare Dienste	170
3.2.	Antwortcodes	171
4.	Kommunikationsdienste	171
4.1.	Der Dienst StartCommunication	171
4.2.	Der Dienst StopCommunication	173
4.2.1.	Beschreibung der Nachricht	173
4.2.2.	Nachrichtenformat	174
4.2.3.	Parameterdefinition	175
4.3.	Der Dienst TesterPresent	175
4.3.1.	Beschreibung der Nachricht	175
4.3.2.	Nachrichtenformat	175
5.	Verwaltungsdienste	176
5.1.	Der Dienst StartDiagnosticSession	176
5.1.1.	Beschreibung der Nachricht	176
5.1.2.	Nachrichtenformat	177
5.1.3.	Parameterdefinition	178
5.2.	Der Dienst SecurityAccess	178
5.2.1.	Beschreibung der Nachricht	178
5.2.2.	Nachrichtenformat — SecurityAccess — requestSeed	179
5.2.3.	Nachrichtenformat — SecurityAccess — sendKey	180
6.	Datenübertragungsdienste	181
6.1.	Der Dienst ReadDataByIdentifier	181
6.1.1.	Beschreibung der Nachricht	181
6.1.2.	Nachrichtenformat	181
6.1.3.	Parameterdefinition	182
6.2.	Der Dienst WriteDataByIdentifier	183
6.2.1.	Beschreibung der Nachricht	183
6.2.2.	Nachrichtenformat	183
6.2.3.	Parameterdefinition	184
7.	Prüfimpulssteuerung — Funktionseinheit Eingabe/Ausgabe-Steuerung	184
7.1.	Der Dienst InputOutputControlByIdentifier	184

7.1.1.	Beschreibung der Nachricht	184
7.1.2.	Nachrichtenformat	185
7.1.3.	Parameterdefinition	186
8.	Datensatzformate	187
8.1.	Wertebereiche der übertragenen Parameter	187
8.2.	dataRecords-Formate	188

1. EINLEITUNG

In dieser Anlage wird der Datenaustausch zwischen einer Fahrzeugeinheit und einem Prüfgerät über die K-Leitung, die Teil der in Anlage 6 beschriebenen Kalibrierungsschnittstelle ist, beschrieben. Außerdem enthält sie eine Beschreibung der Steuerung der Eingangs-/Ausgangssignalleitung am Kalibrierungsanschluss.

Das Aufbauen der K-Leitungskommunikation wird im Abschnitt 4 ‚Kommunikationsdienste‘ beschrieben.

In dieser Anlage ist vom Konzept der Diagnosevorgänge die Rede, mit dem der Umfang der K-Leitungssteuerung unter verschiedenen Bedingungen festgelegt wird. Der Standardvorgang ist dabei die ‚StandardDiagnosticSession‘, bei der aus einer Fahrzeugeinheit alle Daten ausgelesen, jedoch keine Daten in die Fahrzeugeinheit geschrieben werden können.

Die Auswahl des Diagnosevorgangs wird im Abschnitt 5 ‚Verwaltungsdienste‘ beschrieben.

CPR_001 Im Programmiervorgang ‚ECUProgrammingSession‘ ist es möglich, Daten in die Fahrzeugeinheit einzugeben. Bei der Eingabe von Kalibrierungsdaten (Anforderungen 097 und 098) muss sich die Fahrzeugeinheit außerdem in der Betriebsart KALIBRIERUNG befinden.

Die Datenübertragung über die K-Leitung wird im Abschnitt 6 ‚Datenübertragungsdienste‘ beschrieben. Die Formate der übertragenen Daten werden in Abschnitt 8 ‚Datensatzformate‘ erläutert.

CPR_002 Der Einstellvorgang ‚ECUAdjustmentSession‘ ermöglicht die Auswahl der E/A-Betriebsart der Kalibrierungs-E/A-Signalleitung über die Schnittstelle der K-Leitung. Die Steuerung der Kalibrierungs-E/A-Signalleitung wird in Abschnitt 7 ‚Prüfimpulssteuerung — Funktionseinheit Eingabe/Ausgabe-Steuerung‘ beschrieben.

CPR_003 Im vorliegenden Dokument wird als Adresse für das Prüfgerät durchgängig ‘tt’ verwendet. Ungeachtet dessen, dass für Prüfgeräte bevorzugte Adressen verwendet werden können, muss die FE auf jede Prüfgerätadresse richtig antworten. Die physische Adresse der FE ist 0xEE.

2. BEGRIFFE, BEGRIFFSBESTIMMUNGEN UND REFERENZDOKUMENTE

Für die Service Identifier (SID), die Bedienanforderungen und -antworten sowie die Standardparameter werden Byte-Codierungen und hexadezimale Werte verwendet.

Der Begriff ‚Prüfgerät‘ bezeichnet das zur Eingabe der Programmierungs-/Kalibrierungsdaten in die FE verwendete Gerät.

Die Begriffe ‚Client‘ und ‚Server‘ beziehen sich auf das Prüfgerät bzw. die FE.

Der Begriff ‚ECU‘ bedeutet ‚elektronische Steuereinheit‘ und bezieht sich auf die FE.

Referenzdokumente:

ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999. (Straßenfahrzeuge — Diagnosesysteme — Schlüsselwort 2000 — Teil 2: Sicherungsschicht. 1. Ausgabe 1999)

3. DIENSTEÜBERSICHT

3.1. Verfügbare Dienste

Die folgende Tabelle gibt einen Überblick über die in dieser Anlage beschriebenen Dienste, die im Kontrollgerät verfügbar sein werden.

CPR_004 In der Tabelle sind die Dienste aufgeführt, die bei aktiviertem Diagnosevorgang verfügbar sind.

— Spalte 1 enthält die verfügbaren Dienste.

— Spalte 2 nennt den Abschnitt in der vorliegenden Anlage, in der der Dienst näher beschrieben wird.

- Spalte 3 ordnet die Service-Identifier-Werte bei Anforderungsnachrichten zu.
- Spalte 4 gibt die Dienste des Standardvorgangs ‚StandardDiagnosticSession‘ (SD) an, die in jeder FE implementiert sein müssen.
- Spalte 5 gibt die Dienste des Einstellvorgangs ‚ECUAdjustmentSession‘ (ECUAS) an, die implementiert sein müssen, um die Steuerung der E/A-Signalleitung der für die Kalibrierung vorgesehenen Steckverbindung an der Frontplatte der FE zu gestatten.
- Spalte 6 gibt die Dienste des Programmiervorgangs ‚ECUProgrammingSession‘ (ECUPS) an, die implementiert sein müssen, um die Programmierung von Parametern in der FE zu ermöglichen.

Tabelle 1

Übersicht über die SID-Werte

Bezeichnung des Diagnosedienstes	Abschnitt Nr.	SID-Anforderungswert	Diagnosevorgänge		
			SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Dieses Symbol zeigt an, dass der betreffende Dienst bei diesem Diagnosevorgang obligatorisch ist.
Ein Feld ohne Symbol bedeutet, dass der betreffende Dienst bei diesem Diagnosevorgang nicht zugelassen ist.

3.2. Antwortcodes

Für jeden Dienst sind Antwortcodes festgelegt.

4. KOMMUNIKATIONSDIENSTE

Um die Kommunikation aufzubauen und aufrecht zu erhalten, sind einige Dienste erforderlich, die nicht auf der Anwendungsschicht liegen. Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 2

Kommunikationsdienste

Dienstbezeichnung	Beschreibung
StartCommunication	Client fordert Beginn eines Kommunikationsvorgangs mit einem (mehreren) Server(n) an
StopCommunication	Client fordert Beendigung des laufenden Kommunikationsvorgangs an
TesterPresent	Client teilt dem Server mit, dass die Verbindung noch aktiv ist

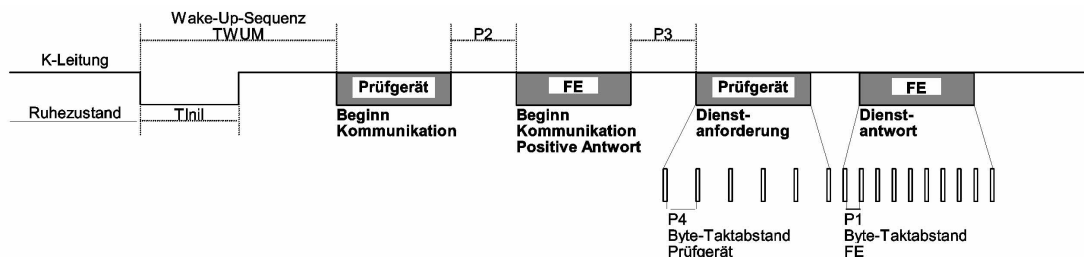
CPR_005 Der Dienst StartCommunication wird genutzt, um eine Kommunikation einzuleiten. Für die Ausführung eines Dienstes ist es immer erforderlich, dass die Kommunikation initialisiert und die für die gewünschte Betriebsart geeigneten Kommunikationsparameter verwendet werden.

4.1. Der Dienst StartCommunication

CPR_006 Bei Erhalt eines StartCommunication-Primitivs prüft die FE, ob die angeforderte Kommunikationsverbindung unter den gegebenen Bedingungen initialisiert werden kann. Gültige Bedingungen für die Initialisierung einer Kommunikationsverbindung sind im Dokument ISO 14230-2 beschrieben.

CPR_007 Die FE führt daraufhin alle erforderlichen Maßnahmen zur Initialisierung der Kommunikationsverbindung aus und sendet ein StartCommunication-Antwort-Primitiv mit den gewählten Positive Response-Parametern.

- CPR_008 Erhält eine bereits initialisierte (und in eine Diagnosesitzung eingetretene) FE die Anforderung StartCommunication (z. B. aufgrund Wiederanlauf des Prüfgeräts nach einer Fehlerbedingung), muss die Anforderung angenommen und die FE neu initialisiert werden.
- CPR_009 Falls sich die Kommunikationsverbindung aus irgendeinem Grund nicht initialisieren lässt, setzt die FE den Betrieb in der gleichen Weise wie unmittelbar vor dem Versuch zur Initialisierung der Kommunikationsverbindung fort.
- CPR_010 Die Anforderungsnachricht StartCommunication muss an eine physische Adresse erfolgen.
- CPR_011 Die Initialisierung der FE für Dienste erfolgt mit Hilfe einer „Schnellinitialisierung“:
- Jeder Aktivität geht ein Bus-Ruhezustandtakt voraus.
 - Das Prüfgerät überträgt anschließend eine Initialisierungssequenz.
 - Alle zum Aufbau der Kommunikation benötigten Informationen sind in der Antwort der FE enthalten.
- CPR_012 Nach Beendigung der Initialisierung:
- Alle Kommunikationsparameter werden entsprechend der Schlüssel-Bytes auf die Werte in Tabelle 5 gesetzt.
 - Die FE wartet auf die erste Anforderung vom Prüfgerät.
 - Die FE befindet sich in der Standarddiagnosebetriebsart, d. h. der „StandardDiagnosticSession“.
 - Die Kalibrierungs-E/A-Signalleitung befindet sich im Standardzustand, d. h. im deaktivierten Zustand.
- CPR_014 Die Übertragungsgeschwindigkeit (Baudrate) auf der K-Leitung beträgt 10emp14;400 Baud.
- CPR_016 Die Schnellinitialisierung wird ausgelöst, indem das Prüfgerät eine Wake-Up-Sequenz (Wup) auf der K-Leitung überträgt. Diese beginnt nach dem Ruhezustandtakt auf der K-Leitung mit einem L-Takt T_{inil}. Das Prüfgerät sendet das erste Bit des Dienstes StartCommunication im Anschluss an einen TWup-Takt, der nach der ersten fallenden Flanke beginnt.



- CPR_017 Die Taktwerte für die Schnellinitialisierung sowie für die Kommunikation generell sind in den nachstehenden Tabellen im einzelnen aufgeführt. Für den Ruhezustandtakt existieren mehrere Möglichkeiten:
- Erste Übertragung nach Einschalten, $T_{\text{Ruhe}} = 300 \text{ ms}$.
 - Nach Abschluss eines Dienstes StopCommunication, $T_{\text{Ruhe}} = P3 \text{ Minimum}$
 - Nach Beendigung der Kommunikation durch Zeitüberschreitung (Time-Out) $P3 \text{ Maximum}$, $T_{\text{Ruhe}} = 0$.

Tabelle 3

Taktwerte zur Schnellinitialisierung

Parameter		Min.	Max.
T _{inil}	25 ± 1 ms	24 ms	26 ms
TWup	50 ± 1 ms	49 ms	51 ms

Tabelle 4

Taktwerte für die Kommunikation

Takt-Parameter	Beschreibung der Parameter	Untere Grenzwerte (in ms)	Obere Grenzwerte (in ms)
		Min.	Max.
P1	Byte-Taktabstand für die FE-Antwort	0	20
P2	Zeit zwischen Prüfgerätenforderung und FE-Antwort bzw. zwei FE-Antworten	25	250
P3	Zeit zwischen Ende der FE-Antworten und Beginn einer neuen Prüfgerätenforderung	55	5 000
P4	Byte-Taktabstand für die Prüfgerätantwort	5	20

CPR_018 Das Nachrichtenformat für die Schnellinitialisierung ist in den nachstehenden Tabellen spezifiziert:

Tabelle 5

Anforderungsnachricht für StartCommunication

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	81	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Service Identifier für Anforderung StartCommunication	81	SCR
#5	Prüfsumme	00-FF	CS

Tabelle 6

Nachricht Positive Response auf StartCommunication

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Positive Response StartCommunication	C1	SCRPR
#6	Schlüssel-Byte 1	EA	KB1
#7	Schlüssel-Byte 2	8F	KB2
#8	Prüfsumme	00-FF	CS

CPR_019 Eine negative Antwort (Negative Response) auf die Anforderungsnachricht StartCommunication gibt es nicht. Kann keine positive Nachricht (Positive Response) gegeben werden, so erfolgt keine Initialisierung der FE, und diese verbleibt in ihrer normalen Betriebsart.

4.2. Der Dienst StopCommunication

4.2.1. Beschreibung der Nachricht

Dieser Dienst der Kommunikationssteuerungsschicht hat zum Zweck, einen Kommunikationsvorgang zu beenden.

CPR_020 Bei Erhalt eines StopCommunication-Primitivs prüft die FE, ob die derzeitigen Bedingungen die Beendigung dieser Kommunikation gestatten. Ist dies der Fall, so führt die FE alle erforderlichen Maßnahmen zur Beendigung dieser Kommunikation durch.

- CPR_021 Ist die Beendigung der Kommunikation möglich, gibt die FE vor der Beendigung der Kommunikation ein StopCommunication-Antwort-Primitiv mit den gewählten Positive Response-Parametern aus.
- CPR_022 Falls sich die Kommunikation aus irgendeinem Grund nicht beenden lässt, gibt die FE ein StopCommunication-Antwort-Primitiv mit den gewählten Parametern für Negative Response aus.
- CPR_023 Wird von der FE eine Zeitüberschreitung aufgrund P3max erkannt, muss die Kommunikation ohne Ausgabe eines Antwortelements beendet werden.

4.2.2. Nachrichtenformat

- CPR_024 Die Nachrichtenformate für die StopCommunication-Primitive sind in den folgenden Tabellen aufgeführt:

Tabelle 7

Anforderungsnachricht für StopCommunication

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	01	LEN
#5	Service Identifier für Anforderung StopCommunication	82	SPR
#6	Prüfsumme	00-FF	CS

Tabelle 8

Nachricht Positive Response auf StopCommunication

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	01	LEN
#5	Service Identifier für Positive Response auf StopCommunication	C2	SPRPR
#6	Prüfsumme	00-FF	CS

Tabelle 9

Nachricht Negative Response auf StopCommunication

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung StopCommunicationentification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Prüfsumme	00-FF	CS

4.2.3. *Parameterdefinition*

Dieser Dienst erfordert keine Parameterdefinition.

4.3. Der Dienst **TesterPresent**

4.3.1. *Beschreibung der Nachricht*

Mit Hilfe des Dienstes **TesterPresent** teilt das Prüfgerät dem Server mit, dass es sich noch immer in einer aktiven Verbindung mit ihm befindet, um zu verhindern, dass der Server automatisch in die normale Betriebsart zurückkehrt und dadurch möglicherweise die Verbindung beendet. Dieser Dienst sorgt durch regelmäßiges Aussenden einer Anforderung dafür, dass die Diagnosesitzung oder Verbindung aktiv bleibt, indem der P3-Zeitgeber jedem Erhalt einer Anforderung für diesen Dienst zurückgesetzt wird.

4.3.2. *Nachrichtenformat*

CPR_079 Die Nachrichtenformate für die **TesterPresent**-Primitive sind in den folgenden Tabellen aufgeführt.

Tabelle 10

Anforderungsnachricht **TesterPresent**

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	Service Identifier für Anforderung TesterPresent	3E	TP
#6	Sub Function = responseRequired = [yes no]	01	RESPREQ_Y
		02	RESPREQ_NO
#7	Prüfsumme	00-FF	CS

CPR_080 Ist der Parameter **responseRequired** auf ‚yes‘ gesetzt, so antwortet der Server mit folgenden positiven Antwortnachrichten. Ist der Parameter auf ‚no‘ gesetzt, sendet der Server keine Antwort.

Tabelle 11

Nachricht **TesterPresent Positive Response**

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	01	LEN
#5	Service Identifier für TesterPresent Positive Response	7E	TPPR
#6	Prüfsumme	00-FF	CS

CPR_081 Der Dienst verwendet die folgenden negativen Antwort-Codes:

Tabelle 12

Nachricht TesterPresent Negative Response

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung TesterPresent	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12	RC_SFNS_IF
		13	RC_IML
#8	Prüfsumme 00-FF CS	00-FF	CS

5. VERWALTUNGSDIENSTE

Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 13

Verwaltungsdienste

Dienstbezeichnung	Beschreibung
StartDiagnosticSession	Client fordert Beginn eines Diagnosevorgangs mit einer FE an
SecurityAccess	Client ruft Funktionen auf, zu denen nur berechtigte Benutzer Zugriff haben

5.1. Der Dienst StartDiagnosticSession

5.1.1. Beschreibung der Nachricht

CPR_025 Der Dienst StartDiagnosticSession dient dazu, verschiedene Diagnosevorgänge im Server zu aktivieren. Ein Diagnosevorgang aktiviert bestimmte Dienste nach Maßgabe von Tabelle 17. Mit einem solchen Vorgang kann der Fahrzeughersteller bestimmte Dienste aktivieren, die hier nicht beschrieben werden. Die Implementierungsregeln haben folgenden Festlegungen zu entsprechen:

- Es ist stets genau ein Diagnosevorgang in der FE aktiv.
- Die FE startet die ‚StandardDiagnosticSession‘ bei jedem Einschaltvorgang. Wird kein anderer Diagnosevorgang gestartet, so läuft die ‚StandardDiagnosticSession‘ so lange wie die FE eingeschaltet ist.
- Wird vom Prüfgerät ein bereits laufender Diagnosevorgang angefordert, sendet die FE eine positive Antwortnachricht (Positive Response).
- Fordert das Prüfgerät einen neuen Diagnosevorgang an, sendet die FE zuerst eine positive Antwortnachricht auf ‚StartDiagnosticSession‘, bevor der neue Diagnosevorgang in der FE aktiviert wird. Kann die FE den angeforderten neuen Diagnosevorgang nicht starten, antwortet sie mit einer negativen Antwortnachricht auf StartDiagnosticSession und setzt den laufenden Diagnosevorgang fort.

CPR_026 Ein Diagnosevorgang darf erst begonnen werden, wenn die Nachrichtenverbindung zwischen dem Client und der FE errichtet wurde.

CPR_027 Nach einer erfolgreichen Anforderung StartDiagnosticSession sind die in Tabelle 4 aufgeführten Taktparameter aktiv, wobei der Parameter diagnosticSession in der Anforderungsnachricht auf ‚StandardSession‘ gesetzt ist, wenn zuvor ein anderer Diagnosevorgang aktiv war.

5.1.2. **Nachrichtenformat**

CPR_028 Die Nachrichtenformate für die StartDiagnosticSession-Primitive sind in den folgenden Tabellen spezifiziert:

Tabelle 14

Anforderungsnachricht StartDiagnosticSession

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	Service Identifier für Anforderung StartDiagnosticSession	10	STDS
#6	diagnosticSession = [ein Wert aus Tabelle 17]	xx	DS_...
#7	Prüfsumme	00-FF	CS

Tabelle 15

Nachricht Positive Response auf StartDiagnosticSession

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	Service Identifier für Positive Response auf StartDiagnosticSession	50	STDSPR
#6	DiagnosticSession = [gleicher Wert wie Byte Nr. 6 in Tabelle 14]	xx	DS_...
#7	Prüfsumme	00-FF	CS

Tabelle 16

Nachricht Negative Response auf StartDiagnosticSession

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung StartDiagnosticSession	10	STDS
#7	ResponseCode = [subFunctionNotSupported ^(a)	12	RC_SFNS
	incorrectMessageLength ^(b)	13	RC_IML
	conditionsNotCorrect ^(c)	22	RC_CNC
#8	Prüfsumme	00-FF	CS

^(a) Der in Byte Nr. 6 der Anforderungsnachricht eingetragene Wert wird nicht unterstützt, d. h. er ist nicht in Tabelle 17 definiert.

^(b) Die Nachricht hat eine falsche Länge.

^(c) Die Bedingungen für die angeforderte StartDiagnosticSession sind nicht erfüllt.

5.1.3. Parameterdefinition

CPR_029 Der Parameter DiagnosticSession (DS_) dient dem Dienst StartDiagnosticSession dazu, das spezielle Verhalten des Servers bzw. der Server zu wählen. Im vorliegenden Dokument sind folgende Diagnosevorgänge spezifiziert:

Tabelle 17

Definition der Werte für diagnosticSession

Hex	Beschreibung	Symbolform
81	StandardDiagnosticSession Dieser Diagnosevorgang aktiviert alle Dienste, die in Spalte 4 ‚SD‘ von Tabelle 1 angegeben sind. Diese Dienste ermöglichen das Auslesen der Daten von einem Server (FE). Dieser Diagnosevorgang ist aktiv, nachdem die Initialisierung zwischen Client (Prüfgerät) und Server (FE) erfolgreich abgeschlossen wurde. Dieser Diagnosevorgang kann durch andere in diesem Abschnitt genannte Diagnosevorgänge überschrieben werden.	SD
85	ECUProgrammingSession Dieser Diagnosevorgang aktiviert alle Dienste, die in Spalte 6 ‚ECUPS‘ von Tabelle 1 angegeben sind. Diese Dienste unterstützen die Speicherprogrammierung eines Servers (FE). Dieser Diagnosevorgang kann durch andere in diesem Abschnitt genannte Diagnosevorgänge überschrieben werden.	ECUPS
87	ECUAdjustmentSession Dieser Diagnosevorgang aktiviert alle Dienste, die in Spalte 5 ‚ECUAS‘ von Tabelle 1 angegeben sind. Diese Dienste unterstützen die Eingabe/Ausgabe-Steuerung eines Servers (FE). Dieser Diagnosevorgang kann durch andere in diesem Abschnitt genannte Diagnosevorgänge überschrieben werden.	ECUAS

5.2. Der Dienst SecurityAccess

Das Schreiben von Kalibrierungsdaten bzw. der Zugriff auf die Eingabe/Ausgabe-Leitung für die Kalibrierung ist nur dann möglich, wenn sich die FE in der Betriebsart KALIBRIERUNG befindet. Der Zugriff auf die Betriebsart KALIBRIERUNG wird erst gewährt, nachdem eine gültige Werkstattkarte in die FE eingesteckt und zusätzlich die richtige persönliche Geheimzahl (PIN) in die FE eingegeben wurde.

Der Dienst SecurityAccess stellt die Möglichkeit zur PIN-Eingabe bereit und zeigt dem Prüfgerät an, ob sich die FE in der Betriebsart KALIBRIERUNG befindet.

Eine PIN-Eingabe durch alternative Methoden ist zulässig.

5.2.1. Beschreibung der Nachricht

Der Dienst SecurityAccess besteht aus der Anforderung requestSeed, der möglicherweise eine Nachricht sendKey folgt. Der Dienst SecurityAccess muss nach dem Dienst StartDiagnosticSession ausgeführt werden.

CPR_033 Mit der SecurityAccess-Anforderung requestSeed stellt das Prüfgerät fest, ob die Fahrzeugeinheit zur Annahme einer PIN bereit ist.

CPR_034 Befindet sich die Fahrzeugeinheit bereits in der Betriebsart KALIBRIERUNG, beantwortet sie die Anforderung durch Versenden eines Seed 0x0000 mit Hilfe des Dienstes auf SecurityAccess Positive Response.

CPR_035 Ist die Fahrzeugeinheit zur Annahme einer PIN zur Verifizierung einer Werkstattkarte bereit, beantwortet sie die Anforderung durch Versenden eines Seed, der größer als 0x0000 ist, mit Hilfe des Dienstes SecurityAccess Positive Response.

CPR_036 Ist die Fahrzeugeinheit zur Annahme einer PIN vom Prüfgerät nicht bereit, weil entweder die eingesteckte Werkstattkarte ungültig ist, keine Werkstattkarte eingesteckt wurde oder die Fahrzeugeinheit eine andere Methode der PIN-Eingabe erwartet, beantwortet sie die Anforderung mit einer Negative Response, wobei der Antwortcode ‚conditionsNotCorrectOrRequestSequenceError‘ lautet.

CPR_037 Das Prüfgerät sendet dann gegebenenfalls eine SecurityAccess-Nachricht sendKey, um eine PIN an die Fahrzeugeinheit zu übergeben. Um ausreichend Zeit für den Prozess der Kartenauthentisierung zu gewähren, sendet die FE den negativen Antwortcode ‚requestCorrectlyReceived-ResponsePending‘, mit dem die Antwortzeit verlängert wird. Die längstmögliche Wartezeit darf jedoch 5 Minuten nicht überschreiten. Sobald der angeforderte Dienst abgeschlossen ist, sendet die FE eine positive oder negative Antwortnachricht mit einem anderen Antwortcode als diesem. Der negative Antwortcode ‚requestCorrectlyReceived-ResponsePending‘ kann so oft von der FE wiederholt werden, bis der angeforderte Dienst abgeschlossen ist und die abschließende Antwortnachricht gesandt wurde.

CPR_038 Die Fahrzeugeinheit darf diese Anforderung nur dann mit dem Dienst SecurityAccess Positive Response beantworten, wenn sie sich in der Betriebsart KALIBRIERUNG befindet.

CPR_039 In den nachstehenden Fällen muss die Fahrzeugeinheit diese Anforderung mit einer Negative Response bei folgendermaßen gesetzten Antwortcodes quittieren:

- subFunctionNotSupported: ungültiges Format für den Parameter der Unterfunktion (accessType),
- conditionsNotCorrectOrRequestSequenceError: Fahrzeugeinheit ist zur Annahme einer PIN-Eingabe nicht bereit,
- invalidKey: ungültige PIN, Zahl der zulässigen PIN-Prüfversuche jedoch nicht überschritten,
- exceededNumberOfAttempts: ungültige PIN und Zahl der zulässigen PIN-Prüfversuche überschritten,
- generalReject: richtige PIN, gegenseitige Authentisierung mit Werkstattkarte ist jedoch fehlgeschlagen.

5.2.2. Nachrichtenformat — SecurityAccess — requestSeed

CPR_040 Die Nachrichtenformate für die SecurityAccess requestSeed-Primitive sind in den folgenden Tabellen spezifiziert:

Tabelle 18

Anforderungsnachricht SecurityAccess

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	Service Identifier für Anforderung SecurityAccess	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Prüfsumme	00-FF	CS

Tabelle 19

Nachricht Positive Response auf SecurityAccess requestSeed

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	04	LEN
#5	SecurityAccess Positive Response Service Id	67	SAPR
#6	accessType — requestSeed	7D	AT_RSD
#7	H-Seed	00-FF	SEEDH
#8	L-Seed	00-FF	SEEDL
#9	Prüfsumme	00-FF	CS

Tabelle 20

Nachricht Negative Response auf SecurityAccess

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22	RC_CNC
		13	RC_IML
#8	Prüfsumme	00-FF	CS

5.2.3. **Nachrichtenformat — SecurityAccess — sendKey**

CPR_041 Die Nachrichtenformate für die SecurityAccess sendKey-Primitive sind in den folgenden Tabellen spezifiziert:

Tabelle 21

Nachricht SecurityAccess — sendKey

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	m+2	LEN
#5	Service Identifier für Anforderung SecurityAccess	27	SA
#6	accessType — sendKey	7E	AT_SK
#7 bis #m+6	Schlüssel 1 (H)	xx	KEY
	...	...	
	Schlüssel m (N, m muss mindestens 4 und darf höchstens 8 betragen)	xx	
#m+7	Prüfsumme	00-FF	CS

Tabelle 22

Nachricht Positive Response auf SecurityAccess — sendKey

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	02	LEN
#5	Service Identifier für Positive Response auf SecurityAccess	67	SAPR
#6	accessType — sendKey	7E	AT_SK
#7	Prüfsumme	00-FF	CS

Tabelle 23

Nachricht Negative Response auf SecurityAccess

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung SecurityAccess	27	SA
#7	ResponseCode = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Prüfsumme	00-FF	CS

6. DATENÜBERTRAGUNGSDIENSTE

Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 24

Datenübertragungsdienste

Dienstbezeichnung	Beschreibung
ReadDataByIdentifier	Client fordert an, dass der aktuelle Wert eines Datensatzes durch Zugriff von recordData-Identifier übertragen wird
WriteDataByIdentifier	Client fordert an, dass ein Datensatz von recordDataIdentifier geschrieben wird

6.1. Der Dienst ReadDataByIdentifier**6.1.1. Beschreibung der Nachricht**

CPR_050 Mit dem Dienst ReadDataByIdentifier fordert der Client vom Server die Übertragung von Datensatzwerten an, die mit durch einen RecordDataIdentifier gekennzeichnet sind. Der Fahrzeughersteller muss dafür sorgen, dass die Serverbedingungen zur Abwicklung dieses Dienstes erfüllt sind.

6.1.2. Nachrichtenformat

CPR_051 Die Nachrichtenformate für die ReadDataByIdentifier-Primitive sind in den folgenden Tabellen aufgeführt:

Tabelle 25

Anforderungsnachricht ReadDataByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Anforderung ReadDataByIdentifier	22	RDBI
#6 bis #7	RecordDataIdentifier = [ein Wert aus Tabelle 28]	xxxx	RDI_...
#8	Prüfsumme	00-FF	CS

Tabelle 26

Nachricht Positive Response auf ReadDataByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	m+3	LEN
#5	Service Identifier für Positive Response auf ReadDataByIdentifier	62	RDBIPR
#6 bis #7	recordDataIdentifier = [gleicher Wert wie Byte 6 bis 7 in Tabelle 25]	xxxx	RDI_...
#8 bis #m+7	dataRecord[] = [data 1 : data m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Prüfsumme	00-FF	CS

Tabelle 27

Nachricht Negative Response auf ReadDataByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung ReadDataByIdentifier	22	RDBI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Prüfsumme	00-FF	CS

6.1.3. Parameterdefinition

CPR_052 Der Parameter recordDataIdentifier (RDI_) in der Anforderungsnachricht ReadDataByIdentifier kennzeichnet einen Datensatz.

CPR_053 Die hier definierten Werte für recordDataIdentifier sind der folgenden Tabelle aufgeführt.

Die Tabelle recordDataIdentifier enthält 4 Spalten mit mehreren Zeilen.

- Die 1. Spalte (Hex) enthält jeweils den hexadezimalen Wert für die in der 3. Spalte angeführte Anforderungsnachricht recordDataIdentifier.
- Die 2. Spalte (Datenelement) gibt zum jeweiligen recordDataIdentifier das Datenelement gemäß Anlage 1 an (ggf. Umkodierung erforderlich).
- Die 3. Spalte (Beschreibung) enthält den dazugehörigen Namen des recordDataIdentifier.
- Die 4. Spalte (Symbolform) gibt die Symbolschreibweise des jeweiligen recordDataIdentifier an.

Tabelle 28

Definition der Werte für recordDataIdentifier

Hex	Datenelement	Beschreibung von recordDataIdentifier (ISO 16844-7)	Symbolform
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Der Parameter dataRecord (DREC_) dient der Nachricht Positive Response auf ReadDataByIdentifier dazu, dem Client (Prüfgerät) den durch die recordDataIdentifier gekennzeichneten Datensatz bereitzustellen. Die Datensatzformate werden in Abschnitt 8 definiert. Es können zusätzliche, vom Benutzer wählbare dataRecord-Werte, z. B. FE-abhängige Eingabedaten, interne Daten und Ausgabedaten integriert werden, diese werden jedoch hier nicht definiert.

6.2. Der Dienst WriteDataByIdentifier**6.2.1. Beschreibung der Nachricht**

CPR_056 Der Dienst WriteDataByIdentifier dient dem Client dazu, Datensatzwerte auf einen Server zu schreiben. Die Daten sind durch einen recordDataIdentifier gekennzeichnet. Der Fahrzeughersteller muss dafür sorgen, dass die Serverbedingungen zur Abwicklung dieses Dienstes erfüllt sind. Zur Aktualisierung der in Tabelle 28 aufgeführten Parameter muss sich die FE in der Betriebsart KALIBRIERUNG befinden.

6.2.2. Nachrichtenformat

CPR_057 Die Nachrichtenformate für die WriteDataByIdentifier-Primitive sind in den folgenden Tabellen aufgeführt:

Tabelle 29

Anforderungsnachricht WriteDataByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	m+3	LEN
#5	Service Identifier für Anforderung WriteDataByIdentifier	2E	WDBI
#6 a #7	recordDataIdentifier = [ein Wert aus Tabelle 28]	xxxx	RDI_...
#8 bis #m+7	dataRecord[] = [data 1 : data m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Prüfsumme	00-FF	CS

Tabelle 30

Nachricht Positive Response auf WriteDataByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Positive Response WriteDataByIdentifier	6E	WDBIPR
#6 bis #7	recordDataIdentifier = [gleicher Wert wie Byte 6 bis 7 in Tabelle 29]0	xxxx	RDI_...
#8	Prüfsumme	00-FF	CS

Tabelle 31

Nachricht Negative Response auf WriteDataByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung WriteDataByIdentifier	2E	WDBI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31	RC_ROOR
		13	RC_IML
		22	RC_CNC
#8	Prüfsumme	00-FF	CS

6.2.3. Parameterdefinition

Der Parameter recordDataIdentifier (RDI_) ist in Tabelle 28 definiert.

Der Parameter dataRecord (DREC_) dient der Aufforderungsnachricht WriteDataByIdentifier dazu, dem Server (FE) den durch die recordDataIdentifier gekennzeichneten Datensatzwerte bereitzustellen. Die Datensatzformate werden in Abschnitt 8 definiert.

7. PRÜFIMPULSSTEUERUNG — FUNKTIONSEINHEIT EINGABE/AUSGABE-STEUERUNG

Die zur Verfügung stehenden Dienste sind in nachstehender Tabelle aufgeführt:

Tabelle 32

Funktionseinheit Eingabe/Ausgabe-Steuerung

Dienstbezeichnung	Beschreibung
InputOutputControlByIdentifier	Der Client fordert die Steuerung einer speziellen Eingabe/Ausgabe für den Server an

7.1. Der Dienst InputOutputControlByIdentifier**7.1.1. Beschreibung der Nachricht**

Über einen der Steckanschlüsse an der Vorderseite ist es möglich, Prüfimpulse mit einem geeigneten Prüfgerät zu steuern bzw. zu überwachen.

CPR_058 Diese Kalibrierungs-E/A-Signalleitung ist mit einem K-Leitungsbefehl konfigurierbar, wobei mit dem Dienst InputOutputControlByIdentifier die für die Leitung gewünschte Eingabe- bzw. Ausgabefunktion gewählt wird. Es gibt folgende Leitungszustände:

- deaktiviert,
- speedSignalInput: über die Kalibrierungs-E/A-Signalleitung wird ein Geschwindigkeitssignal (Testsignal) eingegeben, das das Geschwindigkeitssignal des Weg- und Geschwindigkeitsgebers ersetzt,
- realTimeSpeedSignalOutputSensor: über die Kalibrierungs-E/A-Signalleitung wird das Geschwindigkeitssignal des Weg- und Geschwindigkeitsgebers ausgegeben,
- RTCOutput: über die Kalibrierungs-E/A-Signalleitung wird das UTC-Zeitsignal ausgegeben.

CPR_059 Um den Leitungsstatus zu konfigurieren, muss sich die Fahrzeugeinheit in einem Einstellvorgang befinden und in die Betriebsart KALIBRIERUNG gesetzt sein. Bei Verlassen des Einstellvorgangs bzw. der Betriebsart KALIBRIERUNG muss die Fahrzeugeinheit die Rückkehr der E/A-Signalleitung in den Status ‚deaktiviert‘ (Standardzustand) gewährleisten.

CPR_060 Treffen an der Echtzeit-Eingabeleitung für Geschwindigkeitssignale der FE Geschwindigkeitsimpulse ein, während die E/A-Signalleitung auf Eingabe gesetzt ist, muss die E/A-Signalleitung auf Ausgabe gesetzt werden oder in den deaktivierten Zustand zurückkehren.

CPR_061 Der Ablauf muss wie folgt sein:

- Aufbau der Verbindung durch den Dienst StartCommunication
- Einleiten eines Einstellvorgangs durch den Dienst StartDiagnosticSession und Eintritt in die Betriebsart KALIBRIERUNG (die Reihenfolge dieser beiden Vorgänge ist nicht von Bedeutung).
- Änderung des Ausgabestatus durch den Dienst InputOutputControlByIdentifier.

7.1.2. Nachrichtenformat

CPR_062 Die Nachrichtenformate für die InputOutputControlByIdentifier-Primitive sind in den folgenden Tabellen spezifiziert:

Tabelle 33

Anforderungsnachricht InputOutputControlByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	EE	TGT
#3	Quelladress-Byte	tt	SRC
#4	Zusatzlängen-Byte	xx	LEN
#5	Service Identifier für Anforderung InputOutputControlByIdentifier	30	IOCBI
#6 bis #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 oder #8 bis #9	ControlOptionRecord = [inputOutputControlParameter — ein Wert aus Tabelle 36 controlState — ein Wert aus Tabelle 37 (siehe Hinweis unten)]	xx	COR_... IOCP_...
		xx	CS_...
#9 oder #10	Prüfsumme	00-FF	CS

Hinweis: Der Parameter controlState liegt nur in bestimmten Fällen vor (siehe 7.1.3).

Tabelle 34

Nachricht Positive Response auf InputOutputControlByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	xx	LEN
#5	Service Identifier für Positive Response auf inputOutputControl-ByIdentifier	6F	IOCBIPR
#6 bis #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#7 bis #8	controlStatusRecord = [inputOutputControlParameter (gleicher Wert wie Byte 8 in Tabelle 33)	xx	CSR_ IOCP_...
	controlState (gleicher Wert wie Byte 9 in Tabelle 33)]	xx	CS_...
#9	Prüfsumme	00-FF	CS

Tabelle 35

Nachricht Negative Response auf InputOutputControlByIdentifier

Byte-Nr.	Parameterbezeichnung	Hex-Wert	Symbolform
#1	Format-Byte — Physische Adressierung	80	FMT
#2	Zieladress-Byte	tt	TGT
#3	Quelladress-Byte	EE	SRC
#4	Zusatzlängen-Byte	03	LEN
#5	Service Identifier für Negative Response	7F	NR
#6	Service Identifier für Anforderung inputOutputControlByIdentifier	2F	IOCBNI
#7	responseCode = [incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Prüfsumme	00-FF	CS

7.1.3. Parameterdefinition

CPR_064 Der Parameter inputOutputControlParameter (IOCP_) ist in folgender Tabelle beschrieben:

Tabelle 36

Definition der Werte für inputOutputControlParameter

Hex	Beschreibung	Symbolform
00	ReturnControlToECU Dieser Wert zeigt dem Server (FE) an, dass das Prüfgerät die Steuerung der Kalibrierungs-E/A-Signalleitung beendet hat.	RCTECU
01	ResetToDefault Dieser Wert zeigt dem Server (FE) die Anforderung an, den Status der Kalibrierungs-E/A-Signalleitung in den Standardstatus zurückzusetzen.	RTD
03	ShortTermAdjustment Dieser Wert zeigt dem Server (FE) die Anforderung an, die Kalibrierungs-E/A-Signalleitung auf den im Parameter controlState enthaltenen Wert einzustellen.	STA

CPR_065 Der Parameter controlState liegt nur vor, wenn der inputOutputControlParameter auf ShortTermAdjustment gesetzt ist; folgende Werte sind möglich:

Tabelle 37

Beschreibung der Werte für controlState

Betriebsart	Hex-Wert	Beschreibung
Deaktiviert	00	E/A-Leitung deaktiviert (Ausgangszustand)
Aktiviert	01	Kalibrierungs-E/A-Leitung als speedSignalInput aktiviert
Aktiviert	02	Kalibrierungs-E/A-Leitung als realTimeSpeedSignalOutputSensor aktiviert
Aktiviert	03	Kalibrierungs-E/A-Leitung als RTCOutput aktiviert

8. DATENSATZFORMATE

Dieser Abschnitt enthält:

- allgemeine Regeln für die Parameter, die von der Fahrzeugeinheit zum Prüfgerät übertragen werden,
- die Beschreibung der Formate für die in Abschnitt 6 erläuterten Datenübertragungsdienste.

CPR_067 Alle hier angegebenen Parameter müssen von der FE unterstützt werden.

CPR_068 Von der FE an das Prüfgerät aufgrund einer Anforderungsnachricht übertragene Daten müssen dem jeweiligen Messtyp entsprechen (d. h. dem aktuellen Wert des angeforderten Parameters, wie ihn die FE gemessen oder vorgegeben hat).

8.1. Wertebereiche der übertragenen Parameter

CPR_069 Tabelle 38 enthält die Wertebereiche, mit deren Hilfe die Gültigkeit der übermittelten Parameter festgestellt wird.

CPR_070 Mit den Werten im Bereich ‚Errorindikator‘ kann die Fahrzeugeinheit sofort mitteilen, dass aufgrund eines Fehlers im Kontrollgerät derzeit keine gültigen Werte vorhanden sind.

CPR_071 Mit den Werten im Bereich ‚Nicht verfügbar‘ kann die Fahrzeugeinheit eine Nachricht übermitteln, die einen in diesem Modul nicht verfügbaren oder nicht unterstützten Parameter enthält. Die Werte im Bereich ‚Nicht angefordert‘ ermöglichen es der Fahrzeugeinheit eine Befehlsnachricht zu übermitteln und die Parameter anzugeben, für die es vom anderen Gerät keine Antwort erwartet.

CPR_072 Können wegen eines defekten Bauteils keine gültigen Daten für einen Parameter übermittelt werden, sollte mit dem in Tabelle 38 angegebenen Fehlerindikator anstelle von Daten für den angeforderten Parameter geantwortet werden. Wenn die gemessenen oder errechneten Daten Werte annehmen, die zwar gültig sind, aber außerhalb des festgelegten Wertebereichs für diesen Parameter liegen, ist der Fehlerindikator jedoch nicht zu verwenden. In diesem Fall sollte der jeweilige Mindest- oder Höchstwert für diesen Parameter übertragen werden.

Tabelle 38

Wertebereiche der dataRecords

Wertebereichsname	1 Byte (Hex-Wert)	2 Bytes (Hex-Wert)	4 Bytes (Hex-Wert)	ASCII
Gültiges Signal	00 bis FA	0000 bis FAFF	00000000 bis FFFFFFFF	1 bis 254
Parameterspezifischer Indikator	FB	FB00 bis FBFF	FB000000 bis FBFFFFFF	keiner
Reserviert für künftige Indikatorbits	FC bis FD	FC00 bis FDFF	FC000000 bis FDFFFFFF	keiner
Fehlerindikator	FE	FE00 bis FEFF	FE000000 bis FEFFFFFF	0
Nicht verfügbar oder nicht angefordert	FF	FF00 bis FFFF	FF000000 bis FFFFFFFF	FF

CPR_073 Bei den in ASCII dargestellten Parametern ist der Stern '*' als Trennzeichen reserviert.

8.2. dataRecords-Formate

In Tabelle 39 bis Tabelle 42 sind die Datensatzformate für die Dienste ReadDataByIdentifier und WriteDataByIdentifier angegeben.

CPR_074 In Tabelle 39 sind die Länge, die Auflösung und der Betriebsbereich für jeden durch seinen recordDataIdentifier gekennzeichneten Parameter aufgeführt:

Tabelle 39

dataRecords-Formate

Parameterbezeichnung	Datenlänge (Byte)	Auflösung	Betriebsbereich
TimeDate	8	siehe Tabelle 40	
HighResolutionTotalVehicleDistance	4	Zuwachs 5 m/Bit, Ausgangswert 0 m	0 bis + 21 055 406 km
Kfactor	2	Zuwachs 0,001 Impulse/m/Bit, Ausgangswert 0	0 bis 64,255 pulse/m
LfactorTyreCircumference	2	Zuwachs 0,125 10 ⁻³ m/Bit, Ausgangswert 0	0 bis 8 031 m
WvehicleCharacteristicFactor	2	Zuwachs 0,001 Impulse/m/Bit, Ausgangswert 0	0 bis 64,255 Impulse/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	siehe Tabelle 41	
SpeedAuthorised	2	Zuwachs 1/256 km/h/Bit, Ausgangswert 0	0 bis 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	siehe Tabelle 42	
VIN	17	ASCII	ASCII

CPR_075 Tabelle 40 enthält die Formate der verschiedenen Bytes für den Parameter TimeDate:

Tabelle 40

Ausführliches Format des Parameters TimeDate (recordDataIdentifier-Wert F00B)

Byte	Parameterdefinition	Auflösung	Betriebsbereich
1	Sekunden	Zuwachs 0,25 s/Bit, Ausgangswert 0 s	0 bis 59,75 s
2	Minuten	Zuwachs 1 min/Bit, Ausgangswert 0 min	0 bis 59 min
3	Stunden	Zuwachs 1 h/Bit, Zuwachs 0 h	0 bis 23 h
4	Monat	Zuwachs 1 Monat/Bit, Ausgangswert 0 Monate	1 bis 12 Monate
5	Tag	Zuwachs 0,25 Tag/Bit, Ausgangswert 0 Tage (siehe Hinweis unter Tabelle 41)	0,25 bis 31,75 Tage
6	Jahr	Zuwachs 1 Jahr/Bit, Ausgangswert +1985 Jahre (siehe Hinweis unter Tabelle 41)	1985 bis 2235 Jahre
7	Lokaler Ausgangswert Minuten	Zuwachs 1 min/Bit, Ausgangswert – 125 min	– 59 bis 59 min
8	Lokaler Ausgangswert Stunden	Zuwachs 1 h/Bit, Ausgangswert – 125 h	– 23 bis + 23 h

CPR_076 Tabelle 41 enthält die Formate der verschiedenen Bytes für den Parameter NextCalibrationDate:

Tabelle 41

Ausführliches Format des Parameters NextCalibrationDate (recordDataIdentifier-Wert F022)

Byte	Parameterdefinition	Auflösung	Betriebsbereich
1	Monat	Zuwachs 1 Monat/Bit, Ausgangswert 0 Monate	1 bis 12 Monate
2	Tag	Zuwachs 0,25 Tage/Bit, Ausgangswert 0 Tage (siehe Hinweis unten)	0,25 bis 31,75 Tage
3	Jahr	Zuwachs 1 Jahr/Bit, Ausgangswert +1985 Jahre (siehe Hinweis unten)	1985 bis 2235 Jahre

Hinweis zur Verwendung des Tag-Parameters:

1. Der Datumswert 0 ist ungültig. Die Werte 1, 2, 3 und 4 kennzeichnen den ersten Tag des Monats; die Werte 5, 6, 7 und 8 kennzeichnen den zweiten Tag des Monats usw.
2. Dieser Parameter hat keinen Einfluss auf den Stundenparameter oben.

Hinweis zur Verwendung des Jahr-Parameterbits:

Der Wert 0 für das Jahr kennzeichnet das Jahr 1985; der Wert 1 das Jahr 1986 usw.

CPR_078 Tabelle 42 enthält die Formate der verschiedenen Bytes für den Parameter VehicleRegistrationNumber:

Tabelle 42

Ausführliches Format des Parameters VehicleRegistrationNumber (recordDataIdentifier-Wert F07E)

Byte	Parameterdefinition	Auflösung	Betriebsbereich
1	Codeseite (entsprechend Anhang 1)	ASCII	01 bis 0A
2 bis 14	amtliches Kennzeichen (entsprechend Anhang 1)	ASCII	ASCII

*Anlage 9***BAUARTGENEHMIGUNG — MINDESTANFORDERUNGEN AN DIE DURCHZUFÜHRENDEN PRÜFUNGEN**

INHALTSVERZEICHNIS

1.	Einleitung	191
1.1.	Bauartgenehmigung	191
1.2.	Referenzdokumente	191
2.	Funktionsprüfungen an der Fahrzeugeinheit	192
3.	Funktionsprüfungen am Weg- und/oder Geschwindigkeitsgeber	195
4.	Funktionsprüfungen an Kontrollgerätarten	197
5.	Interoperabilitätsprüfungen	198

1. EINLEITUNG

1.1. Bauartgenehmigung

Die EWG-Bauartgenehmigung von Kontrollgeräten (oder deren Komponenten) oder einer Kontrollgerätkarte beruht auf:

- einer Sicherheitszertifizierung durch eine ITSEC-Stelle anhand einer Sicherheitsvorgabe in völliger Übereinstimmung mit Anlage 10 dieses Anhangs,
- einer Funktionszertifizierung durch die Behörde eines Mitgliedstaates, mit der bestätigt wird, dass das geprüfte Teil hinsichtlich der ausgeführten Funktionen, der Messgenauigkeit und der Umwelteigenschaften die Anforderungen dieses Anhangs erfüllt,
- einer Interoperabilitätszertifizierung durch die zuständige Stelle, mit der bestätigt wird, dass das Kontrollgerät (oder die Kontrollgerätkarte) mit dem erforderlichen Muster der Kontrollgerätkarte (bzw. des Kontrollgeräts) (siehe Kapitel VIII in diesem Anhang) uneingeschränkt interoperabel ist.

In dieser Anlage ist in Form von Mindestanforderungen festgelegt, welche Prüfungen eine Behörde der Mitgliedstaaten während der Funktionsprüfungen und welche Prüfungen eine zuständige Stelle während der Interoperabilitätsprüfungen durchführen muss. Die Verfahren zur Durchführung der Prüfungen bzw. die Art der Prüfungen werden nicht weiter spezifiziert.

Die Aspekte der Sicherheitszertifizierung sind in dieser Anlage nicht enthalten. Werden bestimmte Prüfungen bereits für die Bauartgenehmigung im Rahmen des Verfahrens zur Sicherheitsbewertung und -zertifizierung durchgeführt, so brauchen diese Prüfungen nicht wiederholt zu werden. In diesem Fall sind lediglich die Ergebnisse dieser Sicherheitsprüfungen nachzuprüfen. Zu Informationszwecken sind in dieser Anlage Anforderungen, bei denen während der Sicherheitszertifizierung die Durchführung einer Prüfung erwartet wird (oder die mit durchzuführenden Prüfungen in einem engen Verhältnis stehen), mit einem „*“ gekennzeichnet.

In dieser Anlage wird die Bauartgenehmigung für den Weg- und/oder Geschwindigkeitsgebers getrennt von der für die Fahrzeugeinheit betrachtet, da es sich dabei um Komponenten des Kontrollgeräts handelt. Da Interoperabilität nicht zwischen sämtlichen Modellen von Weg- und/oder Geschwindigkeitsgebern und Fahrzeugeinheiten erforderlich ist, kann die Bauartgenehmigung für einen Weg- und/oder Geschwindigkeitsgeber nur in Verbindung mit der Bauartgenehmigung für eine Fahrzeugeinheit und umgekehrt erteilt werden.

1.2. Referenzdokumente

Referenzdokumente zu dieser Anlage:

IEC 68-2-1	Environmental testing — Part 2: Tests — Tests A: Cold. 1990 + Amendment 2: 1994.
IEC 68-2-2	Environmental testing — Part 2: Tests — Tests B: Dry heat. 1974 + Amendment 2: 1994.
IEC 68-2-6	Basic environmental testing procedures — Test methods — Test Fc and guidance: Vibrations (sinusoidal). 6th edition: 1985.
IEC 68-2-14	Basic environmental testing procedures — Test methods — Test N: Change of temperature. Modification 1: 1986.
IEC 68-2-27	Basic environmental testing procedures — Test methods — Test Ea and guidance: Shock. Edition 3: 1987.
IEC 68-2-30	Basic environmental testing procedures — Test methods — Test Db and guidance: Damp heat, cyclic (12 + 12 — hour cycle). Modification 1: 1985.
IEC 68-2-35	Basic environmental testing procedure — Test methods — Test Fda: Random Vibrations wide band — Reproducibility High. Modification 1: 1983.
IEC 529	Degrees of protection provided by enclosures (IP code). Edition 2: 1989.
IEC 61000-4-2	Electromagnetic Compatibility (EMC) — Testing and measurement techniques — Electrostatic discharge immunity test: 1995/Amendment 1: 1998
ISO 7637-1	Road vehicles — Electrical disturbance by conduction and coupling — Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage — Electrical transient conduction along supply lines only. Edition 2: 1990. (Straßenfahrzeuge; Elektrische Störungen durch Leitung und Kopplung; Teil 1: Personenkraftwagen und leichte Nutzkraftwagen mit 12-V-Bordnetzen — Leitungsgeführte Störgrößen auf Versorgungsleitungen)

- ISO 7637-2 Road vehicles — Electrical disturbance by conduction and coupling — Part 2: Commercial vehicles with nominal 24 V supply voltage — Electrical transient conduction along supply lines only. First edition: 1990. (Straßenfahrzeuge; Elektrische Störungen durch Leitung und Kopplung; Teil 2: Nutzkraftwagen mit 24-V-Bordnetzen; Leitungsgeführte Störgrößen auf Versorgungsleitungen)
- ISO 7637-3 Road vehicles — Electrical disturbance by conduction and coupling — Part 3: Vehicles with 12 V or 24 V supply voltage — Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995. (Straßenfahrzeuge — Elektrische Störungen durch Leitung und Kopplung — Teil 3: Fahrzeuge mit 12 V oder 24 V Nenn-Versorgungsspannung — Kapazitiv und induktiv gekoppelte Störungen auf andere als Versorgungsleitungen)
- ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics. First edition: 1998. (Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 1: Physikalische Eigenschaften)
- ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999. (Informationstechnik — Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 2: Abmessungen und Lage der Kontakte)
- ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997. (Informationstechnik — Identifikationskarten — Chipkarten mit Kontakten — Teil 3: Elektronische Eigenschaften und Übertragungsprotokolle)
- ISO/IEC 10373 Identification cards — Test methods. First edition: 1993. (Identifikationskarten — Prüfverfahren)

2. FUNKTIONSPRÜFUNGEN AN DER FAHRZEUGEINHEIT

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
1.	Administrative Prüfung		
1.1.	Dokumentation	Richtigkeit der Dokumentation	
1.2.	Prüfergebnisse des Herstellers	Ergebnisse der beim Einbau vom Hersteller durchgeführten Prüfung. Nachweis auf Papier	070, 071, 073
2.	Sichtprüfung		
2.1.	Übereinstimmung mit der Dokumentation		
2.2.	Kennung/Markierungen		168, 169
2.3.	Werkstoffe		163 bis 167
2.4.	Plombierung		251
2.5.	Externe Schnittstellen		
3.	Funktionsprüfungen		
3.1.	Mögliche Funktionen		002, 004, 244
3.2.	Betriebsarten		006*, 007*, 008*, 009*, 106, 107
3.3.	Funktionen und Datenzugriffsrechte		010*, 011*, 240, 246, 247
3.4.	Überwachung des Einsteckens und Entnehmens der Karten		013, 014, 015*, 016*, 106
3.5.	Geschwindigkeits- und Wegstreckenmessung		017 bis 026
3.6.	Zeitmessung (Prüfung bei 20 °C)		027 bis 032
3.7.	Überwachung der Fahrtätigkeiten		033 bis 043, 106
3.8.	Überwachung des Status der Fahrzeugführung		044, 045, 106
3.9.	Manuelle Eingabe durch die Fahrer		046 bis 050b
3.10.	Verwaltung der Unternehmenssperrern		051 bis 055
3.11.	Überwachung von Kontrollaktivitäten		056, 057
3.12.	Feststellung von Ereignissen und Störungen		059 bis 069, 106

Nr.	Prüfung	Beschreibung	Anforderungsent- sprechung
3.13.		Kenndaten der Fahrzeugeinheit	075*, 076*, 079
3.14.		Einsteck- und Entnahmedaten der Fahrerkarte	081* bis 083*
3.15.		Fahrertätigkeitsdaten	084* bis 086*
3.16.		Ort des Arbeitstagsbeginns und -endes	087* bis 089*
3.17.		Kilometerstandsdaten	090* bis 092*
3.18.		Detaillierte Geschwindigkeitsdaten	093*
3.19.		Ereignisdaten	094*, 095
3.20.		Störungsdaten	096*
3.21.		Kalibrierungsdaten	097*, 098*
3.22.		Zeiteinstellungsdaten	100*, 101*
3.23.		Kontrolldaten	102*, 103*
3.24.		Unternehmenssperrdaten	104*
3.25.		Erfassen des Herunterladens	105*
3.26.		Daten zu spezifischen Bedingungen	105a*, 105b*
3.27.		Aufzeichnung und Speicherung von Daten auf Kontrollgerätarten	108, 109*, 109a*, 110*, 111, 112
3.28.		Anzeige	072, 106, 113 bis 128, PIC_001, DIS_001
3.29.		Drucken	072, 106, 129 bis 138, PIC_001, PRT_001 bis PRT_012
3.30.		Warnung	106, 139 bis 148, PIC_001
3.31.		Herunterladen von Daten auf externe Datenträger	072, 106, 149 bis 151
3.32.		Datenausgabe an zusätzliche externe Geräte	152, 153
3.33.		Kalibrierung	154*, 155*, 156*, 245
3.34.		Zeiteinstellung	157*, 158*
3.35.		Störungsfreiheit zusätzlicher Funktionen	003, 269

Nr.	Prüfung	Beschreibung	Anforderungsentsprechung
4.	Umweltprüfungen		
4.1.	Temperatur	Funktionsprüfung anhand: — IEC 68-2-1, Prüfung Ad, Prüfdauer 72 Std. bei Mindesttemperatur (- 20 °C), 1 Std. Betrieb, 1 Std. außer Betrieb, — IEC 68-2-2, Prüfung Bd, Prüfdauer 72 Std. bei Höchsttemperatur (+ 70 °C), 1 Std. Betrieb, 1 Std. außer Betrieb Temperaturzyklen: IEC 68-2-14 Prüfung Na zum Nachweis, dass Fahrzeugeinheit einem raschen Wechsel der Umgebungstemperatur standhält, 20 Zyklen, jeweils mit einem Temperaturwechsel zwischen Mindest- (- 20 °C) und Höchsttemperatur (+ 70 °C) und jeweils 2 Std. Verweilzeit bei Mindest- und Höchsttemperatur In Bezug auf Mindest- und Höchsttemperatur sowie während der Temperaturzyklen ist (für die in Abschnitt 3 dieser Tabelle aufgeführten Prüfungen) eine geringere Anzahl an Prüfungen zulässig	159
4.2.	Luftfeuchtigkeit	IEC 68-2-30, Prüfung Db, zum Nachweis, dass die Fahrzeugeinheit einer zyklischen Feuchtigkeitsprüfung (Wärmeprüfung) von sechs 24-Std.-Zyklen jeweils mit einer Temperaturänderung von + 25 °C bis + 55 °C und einer relativen Luftfeuchtigkeit von 97 % bei + 25 °C bzw. entsprechend 93 % bei + 55 °C standhält	160
4.3.	Schwingungen	1. Sinusschwingungen: Nachweis, dass Fahrzeugeinheit Sinusschwingungen mit folgenden Merkmalen standhält konstante Verschiebung zwischen 5 und 11 Hz: max. 10 mm konstante Beschleunigung zwischen 11 und 300 Hz: 5 g Nachweis nach IEC 68-2-6, Prüfung Fc, mit Mindestprüfdauer von 3 × 12 Std. (12 Std. je Achse) 2. Zufallsschwingungen: Nachweis, dass Fahrzeugeinheit Zufallsschwingungen mit folgenden Merkmalen standhält: Frequenz 5—150 Hz, Ebene 0,02 g²/Hz Nachweis nach IEC 68-2-35, Prüfung Ffda, mit Mindestprüfdauer von 3 × 12 Std. (12 Std. je Achse), 1 Std. in Betrieb, 1 Std. außer Betrieb Diese beiden Prüfungen werden an zwei unterschiedlichen Proben des zu prüfenden Gerätetyps durchgeführt	163
4.4.	Schutz vor Wasser und Fremdkörpern	Nachweis, dass Schutzgrad der Fahrzeugeinheit in eingebautem Zustand in einem Fahrzeug unter Betriebsbedingungen nach IEC 529 mindestens IP 40 beträgt	164, 165
4.5.	Überspannungsschutz	Nachweis, dass die Fahrzeugeinheit folgende Versorgungsspannungen aushält: 24-V-Modelle: 34 V bei + 40 °C 1 Std. 12-V-Modelle: 17 V bei + 40 °C 1 Std.	161
4.6.	Falschpolungsschutz	Nachweis, dass die Fahrzeugeinheit einer Umkehrung der Polarität der Stromversorgung standhält	161

Nr.	Prüfung	Beschreibung	Anforderungsent-sprechung
4.7.	Kurzschlusschutz	Nachweis, dass für Eingangs-/Ausgangssignale Schutz vor Kurzschluss der Stromversorgung und vor Erdschluss besteht	161
5.	EMV-Prüfungen		
5.1.	Störaussendung und Störanfälligkeit	Einhaltung der Richtlinie 95/54/EWG	162
5.2.	Elektrostatische Entladung	Einhaltung von IEC 61000-4-2, ± 2 kV (Stufe 1)	162
5.3.	Leitungsgeführte Störgrößen auf Versorgungsleitungen	Bei 24-V-Modellen: Einhaltung von ISO 7637-2 Impuls 1a: $V_s = -100$ V, $R_i = 10$ Ohm Impuls 2: $V_s = +100$ V, $R_i = 10$ Ohm Impuls 3a: $V_s = -100$ V, $R_i = 50$ Ohm Impuls 3b: $V_s = +100$ V, $R_i = 50$ Ohm Impuls 4: $V_s = -16$ V, $V_a = -12$ V, $t_6 = 100$ ms Impuls 5: $V_s = +120$ V, $R_i = 2,2$ Ohm, $t_d = 250$ ms Bei 12-V-Modellen: Einhaltung von ISO 7637-1 Impuls 1: $V_s = -100$ V, $R_i = 10$ Ohm Impuls 2: $V_s = +100$ V, $R_i = 10$ Ohm Impuls 3a: $V_s = -100$ V, $R_i = 50$ Ohm Impuls 3b: $V_s = +100$ V, $R_i = 50$ Ohm Impuls 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms Impuls 5: $V_s = +65$ V, $R_i = 3$ Ohm, $t_d = 100$ ms Impuls 5 ist nur in Fahrzeugeinheiten zu prüfen, die in Fahrzeugen installiert werden sollen, für die keine gemeinsame externe Blindlast vorgesehen ist	162

3. FUNKTIONSPRÜFUNGEN AM WEG- UND/ODER GESCHWINDIGKEITSGEBER

Nr.	Prüfung	Beschreibung	Anforderungsent-sprechung
1.	Administrative Prüfung		
1.1.	Dokumentation	Richtigkeit der Dokumentation	
2.	Sichtprüfung		
2.1.	Übereinstimmung mit der Dokumentation		
2.2.	Kennung/Markierungen		169, 170
2.3.	Werkstoffe		163 bis 167
2.4.	Plombierung		251
3.	Funktionsprüfungen		
3.1.	Kenndaten des Weg- und/oder Geschwindigkeitsgebers		077*
3.2.	Koppelung des Weg- und/oder Geschwindigkeitsgebers mit der Fahrzeugeinheit		099*, 155
3.3.	Messung Wegstrecke/Geschwindigkeit		
	Messgenauigkeit Wegstrecke/Geschwindigkeit		022 bis 026

Nr.	Prüfung	Beschreibung	Anforderungsent- sprechung
4.	Umweltprüfungen		
4.1.	Betriebstemperatur	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) im Temperaturbereich [- 40 °C; + 135 °C] anhand: — IEC 68-2-1, Prüfung Ad, Prüfdauer 96 Std. bei Mindesttemperatur $T_{\min}$ — IEC 68-2-2, Prüfung Bd, Prüfdauer 96 Std. bei Höchsttemperatur $T_{\max}$	159
4.2.	Temperaturzyklen	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) anhand IEC 68-2-14, Prüfung Na, 20 Zyklen, jeweils mit Wechsel von der Mindest- (- 40 °C) zur Höchsttemperatur (+135 °C) und jeweils 2 Std. Verweilzeit bei Mindest- und Höchsttemperatur In Bezug auf Mindest- und Höchsttemperatur sowie während der Temperaturzyklen ist (für die in Prüfung 3.3 aufgeführten Prüfungen) eine geringere Anzahl an Prüfungen zulässig	159
4.3.	Luftfeuchtigkeitszyklen	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) anhand IEC 68-2-30, Prüfung Db, sechs 24-Std.-Zyklen, jeweils mit einer Temperaturänderung von + 25 °C bis + 55 °C und einer relativen Luftfeuchtigkeit von 97 % bei + 25 °C bzw. entsprechend 93 % bei + 55 °C	160
4.4.	Schwingungen	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) anhand IEC 68-2-6, Prüfung Fc, Prüfdauer 100 Frequenzzyklen: konstante Verschiebung zwischen 10 und 57 Hz: max. 1,5 mm konstante Beschleunigung zwischen 57 und 500 Hz: 20 g	163
4.5.	Mechanischer Stoß	Prüfung der Funktionstüchtigkeit (entsprechend Festlegung in Prüfung Nr. 3.3) anhand IEC 68-2-27, Prüfung Ea, 3 Stöße in beiden Richtungen der 3 senkrechten Achsen	163
4.6.	Schutz vor Wasser und vor Fremdkörpern	Nachweis, dass Schutzgrad des Weg- und/oder Geschwindigkeitsgebers in eingebautem Zustand in einem Fahrzeug unter Betriebsbedingungen gemäß IEC 529 IP mindestens 64 beträgt	165
4.7.	Falschpolungsschutz	Nachweis, dass der Weg- und/oder Geschwindigkeitsgeber einer Umkehrung der Polarität der Stromversorgung standhält	161
4.8.	Kurzschlusschutz	Nachweis, dass für Eingangs-/Ausgangssignale Schutz vor Kurzschluss der Stromversorgung und vor Erdschluss besteht	161
5.	EMV		
5.1.	Störaussendung und Störanfälligkeit	Nachweis der Einhaltung der Richtlinie 95/54/EWG	162
5.2.	Elektrostatische Entladung	Einhaltung von IEC 61000-4-2, ± 2 kV (Stufe 1)	162
5.3.	Anfälligkeit gegenüber leitungsgeführten Störgrößen auf Datenleitungen	Einhaltung von ISO 7637-3 (Stufe III)	162

4. FUNKTIONSPRÜFUNGEN AN KONTROLLGERÄTKARTEN

Nr.	Prüfung	Beschreibung	Anforderungsent-sprechung
1.	Administrative Prüfung		
1.1.	Dokumentation	Richtigkeit der Dokumentation	
2.	Sichtprüfung		
2.1.		Gewährleistung, dass sämtliche Schutzanforderungen und die sichtbar anzubringenden Angaben korrekt gedruckt sind und den Vorgaben entsprechen	171 bis 181
3.	Physische Prüfungen		
3.1.	Kontrolle der Abmessungen der Karten und der Lage der Kontakte		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Protokollprüfungen		
4.1.	ATR	Prüfen, dass ATR den Anforderungen entspricht	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Prüfen, dass Protokoll T=0 den Anforderungen entspricht	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Prüfen, dass Kommando PTS durch Einstellen von T=1 ausgehend von T=0 den Anforderungen entspricht	ISO/IEC 7816-3 TCS 309 a 311
4.4.	T=1	Prüfen, dass Protokoll T=1 den Anforderungen entspricht	ISO/IEC 7816-3 TCS 303, / 306
5.	Kartenstruktur		
5.1.		Prüfen, dass die Dateistruktur der Karte den Anforderungen entspricht. Hierzu sind das Vorhandensein der obligatorischen Dateien auf der Karte und die Zugriffsbedingungen darauf zu überprüfen	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Funktionsprüfungen		
6.1.	Normale Verarbeitung	Für jeden Befehl ist jede zulässige Ausführung zumindest einmal zu prüfen (z. B.: Prüfung des Befehls UPDATE BINARY mit CLA = '00', CLA = '0C' und mit unterschiedlichen Parametern P1, P2 und Lc). Prüfen, dass die Operationen auf der Karte tatsächlich ausgeführt wurden (z. B.: durch das Lesen der Datei, in der der Befehl ausgeführt wurde)	TCS 313 bis TCS 379
6.2.	Fehlermeldungen	Für jeden Befehl ist jede Fehlermeldung (entsprechend Anlage 2) zumindest einmal zu prüfen. Jeder generische Fehler ist zumindest einmal zu prüfen (mit Ausnahme von '6400'-Integritätsfehlern, die während der Sicherheitszertifizierung geprüft werden)	
7.	Umweltprüfungen		
7.1.		Gewährleistung, dass die Karten innerhalb der in Übereinstimmung mit ISO/IEC 10373 festgelegten Grenzbedingungen funktionstüchtig sind	185 bis 188 ISO/IEC 7816-1

5. INTEROPERABILITÄTSPRÜFUNGEN

Nr.	Prüfung	Beschreibung
1.	Gegenseitige Authentisierung	Prüfen, dass gegenseitige Authentisierung zwischen der Fahrzeugeinheit und der Kontrollgerätkarte normal abläuft
2.	Lese-/Schreib-Prüfungen	Ausführung eines typischen Tätigkeitsszenarios an der Fahrzeugeinheit. Dabei sind in Abhängigkeit von der zu prüfenden Karte so viele Schreibvorgänge wie bei der Karte möglich zu Ereignissen und Störungen durchzuführen Durch Herunterladen von der Karte ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß erfolgt sind Mit Hilfe eines Tagesausdrucks der Karte ist nachzuprüfen, ob die entsprechenden Aufzeichnungen ordnungsgemäß gelesen werden können

Anlage 10

ALLGEMEINE SICHERHEITSANFORDERUNGEN

In dieser Anlage werden die Mindestanforderungen und -inhalte für Weg- und/oder Geschwindigkeitsgeber, Fahrzeugeinheit und Sicherheitsanforderungen der Kontrollgerätkarten festgelegt.

Zur Formulierung der Sicherheitsanforderungen, die bei der Beantragung einer Sicherheitszertifizierung erfüllt werden müssen, sind die Hersteller aufgefordert, die Dokumente nach Bedarf zu konkretisieren und zu vervollständigen, ohne die hier angegebenen Spezifizierungen möglicher Sicherheitsgefährdungen sowie der Ziele, Verfahrensmöglichkeiten und sicherheitserzwingenden Funktionen zu ändern bzw. zu streichen.

INHALTSVERZEICHNIS

Allgemeine Sicherheitsanforderungen für Weg- und/oder Geschwindigkeitsgeber

1.	Einleitung	204
2.	Abkürzungen, Begriffsbestimmungen und Referenzdokumente	204
2.1.	Abkürzungen	204
2.2.	Begriffsbestimmungen	204
2.3.	Referenzdokumente	204
3.	Grundprinzip des Produkts	205
3.1.	Beschreibung und Verwendung des Weg- und/oder Geschwindigkeitsgebers	205
3.2.	Lebenszyklus des Weg- und/oder Geschwindigkeitgebers	206
3.3.	Sicherheitsgefährdungen	206
3.3.1.	Sicherheitsgefährdungen im Zusammenhang mit der Zugriffskontrolle	206
3.3.2.	Konstruktionsbedingte Sicherheitsgefährdungen	207
3.3.3.	Betriebsbedingte Sicherheitsgefährdungen	207
3.4.	Sicherheitsziele	207
3.5.	Informationstechnische Sicherheitsziele	207
3.6.	Physische, personelle bzw. verfahrenstechnische Mittel	208
3.6.1.	Gerätekonstruktion	208
3.6.2.	Auslieferung der Geräte	208
3.6.3.	Generierung und Lieferung der Sicherheitsdaten	208
3.6.4.	Einbau, Kalibrierung und Nachprüfung des Kontrollgerätes	208
3.6.5.	Kontrolle der Einhaltung von Vorschriften	208
3.6.6.	Software-Upgrades	208
4.	Sicherheitserzwingende Funktionen	208
4.1.	Identifizierung und Authentisierung	208
4.2.	Zugriffskontrolle	209
4.2.1.	Zugriffsberechtigung	209
4.2.2.	Datenzugriffsrechte	209
4.2.3.	Dateistruktur und -zugriffsbedingungen	209
4.3.	Zuordnungsmöglichkeit	209

4.4.	Audit	210
4.5.	Genauigkeit	210
4.5.1.	Maßnahmen zur Kontrolle des Informationsflusses	210
4.5.2.	Interne Datenübertragung	210
4.5.3.	Integrität der Speicherdaten	210
4.6.	Zuverlässigkeit während des Betriebes	210
4.6.1.	Prüfungen	210
4.6.2.	Software	211
4.6.3.	Physischer Schutz	211
4.6.4.	Unterbrechung der Stromversorgung	211
4.6.5.	Rücksetzbedingungen	211
4.6.6.	Datenbereitstellung	211
4.6.7.	Multifunktionsgeräte	211
4.7.	Datenaustausch	211
4.8.	Kryptografische Unterstützung	211
5.	Beschreibung der Sicherheitsmechanismen	212
6.	Mindestrobustheit der Sicherheitsmechanismen	212
7.	Gewährleistungsebene	212
8.	Grundlegendes Prinzip	212

Allgemeine Sicherheitsanforderungen für die Fahrzeugeinheit (FE)

1.	Einführung	214
2.	Abkürzungen, Begriffsbestimmungen und Referenzdokumente	214
2.1.	Abkürzungen	214
2.2.	Begriffsbestimmungen	214
2.3.	Referenzdokumente	214
3.	Grundprinzip des Produkts	214
3.1.	Beschreibung und Verwendung der Fahrzeugeinheit	214
3.2.	Lebenszyklus der Fahrzeugeinheit	216
3.3.	Sicherheitsgefährdungen	216
3.3.1.	Sicherheitsgefährdungen im Zusammenhang mit Identifizierung und Zugangskontrolle	216
3.3.2.	Konstruktionsbedingte Sicherheitsgefährdungen	217
3.3.3.	Betriebsbedingte Sicherheitsgefährdungen	217
3.4.	Sicherheitsziele	217
3.5.	Informationstechnische Sicherheitsziele	218
3.6.	Physische, personelle bzw. verfahrenstechnische Mittel	218
3.6.1.	Gerätekonstruktion	218
3.6.2.	Auslieferung und Aktivierung der Geräte	218

3.6.3. Generierung und Lieferung der Sicherheitsdaten	218
3.6.4. Kartenübergabe	219
3.6.5. Einbau, Kalibrierung und Nachprüfung des Kontrollgerätes	219
3.6.6. Betrieb der Geräte	219
3.6.7. Kontrolle der Einhaltung von Vorschriften	219
3.6.8. Software-Upgrades	219
4. Sicherheitserzwingende Funktionen	219
4.1. Identifizierung und Authentisierung	219
4.1.1. Identifizierung und Authentisierung des Weg- und/oder Geschwindigkeitsgebers	219
4.1.2. Identifizierung und Authentisierung des Benutzers	220
4.1.3. Identifizierung und Authentisierung eines entfernt angeschlossenen Unternehmens	221
4.1.4. Identifizierung und Authentisierung des Verwaltungsgeräts	221
4.2. Zugriffskontrolle	221
4.2.1. Zugriffsberechtigung	221
4.2.2. Funktionszugriffrechte	221
4.2.3. Datenzugriffsrechte	221
4.2.4. Dateistruktur und -zugriffsbedingungen	222
4.3. Zuordnungsmöglichkeit	222
4.4. Audit	222
4.5. Wiederverwendung von Speichermedien	223
4.6. Genauigkeit	223
4.6.1. Maßnahmen zur Kontrolle des Informationsflusses	223
4.6.2. Interne Datenübertragung	223
4.6.3. Integrität der Speicherdaten	223
4.7. Zuverlässigkeit während des Betriebs	223
4.7.1. Prüfungen	223
4.7.2. Software	224
4.7.3. Physischer Schutz	224
4.7.4. Unterbrechung der Stromversorgung	224
4.7.5. Rücksetzbedingungen	224
4.7.6. Datenbereitstellung	224
4.7.7. Multifunktionsgeräte	224
4.8. Datenaustausch	224
4.8.1. Datenaustausch mit dem Weg- und/oder Geschwindigkeitsgeber	224
4.8.2. Datenaustausch mit Kontrollgerätarten	225
4.8.3. Datenaustausch mit externen Datenträgern (Übertragungsfunktion)	225
4.9. Kryptografische Unterstützung	225

5.	Beschreibung der Sicherheitsmechanismen	225
6.	Mindestrobustheit der Sicherheitsmechanismen	225
7.	Gewährleistungsebene	225
8.	Grundlegendes Prinzip	226

Allgemeine Sicherheitsanforderungen für die Kontrollgerätkarte

1.	Einführung	230
2.	Abkürzungen, Begriffsbestimmungen und Referenzdokumente	230
2.1.	Abkürzungen	230
2.2.	Begriffsbestimmungen	231
2.3.	Referenzdokumente	231
3.	Grundprinzip des Produkts	231
3.1.	Beschreibung und Verwendung der Kontrollgerätkarte	231
3.2.	Lebenszyklus der Kontrollgerätkarte	231
3.3.	Sicherheitsgefährdungen	232
3.3.1.	Letztliche Ziele	232
3.3.2.	Angriffswege	232
3.4.	Sicherheitsziele	232
3.5.	Informationstechnische Sicherheitsziele	232
3.6.	Physische, personelle bzw. verfahrenstechnische Mittel	232
4.	Sicherheitserzwingende Funktionen	233
4.1.	Einhaltung von Schutzprofilen	233
4.2.	Identifizierung und Authentisierung des Benutzers	233
4.2.1.	Identifizierung des Benutzers	233
4.2.2.	Autentisierung des Benutzers	233
4.2.3.	Fehlgeschlagene Authentisierungen	233
4.3.	Zugriffskontrolle	234
4.3.1.	Zugriffskontrollregeln	234
4.3.2.	Zugriffskontrollfunktionen	234
4.4.	Zuordnungsmöglichkeit	234
4.5.	Audit	234
4.6.	Genauigkeit	234
4.6.1.	Speicherdatenintegrität	234
4.6.2.	Basisdatenauthentisierung	234
4.7.	Zuverlässigkeit während des Betriebs	235
4.7.1.	Prüfungen	235
4.7.2.	Software	235
4.7.3.	Stromversorgung	235

4.7.4. Rücksetzbedingungen	235
4.8. Datenaustausch	235
4.8.1. Datenaustausch mit einer Fahrzeugeinheit	235
4.8.2. Export von Daten an eine Nicht-Fahrzeugeinheit (Übertragungsfunktion)	235
4.9. Kryptografische Unterstützung	235
5. Beschreibung der Sicherheitsmechanismen	235
6. Mindestrobustheit der Sicherheitsmechanismen	236
7. Gewährleistungsebene	236
8. Grundlegendes Prinzip	236

ALLGEMEINE SICHERHEITSANFORDERUNGEN FÜR WEG- UND/ODER GESCHWINDIGKEITSGEBER

1. Einleitung

In diesem Abschnitt werden der Weg- und/oder Geschwindigkeitsgeber, mögliche Sicherheitsgefährdungen sowie die zu erfüllenden Sicherheitsziele beschrieben. Außerdem enthält er Erläuterungen zu den zur Durchsetzung der Sicherheitsanforderungen erforderlichen Funktionen, und es erfolgt eine Auflistung der Mindestanforderungen an die Sicherheitsmechanismen und die erforderliche Gewährleistungsebene für Entwicklung und Evaluierung.

Die hier aufgeführten Anforderungen entsprechen den Anforderungen im Hauptteil von Anhang I B. Im Interesse einer besseren Verständlichkeit können sich zwischen den Anforderungen im Hauptteil von Anhang I B und den Sicherheitsanforderungen Doppelungen ergeben. Bei Diskrepanzen zwischen einer Sicherheitsanforderung und der Anforderung im Hauptteil von Anhang I B, auf die sich diese Sicherheitsanforderung bezieht, geht die Anforderung im Hauptteil von Anhang I B vor.

Anforderungen im Hauptteil von Anhang I B, auf die sich diese Sicherheitsanforderungen nicht beziehen, sind nicht Gegenstand der Funktionen zur Durchsetzung von Sicherheitsanforderungen.

Zwecks besserer Zuordnung zu den in der Dokumentation über Entwicklung und Evaluierung verwendeten Begriffen wurden für die möglichen Sicherheitsgefährdungen sowie die zu erfüllenden Ziele, Verfahrensmöglichkeiten und SEF-Spezifikationen eindeutige Bezeichnungen gewählt.

2. Abkürzungen, Begriffsbestimmungen und Referenzdokumente**2.1. Abkürzungen**

ROM Festspeicher (Read Only Memory)

SEF Sicherheitserzwingende Funktion

PO Prüfobjekt

FE Fahrzeugeinheit (Vehicle Unit)

2.2. Begriffsbestimmungen

Digitaler Fahrtenschreiber Kontrollgerät

Geräteeinheit Ein an den Weg- und/oder Geschwindigkeitsgeber angeschlossenes Gerät

Weg- und Geschwindigkeitsdaten Die mit der FE ausgetauschten Daten über Fahrgeschwindigkeit und zurückgelegte Wegstrecke

Physisch getrennte Teile Komponenten des Weg- und/oder Geschwindigkeitsgebers, die sich im Gegensatz zu den im Gehäuse des Weg- und/oder Geschwindigkeitsgebers untergebrachten Bauteilen an anderer Stelle im Fahrzeug befinden

Sicherheitsdaten Spezielle Daten, die zur Unterstützung der sicherheitserzwingenden Funktionen erforderlich sind (z. B. kryptografische Schlüssel)

System Gerätetechnik, Menschen bzw. Organisationen, die in welcher Weise auch immer mit den Kontrollgeräten in Beziehung stehen

Benutzer Den Weg- und/oder Geschwindigkeitsgeber anwendende Person

Benutzerdaten Abgesehen von den Weg- und Geschwindigkeits- sowie den Sicherheitsdaten alle sonstigen Daten, die vom Weg- und/oder Geschwindigkeitsgeber aufgezeichnet bzw. gespeichert werden

2.3. Referenzdokumente

ITSEC ITSEC Information Technology Security Evaluation Criteria 1991 (Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik)

3. Grundprinzip des Produkts

3.1. Beschreibung und Verwendung des Weg- und/oder Geschwindigkeitsgebers

Der Weg- und/oder Geschwindigkeitsgeber ist zum Einbau in Straßentransportfahrzeuge vorgesehen. Seine Aufgabe ist es, der FE gesicherte Daten im Hinblick auf die Fahrzeuggeschwindigkeit und die zurückgelegte Wegstrecke zur Verfügung zu stellen.

Der Weg- und/oder Geschwindigkeitsgeber ist mit einem bewegten Fahrzeugteil, dessen Bewegung für die Fahrtgeschwindigkeit bzw. die zurückgelegte Wegstrecke stellvertretend ist, mechanisch verbunden. Er kann im Getriebe oder in einem anderen Teil des Fahrzeugs installiert werden.

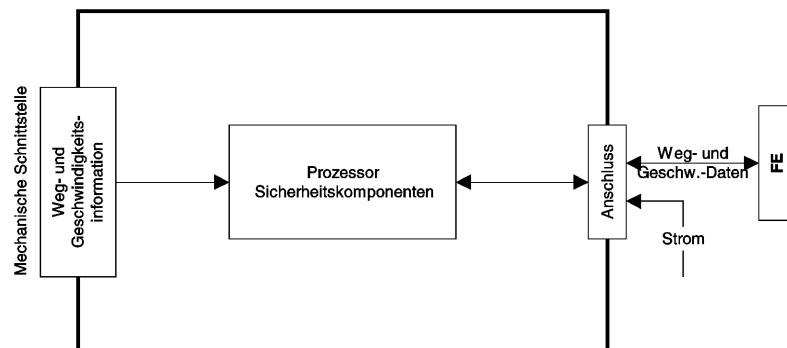
Im Betriebszustand ist der Weg- und/oder Geschwindigkeitsgeber an eine FE angeschlossen.

Ebenso ließe er sich zu Verwaltungszwecken an spezielle Geräte anschließen (durch den Hersteller festzulegen).

Der typische Weg- und/oder Geschwindigkeitsgeber ist in der folgenden Abbildung dargestellt:

Abbildung 1

Typischer Weg- und/oder Geschwindigkeitsgeber

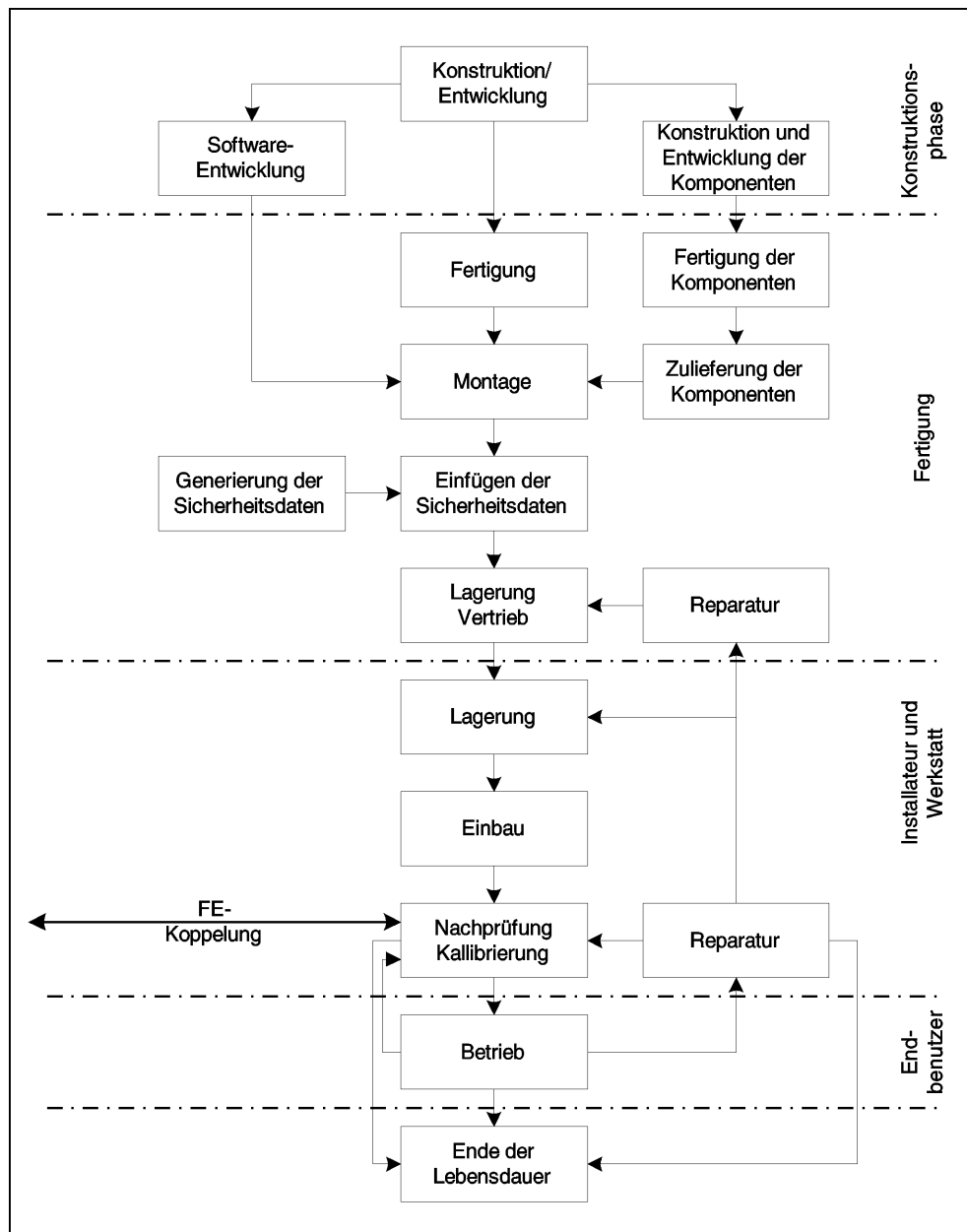


3.2. Lebenszyklus des Weg- und/oder Geschwindigkeitsgebers

Der typische Lebenszyklus des Weg- und/oder Geschwindigkeitsgebers ist in der folgenden Abbildung dargestellt:

Abbildung 2

Typischer Lebenszyklus des Weg- und/oder Geschwindigkeitsgebers



3.3. Sicherheitsgefährdungen

In diesem Abschnitt werden mögliche Sicherheitsgefährdungen des Weg- und/oder Geschwindigkeitsgebers beschrieben.

3.3.1. Sicherheitsgefährdungen im Zusammenhang mit der Zugriffskontrolle

T.Access

Versuch seitens der Benutzer, Zugriff auf ihnen nicht erlaubte Funktionen zu erlangen

3.3.2. Konstruktionsbedingte Sicherheitsgefährdungen

T.Faults	Fehler bei Hardware, Software oder Kommunikationsverfahren können den Weg- und/oder Geschwindigkeitsgeber in einen unvorhergesehenen Zustand versetzen, der seine Sicherheit beeinträchtigt
T.Tests	Die Nutzung nicht validierter Prüfmodi bzw. vorhandener ‚Hintertüren‘ kann die Sicherheit des Weg- und/oder Geschwindigkeitsgebers beeinträchtigen
T.Design	Versuch seitens der Benutzer, auf illegale Weise Kenntnis über Konstruktionsdaten zu erlangen, sei es aus Unterlagen des Herstellers (durch Diebstahl, Bestechung usw.) oder durch Methoden des Reverse Engineering

3.3.3. Betriebsbedingte Sicherheitsgefährdungen

T.Environment	Gefährdung der Sicherheit des Weg- und/oder Geschwindigkeitsgebers durch (thermische, elektromagnetische, optische, chemische, mechanische usw.) Einwirkung von außen
T.Hardware	Versuch seitens der Benutzer, Änderungen an der Weg- und/oder Geschwindigkeitsgeberhardware vorzunehmen
T.Mechanical_Origin	Versuch seitens der Benutzer, die Eingabe des Weg- und/oder Geschwindigkeitsgebers zu manipulieren (z. B. durch Abschrauben vom Getriebe usw.)
T.Motion_Data	Versuch seitens der Benutzer, die Weg- und Geschwindigkeitsdaten des Fahrzeugs zu verfälschen (durch Signaladdition, -modifizierung, -löschung, -wiederholung)
T.Power_Supply	Versuch seitens der Benutzer, Sicherheitsziele des Weg- und/oder Geschwindigkeitsgebers durch Manipulation der Stromversorgung (Leitungstrennung, Spannungserhöhung bzw. -reduzierung) zu untergraben
T.Security_Data	Versuch seitens der Benutzer, auf illegale Weise Kenntnis über Sicherheitsdaten während deren Generierung, Übertragung bzw. Speicherung im Gerät zu erlangen
T.Software	Versuch seitens der Benutzer, Änderungen an der Software des Weg- und/oder Geschwindigkeitsgebers vorzunehmen
T.Stored_Data	Versuch seitens der Benutzer, gespeicherte Daten (Sicherheits- bzw. Benutzerdaten) zu verfälschen

3.4. Sicherheitsziele

Das wichtigste Sicherheitsziel des digitalen Fahrtenschreibersystems ist folgendes:

O.Main	Die von den Kontrollbehörden zu prüfenden Daten müssen verfügbar sein und die Handlungen der kontrollierten Fahrer und Fahrzeuge hinsichtlich Lenk-, Arbeits-, Bereitschafts- und Ruhezeiten sowie Fahrzeuggeschwindigkeit vollständig und genau widerspiegeln
--------	--

Das zum globalen Sicherheitsziel beitragende Sicherheitsziel des Weg- und/oder Geschwindigkeitsgebers ist somit folgendes:

O.Sensor_Main	Die vom Weg- und/oder Geschwindigkeitsgeber übermittelten Daten müssen der FE so bereitgestellt werden, dass die FE die Bewegung des Fahrzeugs in Bezug auf Geschwindigkeit und zurückgelegte Wegstrecke vollständig und genau feststellen kann
---------------	---

3.5. Informationstechnische Sicherheitsziele

Die speziellen, zum Hauptsicherheitsziel beitragenden IT-Sicherheitsziele des Weg- und/oder Geschwindigkeitsgebers sind folgende:

O.Access	Der Weg- und/oder Geschwindigkeitsgeber muss den Zugriff der angeschlossenen Geräteeinheiten auf Funktionen und Daten steuern
O.Audit	Der Weg- und/oder Geschwindigkeitsgeber muss Versuche zur Umgehung seiner Sicherheitsfunktionen prüfen und zu den angeschlossenen Geräteeinheiten zurückverfolgen
O.Authentication	Der Weg- und/oder Geschwindigkeitsgeber muss angeschlossene Geräteeinheiten authentifizieren

O.Processing	Der Weg- und/oder Geschwindigkeitsgeber stellt sicher, dass die Eingabedaten, aus denen sich die Weg- und Geschwindigkeitsdaten ableiten, exakt verarbeitet werden
O.Reliability	Der Weg- und/oder Geschwindigkeitsgeber muss zuverlässig arbeiten
O.Secured_Data_Exchange	Der Weg- und/oder Geschwindigkeitsgeber muss den sicheren Datenaustausch mit der FE gewährleisten

3.6. **Physische, personelle bzw. verfahrenstechnische Mittel**

In diesem Abschnitt werden die physischen, personellen bzw. verfahrenstechnischen Anforderungen, die zur Sicherheit des Weg- und/oder Geschwindigkeitsgebers beitragen, beschrieben.

3.6.1. *Gerätekonstruktion*

M.Development	Die Entwickler des Weg- und/oder Geschwindigkeitsgebers müssen sicherstellen, dass die Zuweisung von Verantwortlichkeiten während des Entwicklungszeitraums in einer die IT-Sicherheit wahren Weise erfolgt
M.Manufacturing	Die Hersteller des Weg- und/oder Geschwindigkeitsgebers müssen sicherstellen, dass die Zuweisung von Verantwortlichkeiten während des Herstellungsprozesses in einer die IT-Sicherheit wahren Weise erfolgt und dass der Weg- und/oder Geschwindigkeitsgeber in diesem Prozess vor physischen Angriffen, die die IT-Sicherheit beeinträchtigen könnten, geschützt wird

3.6.2. *Auslieferung der Geräte*

M.Delivery	Die Hersteller des Weg- und/oder Geschwindigkeitsgebers, die Fahrzeughersteller und die Installateure bzw. Werkstätten müssen beim Umgang mit dem Weg- und/oder Geschwindigkeitsgeber sicherstellen, dass die IT-Sicherheit gewahrt bleibt
------------	--

3.6.3. *Generierung und Lieferung der Sicherheitsdaten*

M.Sec_Data_Generation	Die Algorithmen zur Generierung von Sicherheitsdaten dürfen nur berechtigten und vertrauenswürdigen Personen zugänglich sein
M.Sec_Data_Transport	Die Sicherheitsdaten müssen in einer Weise generiert, transportiert und in den Weg- und/oder Geschwindigkeitsgeber eingebracht werden, die Vertraulichkeit und Integrität der Daten angemessen gewährleistet

3.6.4. *Einbau, Kalibrierung und Nachprüfung des Kontrollgeräts*

M.Approved_Workshops	Einbau, Kalibrierung und Reparatur des Kontrollgeräts dürfen nur durch vertrauenswürdige und zugelassene Installateure bzw. Werkstätten erfolgen
M.Mechanical_Interface	Es müssen Möglichkeiten geschaffen werden (z. B. durch Plombierung), um physische Manipulationen an der mechanischen Schnittstelle zu erkennen
M.Regular_Inspections	Die Kontrollgeräte müssen einer regelmäßigen Nachprüfung und Kalibrierung unterzogen werden

3.6.5. *Kontrolle der Einhaltung von Vorschriften*

M.Controls	Die Einhaltung der gesetzlichen Vorschriften ist regelmäßig und stichprobenartig zu kontrollieren, unter anderem durch Sicherheitsaudits
------------	--

3.6.6. *Software-Upgrades*

M.Software_Upgrade	Neue Softwareversionen dürfen erst nach Erhalt der Sicherheitszertifizierung im Weg- und/oder Geschwindigkeitsgeber implementiert werden
--------------------	--

4. **Sicherheitserzwingende Funktionen**

4.1. **Identifizierung und Authentisierung**

UIA_101	Der Weg- und/oder Geschwindigkeitsgeber muss in der Lage sein, für jede Interaktion die Identität der angeschlossenen Geräteeinheit festzustellen.
---------	--

UIA_102 Die Identität einer angeschlossenen Geräteeinheit setzt sich zusammen aus:

- einer Geräteeinheitsgruppe:
 - Fahrzeugeinheit (FE),
 - Verwaltungsgerät,
 - sonstige Einheit,
- einer Geräteeinheitskennung (nur FE).

UIA_103 Die Geräteeinheitskennung einer FE besteht aus der Bauartgenehmigungsnummer der FE und der Seriennummer der FE.

UIA_104 Der Weg- und/oder Geschwindigkeitsgeber ist in der Lage, die Authentisierung jeder angeschlossenen FE bzw. jedes angeschlossenen Verwaltungsgeräts

- bei Anschließen der Geräteeinheit,
 - bei Wiedereinschalten der Stromversorgung
- vorzunehmen.

UIA_105 Der Weg- und/oder Geschwindigkeitsgeber ist in der Lage, die Authentisierung der angeschlossene FE in bestimmten Abständen zu wiederholen.

UIA_106 Der Weg- und/oder Geschwindigkeitsgeber erkennt und verhindert den Gebrauch kopierter und wieder eingespielter Authentisierungsdaten.

UIA_107 Nach Erkennen einer (vom Hersteller noch festzulegenden, jedoch 20 nicht übersteigenden) Zahl von aufeinander folgenden erfolglosen Authentisierungsversuchen wird die SEF:

- ein Auditprotokoll über das Ereignis anlegen,
- eine Warnung an die Geräteeinheit ausgeben,
- die Ausgabe von Weg- und Geschwindigkeitsdaten im ungesicherten Modus fortsetzen.

4.2. Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass nur speziell dazu berechtigte Personen Informationen aus dem PO auslesen sowie im PO anlegen bzw. nach Änderung in das PO einlesen.

4.2.1. Zugriffsberechtigung

ACC_101 Der Weg- und/oder Geschwindigkeitsgeber kontrolliert die Zugriffsberechtigung auf Funktionen und Daten.

4.2.2. Datenzugriffsrechte

ACC_102 Der Weg- und/oder Geschwindigkeitsgeber stellt sicher, dass die Kenndaten nur ein einziges Mal in den Weg- und/oder Geschwindigkeitsgeber geschrieben werden können (Anforderung 078).

ACC_103 Der Weg- und/oder Geschwindigkeitsgeber darf nur von authentisierten Geräteeinheiten Benutzerdaten annehmen und/oder speichern.

ACC_104 Der Weg- und/oder Geschwindigkeitsgeber setzt geeignete Zugriffsrechte für das Lesen und Schreiben von Sicherheitsdaten durch.

4.2.3. Dateistruktur und -zugriffsbedingungen

ACC_105 Die Strukturen der Anwendungs- und Datendateien und die Zugriffsbedingungen auf diese Dateien werden bereits im Herstellungsprozess angelegt und gegen jegliche spätere Verfälschung bzw. Löschung gesperrt.

4.3. Zuordnungsmöglichkeit

ACT_101 Im Speicher des Weg- und/oder Geschwindigkeitsgebers werden die Kenndaten des Weg- und/oder Geschwindigkeitsgebers gespeichert gehalten (Anforderung 077).

ACT_102 Im Speicher des Weg- und/oder Geschwindigkeitsgebers werden die Installationsdaten abgespeichert (Anforderung 099).

ACT_103 Der Weg- und/oder Geschwindigkeitsgeber ist in der Lage, Zuordnungsdaten auf Verlangen an authentifizierte Geräteeinheiten auszugeben.

4.4. **Audit**

AUD_101 Der Weg- und/oder Geschwindigkeitsgeber legt bei Ereignissen, die seine Sicherheit beeinträchtigen, Auditprotokolle für die betreffenden Ereignisse an.

AUD_102 Folgende Ereignisse beeinträchtigen die Sicherheit des Weg- und/oder Geschwindigkeitsgebers:

- Sicherheitsverletzende Versuche:
 - fehlgeschlagene Authentisierung,
 - Integritätsfehler der Speicherdaten,
 - interner Datenübertragungsfehler,
 - unberechtigtes Öffnen des Gehäuses,
 - Hardwaremanipulation.
- Störung des Gebers.

AUD_103 Die Auditprotokolle enthalten folgende Angaben:

- Datum und Uhrzeit des Ereignisses,
- Art des Ereignisses,
- Identität der angeschlossenen Geräteeinheit.

Stehen die geforderten Daten nicht zur Verfügung, wird ein entsprechender Fehlvermerk ausgegeben (vom Hersteller noch festzulegen).

AUD_104 Der Weg- und/oder Geschwindigkeitsgeber überträgt die angefertigten Auditprotokolle zum Zeitpunkt ihrer Generierung an die FE, und kann sie zugleich in seinem Speicher ablegen.

AUD_105 Für den Fall, dass der Weg- und/oder Geschwindigkeitsgeber Auditprotokolle speichert, muss sichergestellt sein, dass unabhängig von der anderweitigen Speicherbelegung 20 Auditprotokolle gespeichert und diese gespeicherten Auditprotokolle auf Anfrage an authentifizierte Geräteeinheiten ausgegeben werden können.

4.5. **Genauigkeit**

4.5.1. *Maßnahmen zur Kontrolle des Informationsflusses*

ACR_101 Der Weg- und/oder Geschwindigkeitsgeber stellt sicher, dass nur vom mechanischen Gebereingang stammende Weg- und Geschwindigkeitsdaten angenommen und verarbeitet werden.

4.5.2. *Interne Datenübertragung*

Die Anforderungen dieses Absatzes gelten nur, wenn der Weg- und/oder Geschwindigkeitsgeber physisch getrennte Teile nutzt.

ACR_102 Werden Daten zwischen physisch getrennten Teilen des Weg- und/oder Geschwindigkeitsgebers übertragen, müssen diese Daten gegen Verfälschungen geschützt werden.

ACR_103 Bei Erkennen eines Datenübertragungsfehlers im Verlauf einer internen Datenübertragung wird die Übertragung wiederholt und zu dem Ereignis durch die SEF ein Auditprotokoll angelegt.

4.5.3. *Integrität der Speicherdaten*

ACR_104 Der Weg- und/oder Geschwindigkeitsgeber prüft die in seinem Speicher abgelegten Benutzerdaten auf Integritätsfehler.

ACR_105 Bei Erkennen eines Integritätsfehlers der Benutzerdaten generiert die SEF ein Auditprotokoll.

4.6. **Zuverlässigkeit während des Betriebs**

4.6.1. *Prüfungen*

RLB_101 Sämtliche speziell für den Prüfbedarf während der Herstellungsphase erforderlichen Befehle, Handlungen bzw. Prüfpunkte werden vor Abschluss der Herstellungsphase deaktiviert oder entfernt. Es darf nicht möglich sein, sie zum späteren Gebrauch wiederherzustellen.

RLB_102 Der Weg- und/oder Geschwindigkeitsgeber führt zur Funktionsprüfung beim ersten Einschalten sowie während des üblichen Betriebs Selbsttests durch. Die Selbsttests des Weg- und/oder Geschwindigkeitsgebers beinhalten eine Integritätsprüfung der Sicherheitsdaten sowie eine Integritätsprüfung des gespeicherten Ausführungscode (sofern dieser nicht im ROM gespeichert ist).

RLB_103 Bei Erkennen einer internen Fehlfunktion während der Selbstprüfung erstellt die SEF ein Auditprotokoll (Geberstörung).

4.6.2. Software

RLB_104 Es darf keine Möglichkeit gegeben sein, die Weg- und/oder Geschwindigkeitsgebersoftware bei der Praxisanwendung zu analysieren bzw. auszutesten.

RLB_105 Eingaben aus externen Quellen dürfen als Ausführungscode nicht akzeptiert werden.

4.6.3. Physischer Schutz

RLB_106 Falls die Konstruktionsweise des Weg- und/oder Geschwindigkeitsgebers ein Öffnen des Gehäuses erlaubt, muss der Weg- und/oder Geschwindigkeitsgeber jedes Öffnen des Gehäuses feststellen, selbst wenn die externe Stromversorgung bis zu 6 Monate unterbrochen ist. Die SEF legt in diesem Fall ein Auditprotokoll über das Ereignis an (hierbei ist zulässig, dass das Auditprotokoll erst nach Wiedereinschalten der Stromversorgung erstellt und gespeichert wird).

Ist der Weg- und/oder Geschwindigkeitsgeber so konstruiert, dass er nicht geöffnet werden kann, muss seine Bauweise dennoch jeden Versuch der physischen Manipulation leicht erkennen lassen (z. B. durch Sichtprüfung).

RLB_107 Der Weg- und/oder Geschwindigkeitsgeber muss bestimmte (vom Hersteller noch festzulegende) Formen der Hardwaremanipulation erkennen.

RLB_108 In vorgenannten Fall erstellt die SEF ein Auditprotokoll und wird der Weg- und/oder Geschwindigkeitsgeber ... (vom Hersteller noch festzulegen).

4.6.4. Unterbrechung der Stromversorgung

RLB_109 Der Weg- und/oder Geschwindigkeitsgeber behält bei Stromunterbrechungen bzw. -schwankungen seinen gesicherten Status bei.

4.6.5. Rücksetzbedingungen

RLB_110 Bei einer Unterbrechung der Stromversorgung, beim Abbruch einer Transaktion vor deren Vollendung bzw. bei Vorliegen jeder sonstigen Rücksetzbedingung muss der Weg- und/oder Geschwindigkeitsgeber sauber zurückgesetzt werden.

4.6.6. Datenbereitstellung

RLB_111 Der Weg- und/oder Geschwindigkeitsgeber stellt sicher, dass auf den Datenbestand bei Bedarf zugegriffen werden kann und dass die Daten weder unnötig abgerufen noch zurückgehalten werden.

4.6.7. Multifunktionsgeräte

RLB_112 Falls der Weg- und/oder Geschwindigkeitsgeber neben der Kontrollgerätfunktion noch weitere Anwendungen bietet, müssen alle diese Anwendungen physisch und/oder logisch voneinander getrennt sein. Jede dieser Anwendungen muss auf eigene Sicherheitsdaten zurückgreifen, und es darf immer nur eine Funktion aktiv sein.

4.7. Datenaustausch

DEX_101 Der Weg- und/oder Geschwindigkeitsgeber überträgt die Weg- und Geschwindigkeitsdaten mit den zugehörigen Sicherheitsattributen an die FE, so dass die FE in die Lage versetzt wird, die Integrität und Authentizität der Daten festzustellen.

4.8. Kryptographische Unterstützung

Je nach Sicherheitsmechanismus und vom Hersteller gewählten Lösungen gelten die Anforderungen dieses Absatzes nur soweit erforderlich.

CSP_101 Jede vom Weg- und/oder Geschwindigkeitsgeber durchgeführte kryptografische Operation entspricht einem genau festgelegten Algorithmus und einer genau festgelegten Schlüsselgröße.

CSP_102 Falls der Weg- und/oder Geschwindigkeitsgeber kryptografische Schlüssel generiert, müssen diese genau festgelegten Schlüsselgenerierungsalgorithmen und genau festgelegten Schlüsselgrößen entsprechen.

CSP_103 Falls der Weg- und/oder Geschwindigkeitsgeber kryptografische Schlüssel vergibt, muss dies nach genau festgelegten Schlüsselvergabemethoden erfolgen.

CSP_104 Falls der Weg- und/oder Geschwindigkeitsgeber auf kryptografische Schlüssel zugreift, muss dies nach genau festgelegten Schlüsselzugriffsmethoden erfolgen.

CSP_105 Falls der Weg- und/oder Geschwindigkeitsgeber kryptografische Schlüssel vernichtet, muss dies nach genau festgelegten Schlüsselvernichtungsmethoden erfolgen.

5. Beschreibung der Sicherheitsmechanismen

Die der Erfüllung der sicherheitserzwingenden Funktionen des Weg- und/oder Geschwindigkeitsgebers dienenden Sicherheitsmechanismen werden durch die Hersteller des Weg- und/oder Geschwindigkeitsgebers bestimmt.

6. Mindestrobustheit der Sicherheitsmechanismen

Die Mindestrobustheit der Sicherheitsmechanismen des Weg- und/oder Geschwindigkeitsgebers ist Hoch, gemäß Definition in ITSEC.

7. Gewährleistungsebene

Die für den Weg- und/oder Geschwindigkeitsgeber vorgegebene Gewährleistungsebene ist die ITSEC-Ebene E3, gemäß Definition in ITSEC.

8. Grundlegendes Prinzip

Mit der folgenden Matrix wird das Prinzip der SEF begründet. Hierzu wird verdeutlicht:

- welche SEF bzw. Mittel welchen Sicherheitsgefährdungen entgegenwirken,
- welche SEF welche IT-Sicherheitsziele erfüllen.

	Sicherheitsgefährdungen												IT-Zielsetzungen					
	Zugriff	Fehler/Störungen	Prüfungen	Konstruktion	Umfeld	Hardware	Mechanischer Ursprung	Daten Weg und Geschwindigkeit	Stromversorgung	Sicherheitsdaten	Software	Speicherdaten	Zugriff	Audit	Authentisierung	Datenverarbeitung	Gewährleistung	Gesicherter Datenaustausch
Physische, personelle, verfahrenstechnische Mittel																		
Entwicklung		x	x	x														
Herstellung			x	x														
Auslieferung						x					x	x						
Generierung von Sicherheitsdaten										x								
Transport von Sicherheitsdaten										x								
Zugelassene Werkstätten							x											
Mechanische Schnittstelle							x											
Regelmäßige Nachprüfung						x	x		x		x							
Durchsetzung gesetzl. Vorschriften					x	x	x		x	x	x							
Software-Upgrades											x							
Sicherheitserzwingende Funktionen																		
Kennung und Authentisierung																		
UIA_101 Geräteidentifizierung	x							x					x		x			x
UIA_102 Gerätekenndaten	x												x		x			
UIA_103 FE-Kenndaten														x				
UIA_104 Geräteauthentisierung	x							x					x		x			x
UIA_105 Neuauthentisierung	x							x					x		x			x
UIA_106 Fälschungssichere Authentisierung	x							x					x		x			
UIA_107 Authentisierungsfehler								x						x			x	
Zugriffskontrolle																		
ACC_101 Zugriffskontrollregeln	x									x		x	x					
ACC_102 Weg- und/oder Geschwindigkeitsgeber-Kennung												x	x					

[illegible]

ALLGEMEINE SICHERHEITSANFORDERUNGEN FÜR DIE FAHRZEUGEINHEIT (FE)

1. Einführung

In diesem Abschnitt werden die Fahrzeugeinheit, mögliche Sicherheitsgefährdungen sowie die zu erfüllenden Sicherheitsziele beschrieben. Außerdem enthält er Erläuterungen zu den zur Durchsetzung der Sicherheitsanforderungen erforderlichen Funktionen, und es erfolgt eine Auflistung der Mindestanforderungen an die Sicherheitsmechanismen und die erforderliche Gewährleistungsebene für Entwicklung und Evaluierung.

Die hier aufgeführten Anforderungen entsprechen den Anforderungen im Hauptteil von Anhang I B. Im Interesse einer besseren Verständlichkeit können sich Doppelungen zwischen den Anforderungen im Hauptteil von Anhang I B und den Sicherheitsanforderungen ergeben. Bei Diskrepanzen zwischen einer Sicherheitsanforderung und der Anforderung im Hauptteil von Anhang I B, auf die sich diese Sicherheitsanforderung bezieht, geht die Anforderung im Hauptteil von Anhang I B vor.

Anforderungen im Hauptteil von Anhang I B, auf die sich diese Sicherheitsanforderungen nicht beziehen, sind nicht Gegenstand der Funktionen zur Durchsetzung von Sicherheitsanforderungen.

Zwecks besserer Zuordnung zu den in der Dokumentation über Entwicklung und Evaluierung verwendeten Begriffen wurden für die Sicherheitsgefährdungen, die Ziele, Verfahrensmöglichkeiten und SEF-Spezifikationen eindeutige Bezeichnungen gewählt.

2. Abkürzungen, Begriffsbestimmungen und Referenzdokumente**2.1. Abkürzungen**

PIN	Persönliche Geheimzahl
ROM	Festspeicher (Read Only Memory)
SEF	Sicherheitserzwingende Funktion
PO	Prüfobjekt
FE	Fahrzeugeinheit (Vehicle Unit)

2.2. Begriffsbestimmungen

Digitaler Fahrtenschreiber	Kontrollgerät
Weg- und Geschwindigkeitsdaten	Die mit dem Weg- und/oder Geschwindigkeitsgeber ausgetauschten Daten über Fahr- geschwindigkeit und zurückgelegte Wegstrecke
Physisch getrennte Teile	Komponenten der FE, die sich im Gegensatz zu den im Gehäuse der FE untergebrach- ten Bauteilen an anderer Stelle im Fahrzeug befinden
Sicherheitsdaten	Spezielle Daten, die zur Unterstützung der sicherheitserzwingenden Funktionen erfor- derlich sind (z. B. kryptografische Schlüssel)
System	Gerätetechnik, Menschen bzw. Organisationen, die in welcher Weise auch immer mit den Kontrollgeräten in Beziehung stehen
Benutzer	Als Benutzer sind die Personen zu verstehen, die das Gerät anwenden. Die Benutzer einer FE sind in der Regel Fahrer, Kontrolleure, Werkstätten und Unternehmen
Benutzerdaten	Mit Ausnahme der Weg- und Geschwindigkeits- sowie Sicherheitsdaten, alle sons- tigen nach Kapitel III.12 erforderlichen Daten, die von der FE aufgezeichnet bzw. gespeichert werden

2.3. Referenzdokumente

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 (Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik)
-------	---

3. Grundprinzip des Produkts**3.1. Beschreibung und Verwendung der Fahrzeugeinheit**

Die FE ist zum Einbau in Straßentransportfahrzeuge vorgesehen. Ihre Aufgabe ist es, Daten über die Tätigkeit der Fahrer aufzuzeichnen, zu speichern, anzuzeigen, auszudrucken und auszugeben.

Sie ist an einen Weg- und/oder Geschwindigkeitsgeber angeschlossen, mit dem sie Daten über die Fahrzeugbewegung austauscht.

Die Benutzer identifizieren sich gegenüber der FE durch Kontrollgerätkarten.

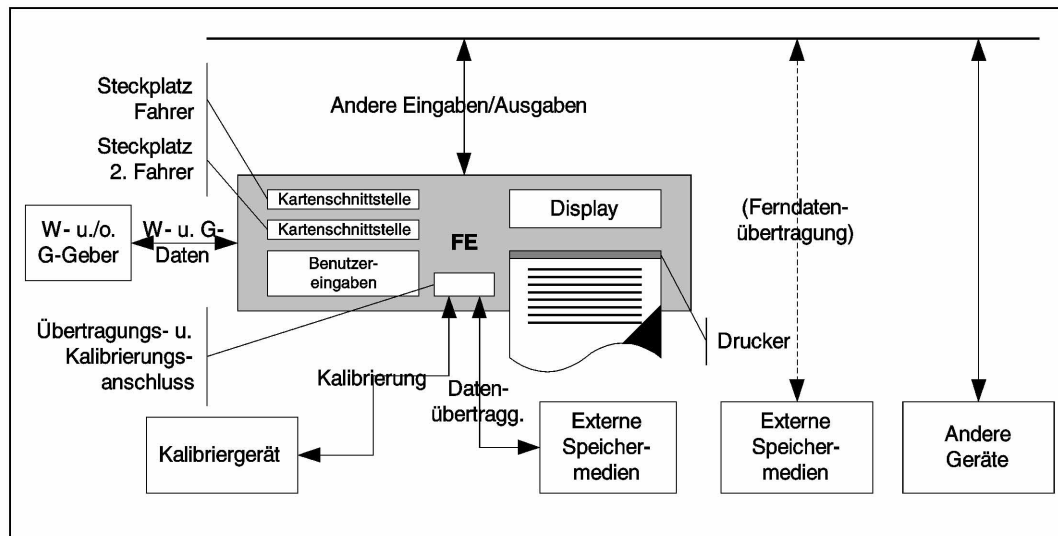
Die FE zeichnet die Tätigkeitsdaten der Benutzer auf und legt sie in seinem Massenspeicher ab. Die Benutzerdaten werden außerdem auf Kontrollgerätkarten aufgezeichnet.

Die FE gibt die Daten an Anzeigegerät, Drucker und externe Geräte aus.

Die Betriebsumgebung einer im Fahrzeug installierten Fahrzeugeinheit wird in der folgenden Abbildung beschrieben:

Abbildung 2

Betriebsumgebung der FE



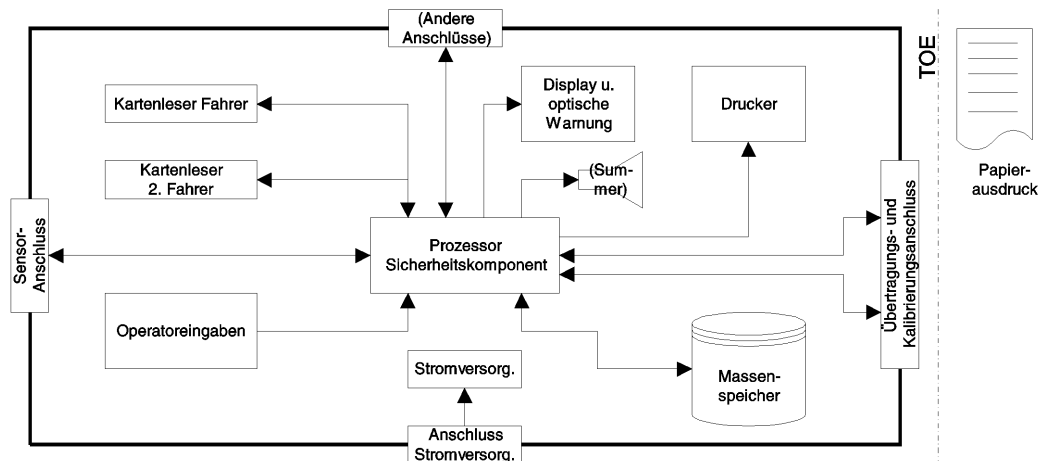
Allgemeine Merkmale, Funktionen und Betriebsarten der FE werden in Anhang I B, Kapitel II, beschrieben.

Die Funktionsanforderungen an die FE werden in Anhang I B, Kapitel III, beschrieben.

Eine typische FE ist in der folgenden Abbildung dargestellt:

Abbildung 3

Typische Fahrzeugeinheit (FE) (...) optional



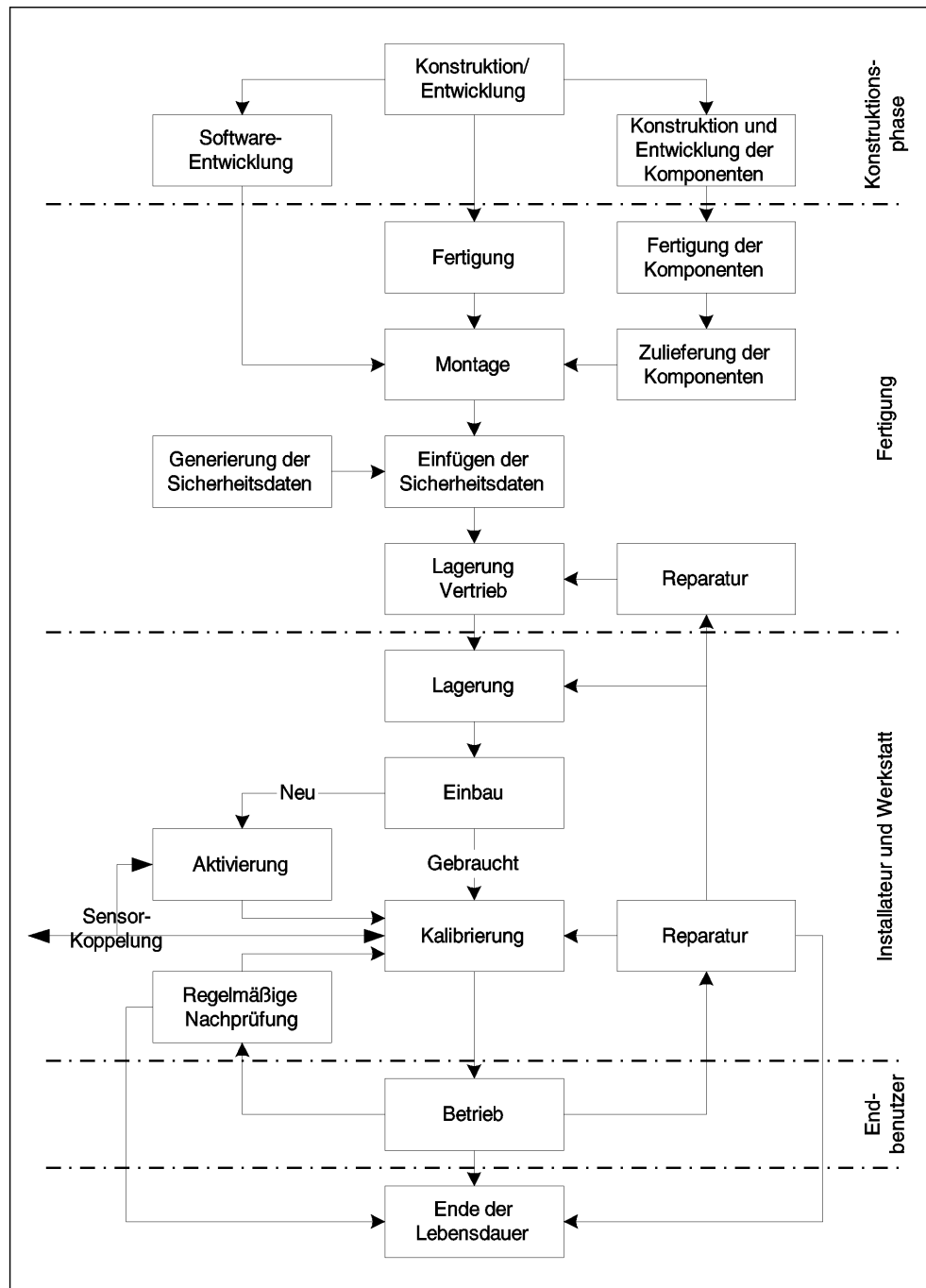
Zu beachten ist, dass zwar der Druckermechanismus ein Teil des PO ist, das einmal ausgedruckte Dokument jedoch nicht mehr.

3.2. Lebenszyklus der Fahrzeugeinheit

Der typische Lebenszyklus der FE ist in der folgenden Abbildung dargestellt:

Abbildung 4

Typischer Lebenszyklus der FE



3.3. Sicherheitsgefährdungen

In diesem Abschnitt werden mögliche Sicherheitsgefährdungen für die FE beschrieben.

3.3.1. Sicherheitsgefährdungen im Zusammenhang mit Identifizierung und Zugangskontrolle

T.Access Versuch seitens der Benutzer, Zugriff auf ihnen nicht erlaubte Funktionen zu erlangen (z. B. wenn Fahrer Zugriff auf die Kalibrierfunktion erlangen)

T.Identification Versuch seitens der Benutzer, sich mehrfach oder gar nicht zu identifizieren

3.3.2. Konstruktionsbedingte Sicherheitsgefährdungen

T.Faults	Fehler bei Hardware, Software oder Kommunikationsverfahren können die FE in einen unvorhergesehenen Zustand versetzen, der ihre Sicherheit beeinträchtigt
T.Tests	Die Nutzung nicht validierter Prüfmodi bzw. vorhandener ‚Hintertüren‘ kann die Sicherheit der FE beeinträchtigen
T.Design	Versuch seitens der Benutzer, auf illegale Weise Kenntnis über Konstruktionsdaten zu erlangen, sei es aus Unterlagen des Herstellers (durch Diebstahl, Bestechung usw.) oder durch Methoden des Reverse Engineering

3.3.3. Betriebsbedingte Sicherheitsgefährdungen

T.Calibration_Parameters	Versuch seitens der Benutzer, falsch kalibrierte Geräte zu verwenden (durch Änderung der Kalibrierungsdaten bzw. aufgrund organisatorischer Schwachpunkte)
T.Card_Data_Exchange	Versuch seitens der Benutzer, Daten während deren Austauschs zwischen FE und Kontrollgerätarten zu verfälschen (durch Signaladdition, -modifizierung, -löschung, -wiederholung)
T.Clock	Versuch seitens der Benutzer, die Systemuhr zu verstellen
T.Environment	Versuch seitens der Benutzer, die Sicherheit der FE durch äußere (thermische, elektromagnetische, optische, chemische, mechanische usw.) Einwirkungen zu durchbrechen
T.Fake_Devices	Versuch seitens der Benutzer, nachgebaute Geräte (Weg- und/oder Geschwindigkeitsgeber, Smartcards) an die FE anzuschließen
T.Hardware	Versuch seitens der Benutzer, Änderungen an der FE-Hardware vorzunehmen
T.Motion_Data	Versuch seitens der Benutzer, die Weg- und Geschwindigkeitsdaten des Fahrzeugs zu verfälschen (durch Signaladdition, -modifizierung, -löschung, -wiederholung)
T.Non_Activated	Verwendung nichtaktivierter Geräte durch Benutzer
T.Output_Data	Versuch seitens der Benutzer, die Datenausgabe zu manipulieren (Ausdruck, Anzeige bzw. Übertragung)
T.Power_Supply	Versuch seitens der Benutzer, Sicherheitsziele der FE durch Manipulation der Stromversorgung (Leitungstrennung, Spannungserhöhung bzw. -reduzierung) zu untergraben
T.Saturation	Versuch seitens der Benutzer, den Massenspeicher so zu erschöpfen (selbst durch legalen Gebrauch), dass bereits gespeicherte Daten gelöscht werden
T.Security_Data	Versuch seitens der Benutzer, auf illegale Weise Kenntnis über Sicherheitsdaten während deren Generierung, Übertragung bzw. Speicherung im Gerät zu erlangen
T.Software	Versuch seitens der Benutzer, Änderungen an der FE-Software vorzunehmen
T.Stored_Data	Versuch seitens der Benutzer, gespeicherte Daten (Sicherheits- bzw. Benutzerdaten) zu verfälschen

3.4. Sicherheitsziele

Das wichtigste Sicherheitsziel des digitalen Fahrtenschreibersystems ist Folgendes:

O.Main	Die von den Kontrollbehörden zu prüfenden Daten müssen verfügbar sein und die Handlungen der kontrollierten Fahrer und Fahrzeuge hinsichtlich Lenk-, Arbeits-, Bereitschafts- und Ruhezeiten sowie Fahrzeuggeschwindigkeit vollständig und genau widerspiegeln
--------	--

Das zum globalen Sicherheitsziel beitragende Sicherheitsziel der FE ist somit Folgendes:

O.VU_Main	Die zu messenden und aufzuzeichnenden sowie daraufhin von den Kontrollbehörden zu prüfenden Daten müssen verfügbar sein und die Tätigkeiten der kontrollierten Fahrer und Fahrzeuge hinsichtlich Lenk-, Arbeits-, Bereitschafts- und Ruhezeiten sowie Fahrzeuggeschwindigkeit genau widerspiegeln
O.VU_Export	Mit der FE muss es möglich sein, Daten an externe Datenträger so zu exportieren, dass sich die Integrität und Authentizität dieser Daten verifizieren lässt

3.5. *Informationstechnische Sicherheitsziele*

Die speziellen, zum Hauptsicherheitsziel beitragenden IT-Sicherheitsziele der FE sind Folgende:

O.Access	Die FE muss den Zugriff der Benutzer auf Funktionen und Daten steuern
O.Accountability	Die FE muss exakte Zuordnungsdaten erfassen
O.Audit	Die FE muss Versuche zur Umgehung ihrer Sicherheitsfunktionen prüfen und zu den betreffenden Benutzern zurückverfolgen
O.Authentication	Die FE sollte Benutzer und angeschlossene Geräteeinheiten authentisieren (wenn ein vertrauenswürdiger Weg zwischen Geräteeinheiten eingerichtet werden muss)
O.Integrity	Die FE muss die Integrität der Speicherdaten wahren
O.Output	Die FE stellt sicher, dass die Datenausgabe die gemessenen bzw. gespeicherten Daten genau widerspiegelt
O.Processing	Die FE stellt sicher, dass die Eingabedaten, aus denen sich die Benutzerdaten ableiten, exakt verarbeitet werden
O.Reliability	Die FE muss zuverlässig arbeiten
O.Secured_Data_Exchange	Die FE muss den sicheren Datenaustausch mit dem Weg- und/oder Geschwindigkeitsgeber und mit Kontrollgerätkarten gewährleisten

3.6. *Physische, personelle bzw. verfahrenstechnische Mittel*

In diesem Abschnitt werden die physischen, personellen bzw. verfahrenstechnischen Anforderungen, die zur Sicherheit der FE beitragen, beschrieben.

3.6.1. *Gerätekonstruktion*

M.Development	Die Entwickler der FE müssen sicherstellen, dass die Zuweisung von Verantwortlichkeiten während des Entwicklungszeitraums in einer die IT-Sicherheit wahrenen Weise erfolgt
M.Manufacturing	Die Hersteller der FE müssen sicherstellen, dass die Zuweisung von Verantwortlichkeiten während des Herstellungsprozesses in einer die IT-Sicherheit wahrenen Weise erfolgt und dass die FE in diesem Prozess vor physischen Angriffen, die die IT-Sicherheit beeinträchtigen könnten, geschützt wird

3.6.2. *Auslieferung und Aktivierung der Geräte*

M.Delivery	Die Hersteller der FE, die Fahrzeughersteller und die Installateure bzw. Werkstätten müssen beim Umgang mit noch nicht aktivierten FE sicherstellen, dass die Sicherheit der FE gewahrt bleibt
M.Activation	Die Fahrzeughersteller und die Installateure bzw. Werkstätten müssen die FE nach erfolgtem Einbau aktivieren, und zwar noch bevor das Fahrzeug den Einbauort verlässt

3.6.3. *Generierung und Lieferung der Sicherheitsdaten*

M.Sec_Data_Generation	Die Algorithmen zur Generierung von Sicherheitsdaten dürfen nur berechtigten und vertrauenswürdigen Personen zugänglich sein
M.Sec_Data_Transport	Die Sicherheitsdaten müssen in einer Weise generiert, transportiert und in die FE eingebracht werden, die Vertraulichkeit und Integrität der Daten angemessen gewährleistet

3.6.4. Kartenübergabe

M.Card_Availability	Kontrollgerätkarten dürfen nur berechtigten Personen zugänglich gemacht und übergeben werden
M.Driver_Card_Uniqueness	Ein Fahrer darf immer nur eine gültige Fahrerkarte besitzen
M.Card_Traceability	Die Übergabe der Karten muss rückverfolgbar sein (weiße und schwarze Listen), und für die Sicherheitsaudits müssen schwarze Listen herangezogen werden

3.6.5. Einbau, Kalibrierung und Nachprüfung des Kontrollgeräts

M.Approved_Workshops	Einbau, Kalibrierung und Reparatur des Kontrollgeräts dürfen nur durch vertrauenswürdige und zugelassene Installateure bzw. Werkstätten erfolgen
M.Regular_Inpections	Die Kontrollgeräte müssen einer regelmäßigen Nachprüfung und Kalibrierung unterzogen werden
M.Faithful_Calibration	Zugelassene Installateure und Werkstätten müssen bei der Kalibrierung die richtigen Fahrzeugparameter in die Kontrollgeräte eingeben

3.6.6. Betrieb der Geräte

M.Faithful_Drivers	Die Fahrer müssen sich an die Vorschriften halten und verantwortungsvoll handeln (z. B. ihre Fahrerkarten benutzen, manuell auszuwählende Tätigkeiten korrekt anwählen usw.)
--------------------	--

3.6.7. Kontrolle der Einhaltung von Vorschriften

M.Controls	Die Einhaltung der gesetzlichen Vorschriften ist regelmäßig und stichprobenartig zu kontrollieren, unter anderem durch Sicherheitsaudits
------------	--

3.6.8. Software-Upgrades

M.Software_Upgrade	Neue Softwareversionen dürfen erst nach Erhalt der Sicherheitszertifizierung in der FE implementiert werden
--------------------	---

4. Sicherheitserzwingende Funktionen

4.1. Identifizierung und Authentisierung

4.1.1. Identifizierung und Authentisierung des Weg- und/oder Geschwindigkeitsgebers

UIA_201 Die FE ist in der Lage, für jede Interaktion die Identität des angeschlossenen Weg- und/oder Geschwindigkeitsgebers festzustellen.

UIA_202 Die Kennung des Weg- und/oder Geschwindigkeitsgebers setzt sich zusammen aus der Bauartgenehmigungsnummer und der Seriennummer des Weg- und/oder Geschwindigkeitsgebers.

UIA_203 Die FE authentisiert den angeschlossenen Weg- und/oder Geschwindigkeitsgeber:

- bei Anschließen des Weg- und/oder Geschwindigkeitsgebers,
- bei jeder Kalibrierung des Kontrollgeräts,
- bei Wiedereinschalten der Stromversorgung.

Die Authentisierung erfolgt gegenseitig und wird durch die FE ausgelöst.

UIA_204 Die FE identifiziert und authentisiert in regelmäßigen Intervallen (Intervalldauer vom Hersteller noch festzulegen, jedoch häufiger als einmal pro Stunde) den angeschlossenen Weg- und/oder Geschwindigkeitsgeber erneut und stellt dabei sicher, dass der bei der zuletzt erfolgten Kalibrierung des Kontrollgeräts erkannte Weg- und/oder Geschwindigkeitsgeber nicht ausgetauscht wurde.

UIA_205 Die FE erkennt und verhindert den Gebrauch kopierter und wieder eingespielter Authentisierungsdaten.

UIA_206 Nach Erkennen einer (vom Hersteller noch festzulegenden, jedoch 20 nicht übersteigenden) Zahl von aufeinander folgenden erfolglosen Authentisierungsversuchen und/oder nach Erkennen, dass der Weg- und/oder Geschwindigkeitsgeber ohne Berechtigung (d. h. nicht während einer Kalibrierung des Kontrollgeräts) ausgewechselt wurde, wird die SEF:

- ein Auditprotokoll über das Ereignis anlegen,
- den Benutzer warnen,
- die vom Weg- und/oder Geschwindigkeitsgeber gesendeten ungesicherten Weg- und Geschwindigkeitsdaten weiterhin annehmen und nutzen.

4.1.2. Identifizierung und Authentisierung des Benutzers

UIA_207 Die FE wird die Identität von zwei Benutzern durch Überwachung der in den Kartensteckplatz des Fahrers bzw. in den Kartensteckplatz des zweiten Fahrers eingesteckten Kontrollgerätkarten ständig und ausgewählt nachprüfen.

UIA_208 Die Benutzeridentität setzt sich zusammen aus:

- einer Benutzergruppe:
 - FAHRER (Fahrerkarte),
 - KONTROLLEUR (Kontrollkarte),
 - WERKSTATT (Werkstattkarte),
 - UNTERNEHMEN (Unternehmenskarte),
 - UNBEKANNT (keine Karte eingesteckt),
- einer Benutzerkennung, bestehend aus:
 - dem Code des die Karte ausstellenden Mitgliedstaats und der Kartenummer,
 - UNBEKANNT, falls die Benutzergruppe UNBEKANNT ist.

UNBEKANNTE Identitäten können implizit oder explizit bekannt sein.

UIA_209 Die FE authentisiert ihre Benutzer bei Einstecken der Karte.

UIA_210 Die FE authentisiert ihre Benutzer erneut:

- bei Wiederschalten der Stromversorgung,
- regelmäßig nach bestimmten Ereignissen (vom Hersteller noch festzulegen, jedoch öfter als einmal am Tag).

UIA_211 Die Authentisierung besteht in der Nachweisführung, dass die eingesteckte Karte eine gültige Kontrollgerätkarte ist, die über Sicherheitsdaten verfügt, die nur aus dem System selbst stammen können. Die Authentisierung erfolgt gegenseitig und wird durch die FE ausgelöst.

UIA_212 Zusätzlich ist auch eine erfolgreiche Authentisierung der Werkstätten mittels PIN-Prüfung erforderlich. Eine PIN umfasst mindestens 4 Zeichen.

Anmerkung: Falls die PIN durch ein in der Nähe der FE angeordnetes externes Gerät an die FE übertragen wird, ist ein Schutz der PIN während der Übertragung nicht erforderlich.

UIA_213 Die FE erkennt und verhindert den Gebrauch kopierter und wieder eingespielter Authentisierungsdaten.

UIA_214 Nach 5 aufeinander folgenden erfolglosen Authentisierungsversuchen wird die SEF:

- ein Auditprotokoll über das Ereignis anlegen,
- eine Warnung an den Benutzer ausgeben,
- davon ausgehen, dass der Benutzer UNBEKANNT und die Karte ungültig ist (Begriffsbestimmung z) und Anforderung 007).

4.1.3. Identifizierung und Authentisierung eines entfernt angeschlossenen Unternehmens

Die Fähigkeit zum entfernten Anschluss von Unternehmen ist optional. Dieser Absatz gilt daher nur, wenn dieses Merkmal implementiert ist.

- UIA_215 Bei jeder Interaktion mit einem entfernt angeschlossenen Unternehmen muss die FE zur Feststellung der Identität des Unternehmens in der Lage sein.
- UIA_216 Die Identität des entfernt angeschlossenen Unternehmens setzt sich aus dem Code des die Unternehmenskarte ausstellenden Mitgliedsstaats und der Nummer seiner Unternehmenskarte zusammen.
- UIA_217 Die FE muss das entfernt angeschlossene Unternehmen erst erfolgreich authentisieren, bevor sie jeglichen Datenexport an das Unternehmen zulässt.
- UIA_218 Die Authentisierung besteht in der Nachweisführung, dass das Unternehmen im Besitz einer gültigen Unternehmenskarte ist, die über Sicherheitsdaten verfügt, die nur aus dem System selbst stammen können.
- UIA_219 Die FE erkennt und verhindert den Gebrauch kopierter und wieder eingespielter Authentisierungsdaten.
- UIA_220 Nach 5 aufeinander folgenden erfolglosen Authentisierungsversuchen sendet die FE:

— An das entfernt angeschlossene Unternehmen eine Warnung aus.

4.1.4. Identifizierung und Authentisierung des Verwaltungsgeräts

Die Hersteller der FE können spezielle Geräte für zusätzliche FE-Verwaltungsfunktionen vorsehen (z. B. für Software-Upgrade, Neuladen von Sicherheitsdaten, ...). Dieser Absatz gilt daher nur, wenn dieses Merkmal implementiert ist.

- UIA_221 Bei jeder Interaktion mit einem Verwaltungsgerät muss die FE zur Feststellung der Identität des Geräts in der Lage sein.
- UIA_222 Die FE muss das Verwaltungsgerät erst erfolgreich authentisieren, bevor sie jegliche weitere Interaktion zulässt.
- UIA_223 Die FE erkennt und verhindert den Gebrauch kopierter und wieder eingespielter Authentisierungsdaten.

4.2. Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass nur speziell dazu berechtigte Personen Informationen aus dem PO auslesen sowie im PO anlegen bzw. nach Änderung in das PO einlesen.

Zu beachten ist, dass die von der FE aufgezeichneten Benutzerdaten zwar private bzw. kommerziell sensible Aspekte beinhalten, ihrem Wesen nach jedoch nicht vertraulich sind. Aus diesem Grund ist die auf das Zugriffsrecht zum Lesen von Daten bezogene funktionelle Anforderung (Anforderung 011) nicht Gegenstand einer sicherheitserzwingenden Funktion.

4.2.1. Zugriffsberechtigung

- ACC_201 Die FE verwaltet und prüft die Zugriffsberechtigung auf Funktionen und Daten.

4.2.2. Funktionszugriffrechte

- ACC_202 Die FE dient der Durchsetzung der Vorschriften zur Betriebsartauswahl (Anforderungen 006 bis 009).
- ACC_203 Mit der FE werden ausgehend von der Betriebsart die Vorschriften für die Funktionszugriffskontrolle durchgesetzt (Anforderung 010).

4.2.3. Datenzugriffsrechte

- ACC_204 Die FE dient der Durchsetzung der Vorschriften für den Schreibzugriff auf die FE-Kennndaten (Anforderung 076)
- ACC_205 Die FE dient der Durchsetzung der Vorschriften für den Schreibzugriff auf die gekoppelten Weg- und/oder Geschwindigkeitsgeberkennndaten (Anforderungen 079 und 155)
- ACC_206 Nach der FE-Aktivierung stellt die FE sicher, dass Kalibrierungsdaten einzig in der Betriebsart Kalibrierung in die FE eingegeben und in ihrem Massenspeicher abgelegt werden können (Anforderungen 154 und 156).
- ACC_207 Nach der FE-Aktivierung sorgt die FE für die Durchsetzung der Vorschriften für den Schreib- und Löschzugriff auf die Kalibrierungsdaten (Anforderung 097).

ACC_208 Nach der FE-Aktivierung stellt die FE sicher, dass Zeiteinstellungsdaten einzig in der Betriebsart Kalibrierung in die FE eingegeben und in ihrem Massenspeicher abgelegt werden können. (Diese Anforderung trifft nicht auf geringfügige Zeiteinstellungen zu, wie sie im Rahmen der Anforderungen 157 und 158 gestattet sind.)

ACC_209 Nach der FE-Aktivierung sorgt die FE für die Durchsetzung der Vorschriften für den Schreib- und Löschzugriff auf die Zeiteinstellungsdaten (Anforderung 100).

ACC_210 Die FE gewährleistet angemessene Zugriffsrechte zum Lesen und Schreiben von Sicherheitsdaten (Anforderung 080).

4.2.4. Dateistruktur und -zugriffsbedingungen

ACC_211 Die Strukturen der Anwendungs- und Datendateien und die Zugriffsbedingungen auf diese Dateien werden bereits im Herstellungsprozess angelegt und gegen jegliche spätere Verfälschung bzw. Löschung gesperrt.

4.3. Zuordnungsmöglichkeit

ACT_201 Die FE stellt sicher, dass den Fahrern ihre Tätigkeiten zugeordnet werden können (Anforderungen 081, 084, 087, 105a, 105b, 109 und 109a).

ACT_202 Die FE speichert Kenndaten dauerhaft (Anforderung 075).

ACT_203 Die FE stellt sicher, dass den Werkstätten ihre Tätigkeiten zugeordnet werden können (Anforderungen 098, 101 und 109).

ACT_204 Die FE stellt sicher, dass den Kontrolleuren ihre Tätigkeiten zugeordnet werden können (Anforderungen 102, 103 und 109).

ACT_205 Die FE zeichnet Kilometerstände (Anforderung 090) und Geschwindigkeitsdaten mit Detailangaben auf (Anforderung 093).

ACT_206 Die FE stellt sicher, dass die Anforderungen 081 bis 093 und 102 bis einschließlich 105b betreffende Benutzerdaten nach Aufzeichnung nicht mehr geändert werden, außer wenn diese zu den ältesten Daten werden, die bei erschöpftem Speicher durch neue Daten überschrieben werden.

ACT_207 Die FE darf bereits auf einer Kontrollgerätekarte gespeicherte Daten nicht ändern (Anforderungen 109 und 109a), außer beim Überschreiben der ältesten Daten durch neue Daten (Anforderung 110) bzw. im in der Anmerkung zu Absatz 2.1 in Anlage 1 beschriebenen Fall.

4.4. Audit

Die Möglichkeit der Durchführung von Audits ist nur für Ereignisse erforderlich, die auf einen Versuch der Manipulation bzw. Sicherheitsverletzung hindeuten. Für die übliche Ausübung von Rechten sind Auditfähigkeiten auch dann, wenn dies sicherheitserzwingend ist, nicht gefordert.

AUD_201 Die FE muss Ereignisse, die ihre Sicherheit beeinträchtigen, mit den dazugehörigen Daten aufzeichnen (Anforderungen 094, 096 und 109).

AUD_202 Folgende Ereignisse beeinträchtigen die Sicherheit der FE:

- Sicherheitsverletzende Versuche:
 - fehlgeschlagene Authentisierung des Weg- und/oder Geschwindigkeitsgebers,
 - fehlgeschlagene Authentisierung der Kontrollgerätekarte,
 - unberechtigtes Auswechseln des Weg- und/oder Geschwindigkeitsgebers,
 - Integritätsfehler der Karteneingabedaten,
 - Integritätsfehler der gespeicherten Benutzerdaten,
 - interner Datenübertragungsfehler,
 - unberechtigtes Öffnen des Gehäuses,
 - Hardwaremanipulation,

- Letzte Kartentransaktion nicht ordnungsgemäß abgeschlossen,
- Weg- und Geschwindigkeitsdatenfehlerereignis,
- Unterbrechung der Stromversorgung,
- FE-interne Störung.

AUD_203 Mit der FE werden die Speichervorschriften für Auditprotokolle durchgesetzt (Anforderung 094 und 096).

AUD_204 Die FE legt die vom Weg- und/oder Geschwindigkeitsgeber generierten Auditprotokolle in ihrem Massenspeicher ab.

AUD_205 Es muss möglich sein, Auditprotokolle auszudrucken, anzuzeigen und zu übertragen.

4.5. **Wiederverwendung von Speichermedien**

REU_201 Die FE stellt sicher, dass Zwischenspeichermedien wiederverwendet werden können, ohne einen unzulässigen Informationsfluss zu beinhalten.

4.6. **Genauigkeit**

4.6.1. *Maßnahmen zur Kontrolle des Informationsflusses*

ACR_201 Die FE stellt sicher, dass die Anforderungen 081, 084, 087, 090, 093, 102, 104, 105, 105a und 109 betreffende Benutzerdaten nur verarbeitet werden, wenn sie von den richtigen Eingabequellen stammen:

- Weg- und Geschwindigkeitsdaten des Fahrzeugs,
- Echtzeituhr der FE,
- Kalibrierungsparameter des Kontrollgeräts,
- Kontrollgerätkarten,
- Eingaben durch Benutzer.

ACR_201a Die FE stellt sicher, dass die Anforderung 109a betreffende Benutzerdaten nur für den Zeitraum von der letzten Kartenentnahme bis zum derzeitigen Einstecken der Karte eingegeben werden können (Anforderung 050a).

4.6.2. *Interne Datenübertragung*

Die Anforderungen dieses Absatzes gelten nur, wenn die FE physisch getrennte Teile nutzt.

ACR_202 Werden Daten zwischen physisch getrennten Teilen der FE übertragen, müssen diese Daten gegen Verfälschungen geschützt werden.

ACR_203 Bei Erkennen eines Datenübertragungsfehlers im Verlauf einer internen Datenübertragung wird die Übertragung wiederholt und über das Ereignis ein Auditprotokoll durch die SEF angelegt.

4.6.3. *Integrität der Speicherdaten*

ACR_204 Die FE prüft die in ihrem Speicher abgelegten Benutzerdaten auf Integritätsfehler.

ACR_205 Bei Erkennen eines Integritätsfehlers der Benutzerdaten generiert die SEF ein Auditprotokoll.

4.7. **Zuverlässigkeit während des Betriebs**

4.7.1. *Prüfungen*

RLB_201 Sämtliche speziell für den Prüfbedarf während der Herstellungsphase der FE erforderlichen Befehle, Handlungen bzw. Prüfpunkte werden vor Aktivierung der FE deaktiviert oder entfernt. Es darf nicht möglich sein, sie zum späteren Gebrauch wiederherzustellen.

RLB_202 Die FE führt zur Funktionsprüfung beim ersten Einschalten sowie während des normalen Betriebs Selbsttests durch. Die Selbsttests der FE beinhalten eine Integritätsprüfung der Sicherheitsdaten sowie eine Integritätsprüfung des gespeicherten Ausführungscodes (sofern dieser nicht im ROM gespeichert ist).

RLB_203 Bei Erkennen einer internen Fehlfunktion während der Selbstprüfung wird die SEF:

- ein Auditprotokoll erstellen (außer in der Betriebsart Kalibrierung) (FE-interne Störung),
- die Speicherdatenintegrität wahren.

4.7.2. Software

RLB_204 Es darf keine Möglichkeit gegeben sein, die Software nach Aktivierung der FE bei der Praxisanwendung zu analysieren bzw. auszutesten.

RLB_205 Eingaben aus externen Quellen dürfen als Ausführungscodes nicht akzeptiert werden.

4.7.3. Physischer Schutz

RLB_206 Falls die Konstruktionsweise der FE ein Öffnen des Gehäuses erlaubt, muss die FE jedes Öffnen des Gehäuses feststellen, selbst wenn die externe Stromversorgung bis zu 6 Monate unterbrochen ist. Die SEF legt in diesem Fall ein Auditprotokoll an (hierbei ist zulässig, dass das Auditprotokoll erst nach Wiedereinschalten der Stromversorgung erstellt und gespeichert wird).

Ist die FE so konstruiert, dass sie nicht geöffnet werden kann, muss ihre Bauweise dennoch jeden Versuch der physischen Manipulation leicht erkennen lassen (z. B. durch Sichtprüfung).

RLB_207 Die FE muss nach ihrer Aktivierung bestimmte (vom Hersteller noch festzulegende) Formen der Hardwaremanipulation erkennen.

RLB_208 In vorgenannten Fall erstellt die SEF ein Auditprotokoll und wird die FE ... (vom Hersteller noch festzulegen).

4.7.4. Unterbrechung der Stromversorgung

RLB_209 Die FE erkennt Abweichungen von den festgelegten Stromwerten einschließlich einer Unterbrechung der Stromversorgung.

RLB_210 Im vorgenannten Fall wird die SEF:

- ein Auditprotokoll erstellen (außer in der Betriebsart Kalibrierung),
- den Sicherheitsstatus der FE wahren,
- die Sicherheitsfunktionen für die noch in Betrieb befindlichen Komponenten bzw. noch laufenden Prozesse aufrechterhalten,
- die Speicherdatenintegrität wahren.

4.7.5. Rücksetzbedingungen

RLB_211 Bei einer Unterbrechung der Stromversorgung, beim Abbruch einer Transaktion vor deren Vervollständigung bzw. bei Vorliegen jeder sonstigen Rücksetzbedingung muss die FE sauber zurückgesetzt werden.

4.7.6. Datenbereitstellung

RLB_212 Die FE stellt sicher, dass auf den Datenbestand bei Bedarf zugegriffen werden kann und dass die Daten weder unnötig abgerufen noch zurückgehalten werden.

RLB_213 Die FE muss gewährleisten, dass die Kartenfreigabe erst erfolgt, nachdem die relevanten Daten auf die Karten gespeichert wurden (Anforderungen 015 und 016).

RLB_214 Im vorgenannten Fall wird die SEF ein Auditprotokoll über das Ereignis anlegen.

4.7.7. Multifunktionsgeräte

RLB_215 Falls die FE neben der Kontrollgerätfunktion noch weitere Anwendungen bietet, müssen alle diese Anwendungen physisch und/oder logisch voneinander getrennt sein. Jede dieser Anwendungen muss auf eigene Sicherheitsdaten zurückgreifen, und es darf immer nur eine Funktion aktiv sein.

4.8. Datenaustausch

Dieser Absatz betrifft den Datenaustausch zwischen der FE und angeschlossenen Geräten.

4.8.1. Datenaustausch mit dem Weg- und/oder Geschwindigkeitsgeber

DEX_201 Die FE prüft die Integrität und Authentizität der vom Weg- und/oder Geschwindigkeitsgeber importierten Daten.

DEX_202 Bei Erkennen eines Integritäts- bzw. Authentizitätsfehlers der Weg- und Geschwindigkeitsdaten wird die SEF:

- ein Auditprotokoll generieren,
- die importierten Daten weiterhin verwenden.

4.8.2. Datenaustausch mit Kontrollgerätarten

DEX_203 Die FE prüft die Integrität und Authentizität der von den Kontrollgerätarten importierten Daten.

DEX_204 Bei Erkennen eines Integritäts- bzw. Authentizitätsfehlers der Weg- und Geschwindigkeitsdaten wird die FE:

- ein Auditprotokoll generieren,
- die Daten nicht verwenden.

DEX_205 Die FE exportiert die Daten mit den zugehörigen Sicherheitsattributen an die Kontrollgerätarten, so dass die Karte die Integrität und Authentizität der Daten prüfen kann.

4.8.3. Datenaustausch mit externen Datenträgern (Übertragungsfunktion)

DEX_206 Die FE generiert für an externe Datenträger übertragene Daten einen Herkunftsnachweis.

DEX_207 Die FE stellt dem Empfänger der übertragenen Daten eine Fähigkeit zur Prüfung des Herkunftsnachweises bereit.

DEX_208 Die FE exportiert die Daten mit den zugehörigen Sicherheitsattributen an den externen Datenträger, so dass sich Integrität und Authentizität der Daten prüfen lassen.

4.9. Kryptografische Unterstützung

Je nach Sicherheitsmechanismus und vom Hersteller gewählten Lösungen gelten die Anforderungen dieses Absatzes nur soweit erforderlich.

CSP_201 Jede von der FE durchgeführte kryptografische Operation entspricht einem genau festgelegten Algorithmus und einer genau festgelegten Schlüsselgröße.

CSP_202 Falls die FE kryptografische Schlüssel generiert, müssen diese genau festgelegten Schlüsselgenerierungsalgorithmen und genau festgelegten Schlüsselgrößen entsprechen.

CSP_203 Falls die FE kryptografische Schlüssel vergibt, muss dies nach genau festgelegten Schlüsselvergabemethoden erfolgen.

CSP_204 Falls die FE auf kryptografische Schlüssel zugreift, muss dies nach genau festgelegten Schlüsselzugriffsmethoden erfolgen.

CSP_205 Falls die FE kryptografische Schlüssel vernichtet, muss dies nach genau festgelegten Schlüsselvernichtungsmethoden erfolgen.

5. Beschreibung der Sicherheitsmechanismen

Die geforderten Sicherheitsmechanismen werden in Anlage 11 beschrieben.

Alle sonstigen Sicherheitsmechanismen werden durch die Hersteller festgelegt.

6. Mindestrobustheit der Sicherheitsmechanismen

Die Mindestrobustheit der Sicherheitsmechanismen der Fahrzeugeinheit ist Hoch, gemäß Definition in ITSEC.

7. Gewährleistungsebene

Die für die Fahrzeugeinheit vorgegebene Gewährleistungsebene ist die ITSEC-Ebene E3, gemäß Definition in ITSEC.

8. Grundlegendes Prinzip

Die folgenden Kreuzgitter sollen das Prinzip der SEF begründen, indem sie verdeutlichen:

- welche SEF bzw. Mittel welchen Sicherheitsgefährdungen entgegenwirken,
- welche SEF welche IT-Sicherheitsziele erfüllen.

	Sicherheitsgefährdungen																IT-Zielsetzungen										
	Zugriff	Identifizierung	Fehler/Störungen	Prüfungen	Konstruktion	Kalibrierungsparameter	Kartendatenaustausch	Uhr	Umfeld	Nachgebaute Geräte	Hardware	Weg-/Geschwindigkeitsdaten	Nicht aktiviert	Ausgabedaten	Stromversorgung	Sicherheitsdaten	Software	Speicherdaten	Zugriff	Zuordnungsmöglichkeit	Audit	Authentisierung	Integrität	Ausgabe	Datenverarbeitung	Verlässlichkeit	Gesicherter Datenaustausch
Physische, personelle, verfahrenstechnische Mittel																											
Entwicklung			x	x	x																						
Herstellung				x	x																						
Auslieferung													x														
Aktivierung	x											x															
Generierung von Sicherheitsdaten													x														
Transport von Sicherheitsdaten																x											
Kartenverfügbarkeit		x																									
Nur eine Karte pro Fahrer		x																									
Rückverfolgbarkeit der Karte		x																									
Zugelassene Werkstätten						x		x																			
Regelmäßige Nachprüfung, Kalibrierung						x		x				x	x			x											
Verlässliche Werkstätten						x		x																			
Verlässliche Fahrer		x																									
Durchsetzung gesetzlicher Vorschriften		x				x		x	x		x		x		x		x	x									
Software-Upgrade																		x									
Sicherheitserzwingende Funktionen																											
Identifizierung und Authentisierung																											
UIA_201 Geberidentifizierung										x		x										x					x
UIA_202 Geberidentität										x		x									x						x
UIA_203 Geberauthentisierung										x		x									x						x
UIA_204 Sensor-Neuidentifizierung und -Neuauthentisierung										x		x									x						x
UIA_205 Fälschungssichere Authentisierung										x		x									x						
UIA_206 Fehlgeschlagene Authentisierung										x		x									x					x	
UIA_207 Benutzeridentifizierung	x	x								x								x			x						x
UIA_208 Benutzeridentität	x	x								x								x			x						x
UIA_209 Benutzerauthentisierung	x	x								x								x			x						x
UIA_210 Benutzer-Neuauthentisierung	x	x								x								x			x						x
UIA_211 Authentisierungsmittel	x	x								x								x			x						
UIA_212 PIN-Prüfungen	x	x				x		x										x			x						
UIA_213 Fälschungssichere Authentisierung	x	x								x								x			x						

	Sicherheitsgefährdungen																IT-Zielsetzungen										
	Zugriff	Identifizierung	Fehler/Störungen	Prüfungen	Konstruktion	Kalibrierungsparameter	Kartendatenaustausch	Uhr	Umfeld	Nachgebaute Geräte	Hardware	Weg-/Geschwindigkeitsdaten	Nicht aktiviert	Ausgabedaten	Stromversorgung	Sicherheitsdaten	Software	Speicherdaten	Zugriff	Zuordnungsmöglichkeit	Audit	Authentisierung	Integrität	Ausgabe	Datenverarbeitung	Verlässlichkeit	Gesicherter Datenaustausch
UIA_214 Fehlgeschlagene Authentisierung	x	x								x											x						
UIA_215 Identifizierung entfernter Benutzer	x	x																	x			x					x
UIA_216 Identität entfernter Benutzer	x	x																	x			x					
UIA_217 Authentisierung entfernter Benutzer	x	x																	x			x					x
UIA_218 Authentisierungsmittel	x	x																	x			x					
UIA_219 Fälschungssichere Authentisierung	x	x																	x			x					
UIA_220 Fehlgeschlagene Authentisierung	x	x																									
UIA_221 Verwaltungsgerät-Identifizierung	x	x																	x			x					
UIA_222 Verwaltungsgerät-Authentisierung	x	x																	x			x					
UIA_223 Fälschungssichere Authentisierung	x	x																	x			x					
Zugriffskontrolle																											
ACC_201 Zugriffskontrollregeln	x					x	x										x		x	x							
ACC_202 Zugriffsrechte auf Funktionen	x					x	x													x							
ACC_203 Zugriffsrechte auf Funktionen	x					x	x													x							
ACC_204 FE-Kennung																			x	x							
ACC_205 Kennung angeschlossener Geber										x									x	x							
ACC_206 Kalibrierungsdaten	x					x													x	x							
ACC_207 Kalibrierungsdaten						x													x	x							
ACC_208 Zeiteinstellungsdaten								x											x	x							
ACC_209 Zeiteinstellungsdaten								x											x	x							
ACC_210 Sicherheitsdaten																	x		x	x							
ACC_211 Datenstruktur und Zugriffsbedingungen	x					x											x		x	x							
Zuordnungsmöglichkeit																											
ACT_201 Zuordnung zu Fahrern																				x							
ACT_202 FE-Kennndaten																				x	x						
ACT_203 Zuordnung zu Werkstätten																				x							
ACT_204 Zuordnung zu Kontrolleuren																				x							
ACT_205 Zuordnung zu Fahrzeugen																				x							
ACT_206 Zuordnungsdatenänderung																			x				x			x	
ACT_207 Zuordnungsdatenänderung																			x				x			x	

[illegible]

[illegible]

ALLGEMEINE SICHERHEITSANFORDERUNGEN FÜR DIE KONTROLLGERÄTKARTE

1. Einführung

In diesem Abschnitt werden die Kontrollgerätkarte, mögliche Sicherheitsgefährdungen sowie die zu erfüllenden Sicherheitsziele beschrieben. Außerdem enthält er Erläuterungen zu den zur Durchsetzung der Sicherheitsanforderungen erforderlichen Funktionen, und es erfolgt eine Auflistung der Mindestanforderungen an die Sicherheitsmechanismen und die erforderliche Gewährleistungsebene für Entwicklung und Evaluierung.

Die hier aufgeführten Anforderungen entsprechen den Anforderungen im Hauptteil von Anhang I B. Im Interesse einer besseren Verständlichkeit können sich Doppelungen zwischen den Anforderungen im Hauptteil von Anhang I B und den Sicherheitsanforderungen ergeben. Bei Diskrepanzen zwischen einer Sicherheitsanforderung und der Anforderung im Hauptteil von Anhang I B, auf die sich diese Sicherheitsanforderung bezieht, geht die Anforderung im Hauptteil von Anhang I B vor.

Anforderungen im Hauptteil von Anhang I B, auf die sich diese Sicherheitsanforderungen nicht beziehen, sind nicht Gegenstand der Funktionen zur Durchsetzung von Sicherheitsanforderungen.

Eine Kontrollgerätkarte ist eine serienmäßige Chipkarte mit einer speziellen Kontrollgerätenwendung. Sie muss den aktuellen Funktions- und Sicherheitsanforderungen an Chipkarten genügen. Die im Folgenden dargelegten Sicherheitsanforderungen beinhalten daher nur die zusätzlichen Sicherheitsanforderungen in Bezug auf die Kontrollgerätenwendung.

Zwecks besserer Zuordnung zu den in der Dokumentation über Entwicklung und Evaluierung verwendeten Begriffen wurden für die möglichen Sicherheitsgefährdungen sowie die zu erfüllenden Ziele, Verfahrensmöglichkeiten und SEF-Spezifikationen eindeutige Bezeichnungen gewählt.

2. Abkürzungen, Begriffsbestimmungen und Referenzdokumente**2.1. Abkürzungen**

IC	Integrierter Schaltkreis (Elektronisches Bauelement zum Ausführen von Datenverarbeitungs- und/oder Speicherfunktionen)
OS	Betriebssystem
PIN	Persönliche Geheimzahl (Personal Identification Number)
ROM	Festspeicher (Read Only Memory)
SFP	Sicherheitsfunktionsregeln
PO	Prüfobjekt
TSF	Sicherheitsfunktion des Prüfobjekts
FE	Fahrzeugeinheit (Vehicle Unit)

2.2. Begriffsbestimmungen

Digitaler Fahrtenschreiber	Kontrollgerät
Sensible Daten	Von der Kontrollgerätkarte gespeicherte Daten, deren Schutz hinsichtlich Integrität, unberechtigten Zugriff und Vertraulichkeit (sofern auf Sicherheitsdaten zutreffend) erforderlich ist. Zu sensiblen Daten zählen Sicherheitsdaten und Benutzerdaten
Sicherheitsdaten	Spezielle Daten, die zur Unterstützung der sicherheitserzwingenden Funktionen erforderlich sind (z. B. kryptografische Schlüssel)
System	Gerätetechnik, Menschen bzw. Organisationen, die in welcher Weise auch immer mit den Kontrollgeräten in Beziehung stehen
Benutzer	Jede Person oder externe IT-Geräteinheit, die nicht Teil des PO ist, jedoch mit dem PO in Interaktion tritt

Benutzerdaten	Auf der Kontrollgerätekarte gespeicherte sensible Daten, mit Ausnahme der Sicherheitsdaten. Zu den Benutzerdaten zählen Kenndaten und Tätigkeitsdaten
Kenndaten	Die Kenndaten beinhalten die Kenndaten der Karte und die Kenndaten des Karteninhabers
Kartenkenndaten	Benutzerdaten zur Kartenidentifizierung entsprechend den Anforderungen 190, 191, 192, 194, 215, 231 und 235
Karteninhaberkenndaten	Benutzerdaten zur Identifizierung des Karteninhabers entsprechend den Anforderungen 195, 196, 216, 232 und 236
Tätigkeitsdaten	Zu den Tätigkeitsdaten zählen die Karteninhabertätigkeitsdaten, die Ereignis- und Störungsdaten sowie die Kontrolltätigkeitsdaten
Karteninhabertätigkeitsdaten	Die Tätigkeiten des Karteninhabers betreffende Benutzerdaten entsprechend den Anforderungen 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 und 237
Ereignis- und Störungsdaten	Ereignisse bzw. Störungen und Fehlfunktionen betreffende Benutzerdaten entsprechend den Anforderungen 204, 205, 207, 208 und 223
Kontrolltätigkeitsdaten	Die Kontrollen der Durchsetzung gesetzlicher Vorschriften betreffende Benutzerdaten entsprechend den Anforderungen 210 und 225

2.3. Referenzdokumente

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 (Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik)
IC PP	Smartcard Integrated Circuit Protection Profile (Profil für den Schutz von Chipkarten-ICs) — Version 2.0 — Ausgabe September 1998. Eingetragen bei der französischen Zertifizierungsstelle unter Nummer PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile (Profil für den Schutz von Chipkarten-ICs mit eingebetteter Software) — Version 2.0 — Ausgabe Juni 1999. Eingetragen bei der französischen Zertifizierungsstelle unter Nummer PP/9911

3. Grundprinzip des Produkts

3.1. Beschreibung und Verwendung der Kontrollgerätekarte

Eine Kontrollgerätekarte ist eine Chipkarte wie in IC PP und ES PP beschrieben, die eine Anwendung zur Verwendung der Karte mit dem Kontrollgerät beherbergt.

Die grundlegenden Funktionen der Kontrollgerätekarte sind:

- das Speichern der Karten- und der Karteninhaberkenndaten. Diese Daten werden von der Fahrzeugeinheit verwendet, um den Karteninhaber zu identifizieren, dementsprechende Funktionen und Datenzugriffsrechte zu gewähren und sicherzustellen, dass dem Karteninhaber seine Tätigkeiten zugerechnet werden können,
- das Speichern von Karteninhabertätigkeitsdaten, von Ereignis- und Störungsdaten sowie von Kontrolltätigkeitsdaten, die auf den Karteninhaber bezogen sind.

Eine Kontrollgerätekarte ist somit zur Verwendung durch das Kartenschnittstellengerät einer Fahrzeugeinheit gedacht. Ebenso kann es durch jeden sonstigen Kartenleser (z. B. eines PC), der das uneingeschränkte Zugriffsrecht auf jegliche Benutzerdaten hat, verwendet werden.

In der Endnutzungsphase des Lebenszyklus einer Kontrollgerätekarte (Phase 7 des Lebenszyklus gemäß Beschreibung in ES PP), können nur Fahrzeugeinheiten Benutzerdaten auf die Karte schreiben.

Die funktionellen Anforderungen an eine Kontrollgerätekarte sind im Hauptteil von Anhang I B und in Anlage 2 beschrieben.

3.2. Lebenszyklus der Kontrollgerätekarte

Der Lebenszyklus der Kontrollgerätekarte entspricht dem in ES PP beschriebenen Lebenszyklus einer Chipkarte.

3.3. Sicherheitsgefährdungen

Neben den in ES PP und IC PP aufgelisteten allgemeinen Sicherheitsgefährdungen für eine Chipkarte kann es bei Kontrollgerätekarten zu folgenden Sicherheitsgefährdungen kommen.

3.3.1. Letztliche Ziele

Das Ziel von Manipulationen wird letztendlich darin bestehen, die im PO gespeicherten Benutzerdaten zu verfälschen.

T.Ident_Data	Eine erfolgreiche Änderung der im PO abgelegten Kenndaten (z. B. des Kartentyps, des Kartenablaufdatums oder der Karteninhaberkennndaten) würde eine betrügerische Verwendung des PO ermöglichen und eine erhebliche Gefährdung des globalen Sicherheitsziels des Systems bedeuten.
T.Activity_Data	Eine erfolgreiche Änderung der im PO abgelegten Tätigkeitsdaten würde die Sicherheit des PO gefährden.
T.Data_Exchange	Eine erfolgreiche Änderung der Tätigkeitsdaten (Hinzufügung, Löschung, Verfälschung) während des Datenimports bzw. -exports würde die Sicherheit des PO gefährden.

3.3.2. Angriffswege

Angriffe auf die Ressourcen des PO sind möglich durch:

- den Versuch, unrechtmäßige Kenntnis über Hardware- und Softwareentwurf des PO zu erlangen, insbesondere über dessen Sicherheitsfunktionen bzw. Sicherheitsdaten. Unrechtmäßige Kenntnis kann durch Angriffe auf Material der Konstrukteure bzw. Hersteller (Diebstahl, Bestechung) oder durch unmittelbare Untersuchung des PO (physische Erkundung, Interferenzanalyse) erworben werden.
- Ausnutzung von Schwächen im konstruktiven Entwurf bzw. in der Ausführung des PO (Hardware- bzw. Softwarefehler, Übertragungsfehlfunktionen, im PO durch äußere Einwirkungen hervorgerufene Fehler, Ausnutzen von Schwächen der Sicherheitsfunktionen, wie z. B. der Authentisierungsverfahren, Datenzugriffskontrolle, kryptografischen Operationen usw.).
- Manipulation des PO bzw. der Sicherheitsfunktionen des PO durch physische, elektrische oder logische Angriffe bzw. durch eine Kombination derselben.

3.4. Sicherheitsziele

Das wichtigste Sicherheitsziel des gesamten digitalen Fahrtenschreibersystems ist Folgendes:

O.Main	Die von den Kontrollbehörden zu prüfenden Daten müssen verfügbar sein und die Handlungen der kontrollierten Fahrer und Fahrzeuge hinsichtlich Lenk-, Arbeits-, Bereitschafts- und Ruhezeiten sowie Fahrzeuggeschwindigkeit vollständig und genau widerspiegeln.
--------	---

Das zum übergreifenden Sicherheitsziel beitragende Sicherheitsziel des PO ist somit Folgendes:

O.Card_Identification_Data	Das PO muss die während des Prozesses der Kartenpersonalisierung gespeicherten Kartenkenndaten und Karteninhaberkennndaten bewahren.
O.Card_Activity_Storage	Das PO muss die von Fahrzeugeinheiten auf der Karte gespeicherten Benutzerdaten bewahren.

3.5. Informationstechnische Sicherheitsziele

Neben den in ES PP und IC PP aufgelisteten allgemeinen Sicherheitszielen für eine Chipkarte tragen folgende spezielle IT-Sicherheitsziele des PO zu dessen Hauptsicherheitsziel während der Endnutzungsphase des Lebenszyklus bei:

O.Data_Access	Das PO muss die Zugriffsrechte für das Schreiben von Benutzerdaten auf authentifizierte Fahrzeugeinheiten beschränken.
O.Secure_Communications	Das PO muss sichere Kommunikationsprotokolle und -verfahren zwischen der Karte und dem Kartenschnittstellengerät unterstützen, wenn die jeweilige Anwendung dies erfordert.

3.6. Physische, personelle bzw. verfahrenstechnische Mittel

Die physischen, personellen bzw. verfahrenstechnischen Anforderungen, die zur Sicherheit des PO beitragen, sind in ES PP und IC PP aufgeführt (Kapitel zu Sicherheitszielen für das Umfeld).

4. Sicherheitserzwingende Funktionen

In diesem Abschnitt werden einige der zulässigen Operationen wie Zuweisung bzw. Auswahl von ES PP näher spezifiziert und zusätzliche funktionelle Anforderungen an die SEF gestellt.

4.1. Einhaltung von Schutzprofilen

CPP_301 Das PO hält die IC PP ein.

CPP_302 Das PO hält die ES PP, wie im weiteren näher spezifiziert, ein.

4.2. Identifizierung und Authentisierung des Benutzers

Die Karte muss die Geräteeinheit, in die sie eingesteckt wird, identifizieren und erkennen, ob es sich um ein authentisiertes Fahrzeug handelt oder nicht. Die Karte darf ungeachtet der Geräteeinheit, an die sie angeschlossen ist, jegliche Benutzerdaten exportieren. Eine Ausnahme bildet die Kontrollkarte, die die Karteninhaberdaten nur an authentisierte Fahrzeugeinheiten exportieren darf (damit sich ein Kontrolleur durch Lesen seines Namens auf der Anzeige bzw. dem Ausdruck vergewissern kann, dass es sich bei der Fahrzeugeinheit nicht um einen Nachbau handelt).

4.2.1. Identifizierung des Benutzers

Zuweisung (FIA_UID.1.1) Liste von TSF-vermittelten Handlungen: keine.

Zuweisung (FIA_ATD.1.1) Liste von Sicherheitsattributen:

- USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,
- USER_ID: aml. Kennzeichen (VRN) und Code des registrierenden Mitgliedstaats (USER_ID ist nur bei USER_GROUP = VEHICLE_UNIT bekannt).

4.2.2. Authentisierung des Benutzers

Zuweisung (FIA_UAU.1.1) Liste von TSF-vermittelten Handlungen:

- Fahrer- und Werkstattkarten: Export von Benutzerdaten mit Sicherheitsattributen (Kartendaten-Übertragungsfunktion),
- Kontrollkarte: Export von Benutzerdaten ohne Sicherheitsattribute, mit Ausnahme der Karteninhaberdaten.

UIA_301 Die Authentisierung der Fahrzeugeinheit besteht in der Nachweisführung, dass sie über Sicherheitsdaten verfügt, die nur aus dem System selbst stammen können.

Auswahl (FIA_UAU.3.1 und FIA_UAU.3.2): verhindern.

Zuweisung (FIA_UAU.4.1) Identifizierte(r) Authentisierungsmechanismen(-mus): jeder beliebige Authentisierungsmechanismus.

UIA_302 Die Werkstattkarte stellt durch Prüfung eines PIN-Codes einen zusätzlichen Authentisierungsmechanismus bereit. (Dieser Mechanismus soll es der Fahrzeugeinheit ermöglichen, die Identität des Karteninhabers zu prüfen; er dient indes nicht dem Schutz des Inhalts der Werkstattkarte.)

4.2.3. Fehlgeschlagene Authentisierungen

Die folgenden Zuweisungen beschreiben die Reaktion der Karte auf jede einzelne fehlgeschlagene Authentisierung.

Zuweisung (FIA_AFL.1.1) Nummer: 1, Liste der Authentisierungsereignisse: Authentisierung eines Kartenschnittstellengeräts.

Zuweisung (FIA_AFL.1.2) Handlungsliste:

- Warnung der angeschlossenen Geräteeinheit,
- Behandlung des Benutzers als NON_VEHICLE_UNIT.

Die folgenden Zuweisungen beschreiben die Reaktion der Karte im Fall eines fehlgeschlagenen zusätzlichen Authentisierungsmechanismus gemäß Anforderung UIA_302.

Zuweisung (FIA_AFL.1.1) Nummer: 5, Liste der Authentisierungsereignisse: PIN-Prüfungen (Werkstattkarte).

Zuweisung (FIA_AFL.1.2) *Handlungsliste:*

- Warnung der angeschlossenen Geräteeinheit,
- Sperren des PIN-Prüfverfahrens, so dass jeder nachfolgende Versuch der PIN-Prüfung fehlschlägt,
- Möglichkeit der Anzeige der Sperrung an nachfolgende Benutzer.

4.3. Zugriffskontrolle**4.3.1. Zugriffskontrollregeln**

Während der Endnutzungsphase ihres Lebenszyklus ist die Kontrollgerätkarte Gegenstand der Sicherheitsfunktionsregeln (SFP) für einfache Zugriffskontrolle mit der Bezeichnung AC_SFP.

Zuweisung (FDP_ACC.2.1) *Zugriffskontroll-SFP: AC_SFP.*

4.3.2. Zugriffskontrollfunktionen

Zuweisung (FDP_ACF.1.1) *Zugriffskontroll-SFP: AC_SFP.*

Zuweisung (FDP_ACF.1.1) *Benannte Gruppe von Sicherheitsattributen: USER_GROUP.*

Zuweisung (FDP_ACF.1.2) *Vorschriften für den Zugriff durch/auf kontrollierte Subjekte und kontrollierte Objekte unter Anwendung von kontrollierten Operationen auf kontrollierte Objekte:*

GENERAL_READ	Die Benutzerdaten darf jeder beliebige Benutzer aus dem PO lesen, mit Ausnahme der Karteninhaberdaten, die nur durch die VEHICLE_UNIT aus Kontrollkarten gelesen werden dürfen.
IDENTIF_WRITE	Kenndaten dürfen nur einmal und vor Ende der Phase 6 des Lebenszyklus der Karte geschrieben werden. Während der Endphase des Lebenszyklus der Karte darf kein Benutzer die Kenndaten schreiben oder ändern.
ACTIVITY_WRITE	Tätigkeitsdaten dürfen nur durch die VEHICLE_UNIT in das PO geschrieben werden.
SOFT_UPGRADE	Ein Upgrading der PO-Software durch Benutzer ist nicht gestattet.
FILE_STRUCTURE	Dateistruktur und -zugriffsbedingungen werden vor dem Ende der Phase 6 des Lebenszyklus des PO geschaffen und anschließend gegen jegliche spätere Änderung oder Löschung durch Benutzer gesperrt.

4.4. Zuordnungsmöglichkeit

ACT_301 Das PO muss die Kenndaten dauerhaft gespeichert halten.

ACT_302 Uhrzeit und Datum der Personalisierung des PO werden angegeben. Diese Angaben sind von einer Änderung ausgeschlossen.

4.5. Audit

Die PO muss Ereignisse, die auf eine potentielle Sicherheitsverletzung des PO hindeuten, überwachen.

Zuweisung (FAU_SAA.1.2) *Teilmenge von beschriebenen auditierbaren Ereignissen:*

- fehlgeschlagene Karteninhaberauthentisierung (5 aufeinander folgende erfolglose PIN-Prüfungen),
- Fehler beim Selbsttest,
- Speicherdatenintegritätsfehler,
- Integritätsfehler bei der Eingabe von Tätigkeitsdaten.

4.6. Genauigkeit**4.6.1. Speicherdatenintegrität**

Zuweisung (FDP_SDI.2.2) *Vorzunehmende Handlungen: Warnung der angeschlossenen Geräteeinheit.*

4.6.2. Basisdatenauthentisierung

Zuweisung (FDP_DAU.1.1) *Liste von Objekten bzw. Informationsarten: Tätigkeitsdaten.*

Zuweisung (FDP_DAU.1.2) *Liste von Subjekten: beliebige.*

4.7. **Zuverlässigkeit während des Betriebs**

4.7.1. *Prüfungen*

Auswahl (FPT_TST.1.1): beim ersten Einschalten sowie regelmäßig während des normalen Betriebs.

Hinweis: ‚Beim ersten Einschalten‘ bedeutet: bevor der Code ausgeführt wird (und nicht notwendigerweise während Antwort auf Rücksetzverfahren).

RLB_301 Die Selbsttests des PO beinhalten die Integritätsfeststellung eines jeglichen nicht im ROM abgelegten Softwarecodes.

RLB_302 Bei Erkennen eines Fehlers während der Selbstprüfung warnt die TSF die angeschlossene Geräteeinheit.

RLB_303 Nach Abschluss der OS-Prüfung werden alle speziellen Prüfbefehle und -handlungen deaktiviert bzw. entfernt. Es darf nicht möglich sein, diese Steuerungen zu überschreiben und zur erneuten Verwendung zu reaktivieren. Ausschließlich auf ein bestimmtes Lebenszyklusstadium bezogene Befehle dürfen nie während eines anderen Stadiums zugreifbar sein.

4.7.2. *Software*

RLB_304 Es darf keine Möglichkeit gegeben sein, die Software des PO bei der Praxisanwendung zu analysieren, auszuprüfen oder abzuändern.

RLB_305 Eingaben aus externen Quellen dürfen als Ausführungscode nicht akzeptiert werden.

4.7.3. *Stromversorgung*

RLB_306 Bei Unterbrechungen bzw. der Stromversorgung bzw. bei Stromschwankungen verbleibt das PO im Sicherheitsstatus.

4.7.4. *Rücksetzbedingungen*

RLB_307 Bei einer Unterbrechung der Stromversorgung (bzw. bei Stromschwankungen) am PO, beim Abbruch einer Transaktion vor deren Vollendung bzw. bei Vorliegen jeder sonstigen Rücksetzbedingung muss das PO sauber zurückgesetzt werden.

4.8. **Datenaustausch**

4.8.1. *Datenaustausch mit einer Fahrzeugeinheit*

DEX_301 Das PO prüft die Integrität und Authentizität der von einer Fahrzeugeinheit importierten Daten.

DEX_302 Bei Erkennen eines Integritätsfehlers der importierten Daten wird das PO:

- die datenexportierende Geräteeinheit warnen,
- die Daten nicht verwenden.

DEX_303 Das PO exportiert die Daten mit den zugehörigen Sicherheitsattributen an die Fahrzeugeinheit, so dass die Fahrzeugeinheit die Integrität und Authentizität der empfangenen Daten ebenfalls prüfen kann.

4.8.2. *Export von Daten an eine Nicht-Fahrzeugeinheit (Übertragungsfunktion)*

DEX_304 Das PO muss in der Lage sein, für an externe Datenträger übertragene Daten einen Herkunftsnachweis zu generieren.

DEX_305 Das PO muss in der Lage sein, dem Empfänger der übertragenen Daten eine Fähigkeit zur Prüfung des Herkunftsnachweises bereitzustellen.

DEX_306 Das PO muss in der Lage sein, die Daten mit den zugehörigen Sicherheitsattributen an den externen Datenträger zu exportieren, so dass sich Integrität und Authentizität der übertragenen Daten prüfen lassen.

4.9. **Kryptografische Unterstützung**

CSP_301 Falls die TSF kryptografische Schlüssel generiert, müssen diese genau festgelegten Schlüsselgenerierungsalgorithmen und genau festgelegten Schlüsselgrößen entsprechen. Die generierten kryptografischen Sitzungsschlüssel dürfen nur begrenzt oft (vom Hersteller noch festzulegen, jedoch höchstens 240mal) verwendbar sein.

CSP_302 Falls die TSF kryptografische Schlüssel vergibt, muss dies nach genau festgelegten Schlüsselvergabemethoden erfolgen.

5. **Beschreibung der Sicherheitsmechanismen**

Die geforderten Sicherheitsmechanismen werden in Anlage 11 beschrieben.

Alle sonstigen Sicherheitsmechanismen werden durch die Hersteller des PO festgelegt.

6. Mindestrobustheit der Sicherheitsmechanismen

Die Mindestrobustheit der Sicherheitsmechanismen der Fahrzeugeinheit ist Hoch, gemäß Definition in ITSEC.

7. Gewährleistungsebene

Die für die Kontrollgerätkarte vorgegebene Gewährleistungsebene ist die ITSEC-Ebene E3, gemäß Definition in ITSEC.

8. Grundlegendes Prinzip

Aus der folgenden Matrix ist das Prinzip der zusätzlichen SEF ersichtlich. Hierzu wird verdeutlicht:

- welche SEF welchen Sicherheitsgefährdungen entgegenwirken,
- welche SEF welche IT-Sicherheitsziele erfüllen.

	Sicherheitsgefährdungen										IT-Zielsetzungen									
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Kenndaten	Tätigkeitsdaten	Datenaustausch	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Datenzugriff	Gesicherte Kommunikation
UIA_301 Authentisierungsmittel																			x	
UIA_302 PIN-Prüfungen																			x	
ACT_301 Kenndaten																				
ACT_302 Personalisierungszeitpunkt																				
RLB_301 Softwareintegrität												x		x						
RLB_302 Selbsttests												x		x						
RLB_303 Herstellungsprüfungen					x	x						x		x						
RLB_304 Softwareanalyse					x		x	x				x		x						
RLB_305 Softwareeingabe					x	x		x				x		x						
RLB_306 Stromversorgung									x	x		x		x						
RLB_307 Rücksetzen												x		x						
DEX_301 Gesicherter Datenimport											x									x
DEX_302 Gesicherter Datenimport											x									x
DEX_303 Gesicherter Datenexport an FE											x									x
DEX_304 Herkunftsnachweis												x								x
DEX_305 Herkunftsnachweis												x								x
DEX_306 Gesicherter Datenexport an externe Datenträger												x								x
CSP_301 Schlüsselgenerierung												x								x
CSP_302 Schlüsselvergabe												x								x

Anlage 11

GEMEINSAME SICHERHEITSMCHANISMEN

INHALTSVERZEICHNIS

1.	Allgemeines	238
1.1.	Referenzdokumente	238
1.2.	Notationen und Abkürzungen	239
2.	Kryptografische Systeme und Algorithmen	240
2.1.	Kryptografische Systeme	240
2.2.	Kryptografische Algorithmen	240
2.2.1.	RSA-Algorithmus	240
2.2.2.	Hash-Algorithmus	240
2.2.3.	Datenverschlüsselungsalgorithmus	240
3.	Schlüssel und Zertifikate	240
3.1.	Erzeugung und Verteilung der Schlüssel	240
3.1.1.	Erzeugung und Verteilung der RSA-Schlüssel	240
3.1.2.	RSA-Prüf Schlüssel	242
3.1.3.	Schlüssel für Weg-/Geschwindigkeitsgeber	242
3.1.4.	Erzeugung und Verteilung von T-DES-Sitzungsschlüsseln	242
3.2.	Schlüssel	242
3.3.	Zertifikate	242
3.3.1.	Inhalt der Zertifikate	243
3.3.2.	Ausgestellte Zertifikate	244
3.3.3.	Verifizieren und Entpacken der Zertifikate	245
4.	Gegenseitige Authentisierung	245
5.	Vertraulichkeits-, Integrität- und Authentisierungsmechanismen für die Datenübertragung FE-Karte	248
5.1.	Secure Messaging	248
5.2.	Behandlung von Secure-Messaging-Fehlern	249
5.3.	Algorithmus zur Berechnung der kryptografischen Prüfsummen	250
5.4.	Algorithmus zur Berechnung der Kryptogramme für Vertraulichkeits-DOs	250
6.	Digitale Signaturmechanismen beim Herunterladen von Daten	251
6.1.	Erzeugung der Signatur	251
6.2.	Verifizierung der Signatur	251

1. ALLGEMEINES

Diese Anlage enthält die Spezifizierung der Sicherheitsmechanismen zur Gewährleistung

- der gegenseitigen Authentisierung von Fahrzeugeinheiten (FE) und Kontrollgerätkarten, einschließlich der Sitzungsschlüsselvereinbarung,
- der Vertraulichkeit, Integrität und Authentisierung der Daten, die zwischen FE und Kontrollgerätkarten übertragen werden,
- der Integrität und Authentisierung der Daten, die von FE auf externe Speichermedien heruntergeladen werden,
- der Integrität und Authentisierung der Daten, die von Kontrollgerätkarten auf externe Speichermedien heruntergeladen werden.

1.1. Referenzdokumente

Die folgenden Referenzdokumente werden in dieser Anlage herangezogen:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. April 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. Oktober 1998
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Draft 1999
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997. (Informationstechnik — Identifizierungskarten — Identifizierungskarten mit integrierten Schaltkreisen und Kontakten — Teil 4: Übergreifende Austauschbefehle)
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998. (Informationstechnik — Identifizierungskarten mit integrierten Schaltkreisen und Kontakten — Teil 6: Übergreifende Datenelemente)
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999 (Informationstechnik — Identifizierungskarten — Chipkarten mit Kontakten — Teil 8: Übergreifende sicherheitsbezogene Befehle)
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997. (Informationstechnik — Sicherheitsverfahren — Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht — Teil 2: Mechanismen unter Nutzung einer Hash-Funktion)
ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998. (Informationstechnik — Sicherheitsverfahren — Mechanismen zur Authentifizierung von Instanzen — Teil 3: Authentifizierung von Instanzen unter Nutzung eines Algorithmus mit öffentlichem Schlüssel)
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface (Straßenfahrzeuge — Fahrtenschreibersysteme — Teil 3: Schnittstelle Weg- und Geschwindigkeitsgeber)

1.2. Notationen und Abkürzungen

In dieser Anlage werden folgende Notationen und Abkürzungen verwendet:

(K_a, K_b, K_c)	ein Schlüsselbund zur Verwendung durch den Triple Data Encryption Algorithm
CA	Certification Authority (Zertifizierungsstelle)
CAR	Certification Authority Reference (Referenz der Zertifizierungsstelle)
CC	Cryptographic Checksum (kryptografische Prüfsumme)
CG	Cryptogram (Kryptogramm)
CH	Command Header (Befehlskopf)
CHA	Certificate Holder Authorisation (Autorisierung des Zertifikatsinhabers)
CHR	Certificate Holder Reference (Referenz des Zertifikatsinhabers)
D()	Entschlüsselung mit DES
DE	Datenelement
DO	Datenobjekt
d	privater RSA-Schlüssel, privater Exponent
e	öffentlicher RSA-Schlüssel, öffentlicher Exponent
E()	Verschlüsselung mit DES
EQT	Equipment (Gerät)
$Hash()$	Hash-Wert, ein Ergebnis von $Hash$
$Hash$	Hash-Funktion
KID	Key Identifier (Schlüsselbezeichner)
K_m	T-DES-Schlüssel. Hauptschlüssel gemäß ISO 16844-3
$K_{m_{vu}}$	in Fahrzeugeinheiten integrierter T-DES-Schlüssel
$K_{m_{wc}}$	in Werkstattkarten integrierter T-DES-Schlüssel
m	Nachrichtenrepräsentant, eine ganze Zahl zwischen 0 und $n-1$
n	RSA-Schlüssel, Modulus
PB	Padding Bytes (Füllbytes)
PI	Padding Indicator-Byte (Verwendung im Kryptogramm für Vertraulichkeits-DO)
PV	Plain Value (Klarwert)
s	Signaturrepräsentant, eine ganze Zahl zwischen 0 und $n-1$
SSC	Send Sequence Counter (Sendesequenzzähler)
SM	Secure Messaging
TCBC	TDEA-Modus Cipher Block Chaining
TDEA	Triple Data Encryption Algorithm (Triple-Datenverschlüsselungsalgorithmus)
TLV	Tag Length Value (Tag-Längenwert)
FE	Fahrzeugeinheit (Vehicle Unit, VU)
X.C	Zertifikat von Benutzer X, ausgestellt durch eine Zertifizierungsstelle
X.CA	Zertifizierungsstelle von Benutzer X
X.CA.PK ₀ .X.C	Vorgang des Entpackens eines Zertifikats zur Herauslösung eines öffentlichen Schlüssels; es handelt sich um einen Infix-Operator, dessen linker Operand der öffentliche Schlüssel einer Zertifizierungsstelle und dessen rechter Operand das von der Zertifizierungsstelle ausgestellte Zertifikat ist; das Ergebnis ist der öffentliche Schlüssel von Benutzer X, dessen Zertifikat der rechte Operand darstellt

X.PK	öffentlicher RSA-Schlüssel eines Benutzers X
X.PK[I]	RSA-Chiffrierung einer Information I unter Verwendung des öffentlichen Schlüssels von Benutzer X
X.SK	privater RSA-Schlüssel eines Benutzers X
X.SK[I]	RSA-Chiffrierung einer Information I unter Verwendung des privaten Schlüssels von Benutzer X
'xx'	ein Hexadezimalwert
	Verkettungsoperator

2. KRYPTOGRAPHISCHE SYSTEME UND ALGORITHMEN

2.1. Kryptografische Systeme

CSM_001 Fahrzeugeinheiten und Kontrollgerätkarten verwenden ein klassisches RSA-Public-Key-Verschlüsselungssystem, so dass folgende Sicherheitsmechanismen vorliegen:

- Authentisierung zwischen Fahrzeugeinheiten und Karten,
- Übertragung von Triple-DES-Sitzungsschlüsseln zwischen Fahrzeugeinheiten und Kontrollgerätkarten,
- digitale Signatur von Daten, die von Fahrzeugeinheiten oder Kontrollgerätkarten an externe Medien heruntergeladen werden.

CSM_002 Fahrzeugeinheiten und Kontrollgerätkarten verwenden ein symmetrisches Triple-DES-Verschlüsselungssystem, so dass ein Mechanismus für die Datenintegrität während des Benutzerdatenaustauschs zwischen Fahrzeugeinheiten und Kontrollgerätkarten und gegebenenfalls die Vertraulichkeit beim Datenaustausch zwischen Fahrzeugeinheiten und Kontrollgerätkarten gewährleistet sind.

2.2. Kryptografische Algorithmen

2.2.1. RSA-Algorithmus

CSM_003 Der RSA-Algorithmus wird durch folgende Beziehungen vollständig definiert:

$$\begin{aligned} \text{X.SK}[m] &= s = m^d \bmod n \\ \text{X.PK}[s] &= m = s^e \bmod n \end{aligned}$$

Eine ausführlichere Beschreibung der RSA-Funktion findet sich im Referenzdokument PKCS1.

Der im RSA-Algorithmus verwendete Exponent e muss in allen erzeugten RSA-Schlüsseln ungleich 2 sein.

2.2.2. Hash-Algorithmus

CSM_004 Die Mechanismen für die digitale Signatur verwenden den SHA-1-Hash-Algorithmus gemäß Definition im Referenzdokument SHA-1.

2.2.3. Datenverschlüsselungsalgorithmus

CSM_005 DES-gestützte Algorithmen werden im Modus Cipher Block Chaining verwendet.

3. SCHLÜSSEL UND ZERTIFIKATE

3.1. Erzeugung und Verteilung der Schlüssel

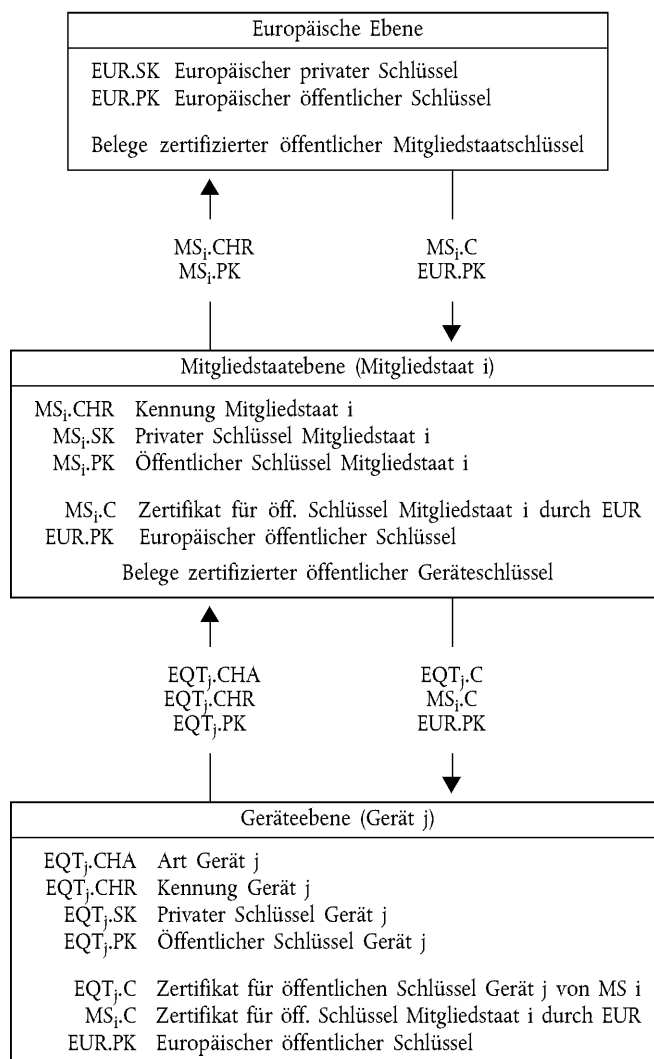
3.1.1. Erzeugung und Verteilung der RSA-Schlüssel

CSM_006 Die Erzeugung der RSA-Schlüssel erfolgt auf drei hierarchischen Funktionsebenen:

- auf europäischer Ebene,
- auf Mitgliedstaatebene,
- auf Geräteebe.

- CSM_007 Auf europäischer Ebene wird ein einziges Schlüsselpaar (EUR.SK und EUR.PK) erzeugt. Der europäische private Schlüssel wird zur Zertifizierung der öffentlichen Schlüssel der Mitgliedstaaten verwendet. Über alle zertifizierten Schlüssel sind Belege aufzubewahren. Diese Aufgaben werden von einer Europäischen Zertifizierungsstelle wahrgenommen, die der Europäischen Kommission untersteht.
- CSM_008 Auf Mitgliedstaatenebene wird ein Mitgliedstaatschlüsselpaar (MS.SK und MS.PK) erzeugt. Öffentliche Mitgliedstaatschlüssel werden von der Europäischen Zertifizierungsstelle zertifiziert. Der private Mitgliedstaatschlüssel wird für die Zertifizierung von öffentlichen Schlüsseln verwendet, die in Geräten (Fahrzeugeinheit oder Kontrollgerätkarte) eingefügt sind. Über alle zertifizierten öffentlichen Schlüssel sind Belege zusammen mit der Kennung des Geräts, für das sie bestimmt sind, aufzubewahren. Diese Aufgaben werden von der Zertifizierungsstelle des jeweiligen Mitgliedstaats wahrgenommen. Ein Mitgliedstaat darf sein Schlüsselpaar in regelmäßigen Abständen ändern.
- CSM_009 Auf Geräteebe wird ein einziges Schlüsselpaar (EQT.SK und EQT.PK) erzeugt und in jedes Gerät eingefügt. Die öffentlichen Geräteschlüssel werden von der Zertifizierungsstelle des jeweiligen Mitgliedstaats zertifiziert. Diese Aufgaben können von Geräteherstellern, Geräteintegratoren und Behörden der Mitgliedstaaten wahrgenommen werden. Dieses Schlüsselpaar wird zur Authentisierung, für die digitale Signatur sowie zur Chiffrierung verwendet.
- CSM_010 Bei der Erzeugung, ggf. bei der Übertragung sowie bei der Speicherung ist die Vertraulichkeit der privaten Schlüssel zu wahren.

Im folgenden Schaubild ist der Datenfluss dieses Prozesses zusammengefasst:



3.1.2. **RSA-Prüfchlüssel**

CSM_011 Zum Zwecke der Geräteprüfung (einschließlich Interoperabilitätsprüfungen) erzeugt die Europäische Zertifizierungsstelle ein anderes einziges europäisches Prüfchlüsselpaar und mindestens zwei Mitgliedstaat-Prüfchlüsselpaare, deren öffentliche Schlüssel mit dem europäischen privaten Prüfchlüssel zertifiziert werden. Von den Herstellern werden in Geräte, die der Bauartgenehmigungsprüfung unterzogen werden, Prüfchlüssel eingefügt, die durch einen dieser Mitgliedstaat-Prüfchlüssel zertifiziert sind.

3.1.3. **Schlüssel für Weg-/Geschwindigkeitsgeber**

Die Geheimhaltung der drei genannten T-DES-Schlüssel ist während der Erzeugung, der Übermittlung und ggf. der Aufbewahrung in geeigneter Weise zu gewährleisten.

Um die Unterstützung von Kontrollgeräten, die der ISO 16844 entsprechen, zu gewährleisten, stellen die Europäische Zertifizierungsstelle und die Zertifizierungsstellen der Mitgliedstaaten darüber hinaus Folgendes sicher:

CSM_036 Europäische Zertifizierungsstelle erzeugt $K_{m_{VU}}$ und $K_{m_{WC}}$ als zwei von einander unabhängige und einmalige Triple-DES-Schlüssel sowie K_m , wobei gilt:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Die Europäische Zertifizierungsstelle übermittelt diese Schlüssel unter geeigneten Sicherheitsvorkehrungen auf deren Anforderung an die Zertifizierungsstellen der Mitgliedstaaten.

CSM_037 Die Zertifizierungsstellen der Mitgliedstaaten:

- verschlüsseln mit K_m die von den Herstellern der Weg-/Geschwindigkeitsgeber angeforderten Weg-/Geschwindigkeitsgeberdaten (die mit K_m zu verschlüsselnden Daten sind ISO 16844-3 festgelegt),
- übermitteln $K_{m_{VU}}$ zum Einbau in die Fahrzeugeinheiten unter geeigneten Sicherheitsvorkehrungen an deren Hersteller,
- stellen sicher, dass $K_{m_{WC}}$ bei der Personalisierung der Karten in alle Werkstattkarten eingefügt wird (`SensorInstallationSecData` in der Grunddatei `Sensor_Installation_Data`).

3.1.4. **Erzeugung und Verteilung von T-DES-Sitzungsschlüsseln**

CSM_012 Im Rahmen des Prozesses der gegenseitigen Authentisierung erzeugen Fahrzeugeinheiten und Kontrollgerätkarten die erforderlichen Daten zur Erstellung eines gemeinsamen Triple-DES-Sitzungsschlüssels und tauschen diese Daten aus. Die Vertraulichkeit dieses Datenaustauschs wird durch einen RSA-Verschlüsselungsmechanismus geschützt.

CSM_013 Dieser Schlüssel wird für alle nachfolgenden kryptografischen Operationen unter Anwendung des Secure Messaging benutzt. Seine Gültigkeit erlischt am Ende der Sitzung (Entnahme oder Zurücksetzen der Karte) und/oder nach 240 Benutzungen (eine Benutzung des Schlüssels = ein mittels Secure Messaging an die Karte gesandter Befehl und die dazugehörige Antwort).

3.2. **Schlüssel**

CSM_014 RSA-Schlüssel haben (ungeachtet der Ebene) folgende Länge: Modulus n 1024 Bit, öffentlicher Exponent e max. 64 Bit, privater Exponent d 1024 Bit.

CSM_015 Triple-DES-Schlüssel haben die Form (K_a, K_b, K_a) , wobei K_a und K_b unabhängige Schlüssel mit einer Länge von 64 Bit sind. Es wird kein Paritätsfehler-Erkennungsbit gesetzt.

3.3. **Zertifikate**

CSM_016 Bei den RSA-Public-Key-Zertifikaten muss es sich um Zertifikate entsprechend der Definition „non self descriptive“ und „card verifiable“ des Referenzdokuments ISO/IEC 7816-8 handeln.

3.3.1. Inhalt der Zertifikate

CSM_017 RSA-Public-Key-Zertifikate sind aus den folgenden Daten in folgender Reihenfolge aufgebaut:

Daten	Format	Bytes	Bemerkung
CPI	INTEGER	1	Certificate Profile Identifier (Zertifikatsprofil '01' in dieser Version)
CAR	OCTET STRING	8	Certification Authority Reference (Referenz der Zertifizierungsstelle)
CHA	OCTET STRING	7	Certificate Holder Authorisation (Autorisierung des Zertifikatsinhabers)
EOV	TimeReal	4	Ablauf der Gültigkeit des Zertifikats, bei Nichtverwendung mit 'FF' gefüllt
CHR	OCTET STRING	8	Certificate Holder Reference (Referenz des Zertifikatsinhabers)
<i>n</i>	OCTET STRING	128	Öffentlicher Schlüssel (Modulus)
<i>e</i>	OCTET STRING	8	Öffentlicher Schlüssel (öffentlicher Exponent)
		164	

Anmerkungen:

1. Mit dem Certificate Profile Identifier (Zertifikatsprofilbezeichner, CPI) wird die genaue Struktur eines Authentisierungszertifikats abgegrenzt. Er kann als interner Gerätebezeichner einer relevanten Kopfliste verwendet werden, die die Verkettung der Datenelemente innerhalb des Zertifikats beschreibt.

Die Kopfliste für diesen Zertifikatsinhalt lautet wie folgt:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Tag für erweiterte Kopfliste	Länge der Kopfliste	CPI-Tag	CPI-Länge	CAR-Tag	CAR-Länge	CHA-Tag	CHA-Länge	EOV-Tag	EOV-Länge	CHR-Tag	CHR-Länge	Tag für öffentlichen Schlüssel (konstruiert)	Länge der folgenden DOS	Modulus-Tag	Modulus-Länge	Tag für öffentlichen Exponenten	Länge des öffentlichen Exponenten

2. „Certification Authority Reference“ (Referenz der Zertifizierungsstelle, CAR) identifiziert die das Zertifikat ausstellende Zertifizierungsstelle so, dass das Datenelement gleichzeitig als Authority Key Identifier (Schlüsselbezeichner der Stelle) zur Angabe des öffentlichen Schlüssels der Zertifizierungsstelle verwendet werden kann (Kodierung siehe „Key Identifier“).
3. Mit „Certificate Holder Authorisation“ (Autorisierung des Zertifikatsinhabers, CHA) wird die Berechtigung des Zertifikatsinhabers ausgewiesen. Sie besteht aus der Kontrollgerätenanwendungs-ID sowie aus der Art des Geräts, für das das Zertifikat bestimmt ist (entsprechend dem Datenelement *EquipmentType*, „00“ für einen Mitgliedstaat).
4. „Certificate Holder Reference“ (Referenz des Zertifikatsinhabers, CHR) dient der eindeutigen Identifizierung des Zertifikatsinhabers, so dass das Datenelement gleichzeitig als „Subject Key Identifier“ (Schlüsselbezeichner des Subjekts) zur Angabe des öffentlichen Schlüssels des Zertifikatsinhabers verwendet werden kann.
5. „Key Identifiers“ (Schlüsselbezeichner, KID) dienen der eindeutigen Identifizierung des Zertifikatsinhabers oder der Zertifizierungsstellen. Sie sind wie folgt kodiert:

5.1. Gerät (FE oder Karte):

Daten	Seriennummer Gerät	Datum	Art	Hersteller
Länge	4 Byte	2 Byte	1 Byte	1 Byte
Wert	Ganze Zahl	MM JJ BCD-Kod.	Herstellerspezifisch	Herstellercode

Dem Hersteller einer FE ist die Kennung des Geräts, in das die Schlüssel eingefügt werden, bei der Beantragung von Zertifikaten unter Umständen nicht bekannt.

Ist dem Hersteller die Geräteerkennung bekannt, sendet er sie mit dem öffentlichen Schlüssel zwecks Zertifizierung an die Zertifizierungsstelle seines Mitgliedstaats. Das Zertifikat enthält dann die Geräteerkennung, und der Hersteller muss sicherstellen, dass Schlüssel und Zertifikat in das vorgesehene Gerät eingefügt werden. Der Key Identifier weist die obengenannte Form auf.

Ist dem Hersteller die Geräteerkennung nicht bekannt, muss er jeden Antrag auf ein Zertifikat eindeutig kennzeichnen und diese Kennung zusammen mit dem öffentlichen Schlüssel zwecks Zertifizierung an die Zertifizierungsstelle seines Mitgliedstaats senden. Das Zertifikat enthält dann die Antragskennung. Nach dem Einfügen der Schlüssel in das Gerät muss der Hersteller der Zertifizierungsstelle die Zuordnung des Schlüssels zum Gerät mitteilen (d. h. Kennung des Zertifikatsantrags, Geräteerkennung). Der Key Identifier (KID) hat folgende Form:

Daten	Seriennummer Zertifikatsantrag	Datum	Art	Hersteller
Länge	4 Byte	2 Byte	1 Byte	1 Byte
Wert	BCD-Kodierung	MM JJ BCD-Kod.	'FF'	Herstellercode

5.2. Zertifizierungsstelle:

Daten	Kennung	Seriennr. Schlüssel	Zusatzinfo	Bezeichner
Länge	4 Byte	1 Byte	2 Byte	1 Byte
Wert	1 Byte numerischer Landescode 3 Byte alphanumerischer Landescode	Ganze Zahl	Zusatzkodierung (CA-spezifisch) 'FF FF' bei Nichtverwendung	'01'

Mit der Seriennummer Schlüssel werden die verschiedenen Schlüssel eines Mitgliedstaates unterschieden, sofern der Schlüssel verändert wird.

- Den Zertifikatsprüfern ist implizit bekannt, dass es sich bei dem zertifizierten Schlüssel um einen für die Authentisierung, für die Verifizierung der digitalen Signatur und für die vertrauliche Chiffrierung relevanten RSA-Schlüssel handelt (das Zertifikat enthält keine Objektkennung zur entsprechenden Spezifizierung).

3.3.2. Ausgestellte Zertifikate

CSM_018 Das ausgestellte Zertifikat ist eine digitale Signatur mit teilweiser Wiederherstellung des Zertifikatsinhalts gemäß ISO/IEC 9796-2 mit angefügter ‚Certification Authority Reference‘.

$$X.C = X.CA.SK['6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

wobei Zertifikatsinhalt $= Cc =$ $\begin{matrix} C_r & || & C_n \\ 106 \text{ Byte} & & 58 \text{ Byte} \end{matrix}$

Anmerkungen:

- Dieses Zertifikat ist 194 Byte lang.
- Die von der Signatur verdeckte CAR wird ebenfalls an die Signatur angefügt, so dass der öffentliche Schlüssel der Zertifizierungsstelle zur Verifizierung des Zertifikats gewählt werden kann.
- Dem Zertifikatsprüfer ist der von der Zertifizierungsstelle für die Unterzeichnung des Zertifikats verwendete Algorithmus implizit bekannt.

4. Die zu dem ausgestellten Zertifikat gehörende Kopfliste lautet wie folgt:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Tag für CV-Zertifikat (konstruiert)	Länge der folgenden DOs	Signatur-Tag	Signaturlänge	Rest-Tag	Restlänge	CAR-Tag	CAR-Länge

3.3.3. Verifizieren und Entpacken der Zertifikate

Das Verifizieren und Entpacken der Zertifikate besteht in der Verifizierung der Signatur entsprechend ISO/IEC 9796-2, wodurch der Zertifikatsinhalt und der enthaltene öffentliche Schlüssel aufgerufen werden: $X.PK = X.CA.PK_o X.C$, sowie in der Verifizierung der Gültigkeit des Zertifikats.

CSM_019 Dazu gehören folgende Schritte:

Verifizierung der Signatur und Abrufen des Inhalts:

- von X.C Abruf von Sign, C_n' y CAR': $X.C = \begin{matrix} \text{Sign} \\ 128 \text{ Byte} \end{matrix} \parallel \begin{matrix} C_n' \\ 58 \text{ Byte} \end{matrix} \parallel \begin{matrix} \text{CAR}' \\ 8 \text{ Byte} \end{matrix}$
- von CAR' Auswahl des entsprechenden öffentlichen Schlüssels der Zertifizierungsstelle (wenn nicht bereits zuvor durch andere Mittel erfolgt),
- Öffnen von Sign mit öffentlichem CA-Schlüssel: $Sr' = X.CA.PK [Sign]$,
- Prüfung Sr' beginnt mit '6A' und endet mit 'BC'
- Berechnung von Cr' und H' : $Sr' = \begin{matrix} '6A' \\ 106 \text{ Byte} \end{matrix} \parallel \begin{matrix} C_r' \\ 106 \text{ Byte} \end{matrix} \parallel \begin{matrix} H' \\ 20 \text{ Byte} \end{matrix} \parallel \begin{matrix} 'BC' \end{matrix}$
- Wiederherstellung des Zertifikatsinhalts $C_r' \parallel C_n'$,
- Prüfung $Hash(C') = H'$

Sind die Prüfungen positiv, ist das Zertifikat echt und sein Inhalt ist C' .

Verifizierung der Gültigkeit. Von C' :

- Prüfung des Ablaufdatums der Gültigkeit, wenn zutreffend,

Abruf und Speicherung des öffentlichen Schlüssels, des Key Identifier, der Certificate Holder Authorisation und des Ablaufs der Gültigkeit des Zertifikats von C' :

- $X.PK = n \parallel e$
- $X.KID = CHR$
- $X.CHA = CHA$
- $X.EOV = EOVS$

4. GEGENSEITIGE AUTHENTISIERUNG

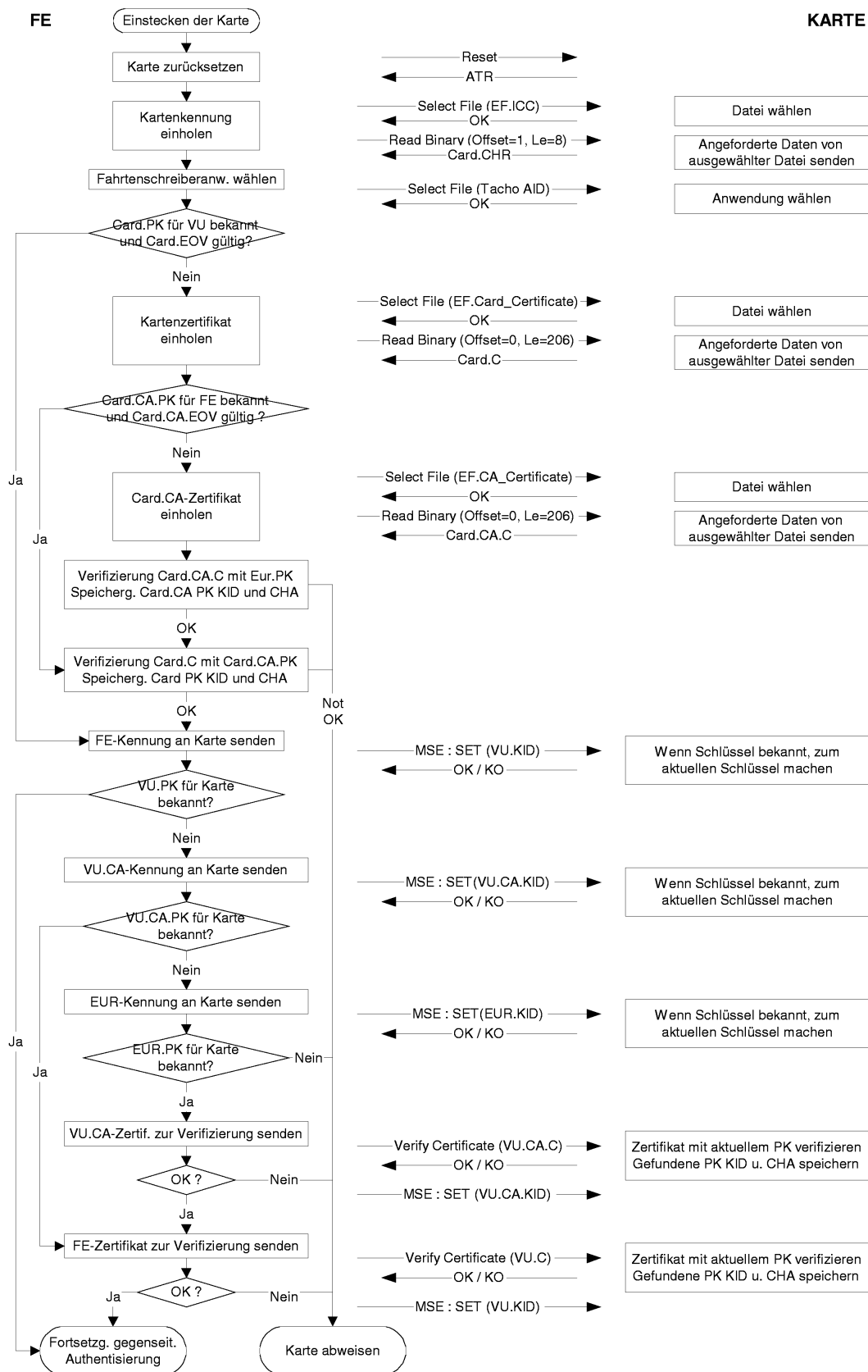
Die gegenseitige Authentisierung zwischen Karten und FE beruht auf dem folgenden Prinzip:

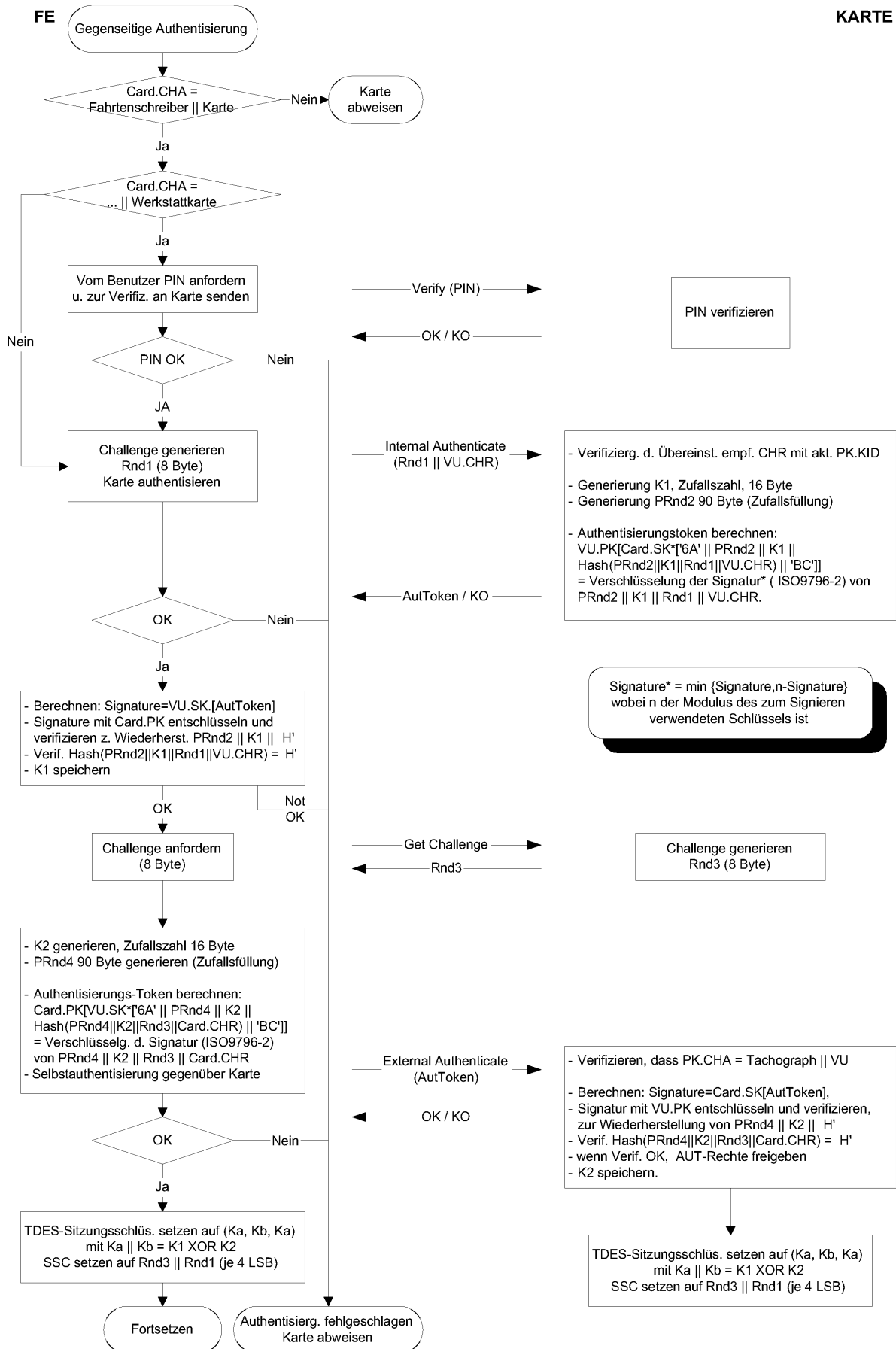
Jede Seite weist der Gegenseite nach, dass sie sich im Besitz eines gültigen Schlüsselpaares befindet, dessen öffentlicher Schlüssel von der Zertifizierungsstelle des jeweiligen Mitgliedstaats zertifiziert worden ist, die wiederum von der europäischen Zertifizierungsstelle zertifiziert wurde.

Der Nachweis wird geführt, indem mit dem privaten Schlüssel eine von der Gegenseite gesandte Zufallszahl signiert wird; die Gegenseite muss bei der Verifizierung dieser Signatur die Zufallszahl wiederherstellen können.

Der Mechanismus wird von der FE beim Einstecken der Karte ausgelöst. Er beginnt mit dem Austausch der Zertifikate und dem Entpacken der öffentlichen Schlüssel und endet mit der Erzeugung eines Sitzungsschlüssels.

CSM_020 Folgendes Protokoll findet Verwendung (Pfeile weisen auf Befehle und ausgetauschte Daten hin, siehe Anlage 2):





5. VERTRAULICHKEITS-, INTEGRITÄTS- UND AUTHENTISIERUNGSMECHANISMEN FÜR DIE DATENÜBERTRAGUNG FE-KARTE

5.1. Secure Messaging

- CSM_021 Die Integrität der Datenübertragung zwischen FE und Karte wird durch Secure Messaging entsprechend den Referenzdokumenten ISO/IEC 7816-4 und ISO/IEC 7816-8 geschützt.
- CSM_022 Müssen Daten während der Übertragung geschützt werden, wird den innerhalb des Befehls oder der Antwort gesandten Datenobjekten ein Datenobjekt „Cryptographic Checksum“ angefügt. Diese kryptografische Prüfsumme wird vom Empfänger verifiziert.
- CSM_023 Die kryptografische Prüfsumme der innerhalb eines Befehls gesandten Daten integriert den Befehlskopf sowie alle gesandten Datenobjekte (= > CLA = '0C', und alle Datenobjekte sind mit Tags zu kapseln, bei denen b1=1).
- CSM_024 Die Statusinformationsbytes der Antwort sind durch eine kryptografische Prüfsumme zu schützen, wenn die Antwort kein Datenfeld enthält.
- CSM_025 Kryptografische Prüfsummen sind 4 Byte lang.

Somit weisen Befehle und Antworten bei Anwendung von Secure Messaging folgende Struktur auf:

Die DO werden als Teilmenge der in ISO/IEC 7816-4 beschriebenen Secure-Messaging-DOs verwendet:

Tag	Mnemonik	Bedeutung
'81'	T _{PV}	Klarwert, nicht in BER-TLV kodiert (durch CC zu schützen)
'97'	T _{LE}	Wert von Le im ungesicherten Befehl (durch CC zu schützen)
'99'	T _{SW}	Status-Info (durch CC zu schützen)
'8E'	T _{CC}	Kryptografische Prüfsumme (CC)
'87'	T _{PI CG}	Padding Indicator Byte Cryptogram (Klarwert, nicht in BER-TLV kodiert)

Ausgehend von einem ungesicherten Befehl-Antwort-Paar:

Befehlskopf	Befehlskörper
CLA INS P1 P2	[L _c -Feld] [Datenfeld] [L _e -Feld]
vier Byte	L Byte, bezeichnet als B ₁ bis B _L

Antwortkörper	Antwortendmarke
[Datenfeld]	SW1 SW2
L _r Datenbyte	zwei Byte

lautet das entsprechende gesicherte Befehl-Antwort-Paar:

Gesicherter Befehl:

Befehlskopf (CH)	Befehlskörper										
CLA INS P1 P2	[Neues L _c -Feld]	[Neues Datenfeld]									[L _e -Feld neu]
'0C'	Länge des neuen Datenfelds	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'
		'81'	L _c	Datenfeld	'97'	'01'	L _e	'8E'	'04'	CC	

In die Prüfsumme zu integrierende Daten = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_c || PB

PB = Padding Bytes (80 .. 00) gemäß ISO-IEC 7816-4 und ISO 9797, Methode 2.

Die PV und LE der DO sind nur vorhanden, wenn entsprechende Daten im ungesicherten Befehl vorliegen.

Gesicherte Antwort:

1. Wenn das Antwortdatenfeld nicht leer ist und vertraulichkeitsgeschützt werden muss:

Antwortkörper						Antwortendmarke
[Neues Datenfeld]						SW1 SW2 neu
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	Datenfeld	'8E'	'04'	CC	

In die Prüfsumme zu integrierende Daten = T_{PI CG} || L_{PI CG} || PI CG || PB

2. Wenn das Antwortdatenfeld nicht leer ist und vertraulichkeitsgeschützt werden muss:

Antwortkörper						Antwortendmarke
[Neues Datenfeld]						SW1 SW2 neu
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Daten in CG: nicht-BER-TLV-kodierte Daten und Füllbytes.

In die Prüfsumme zu integrierende Daten = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Wenn das Antwortdatenfeld leer ist:

Antwortkörper						Antwortendmarke
[Neues Datenfeld]						SW1 SW2 neu
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	SW1 SW2 neu	'8E'	'04'	CC	

In die Prüfsumme zu integrierende Daten = T_{SW} || L_{SW} || SW || PB

5.2. Behandlung von Secure-Messaging-Fehlern

CSM_026 Erkennt die Kontrollgerätkarte beim Interpretieren eines Befehls einen SM-Fehler, müssen die Status-Bytes ohne SM zurückgesandt werden. Laut ISO/IEC 7816-4 sind folgende Status-Bytes zur Anzeige von SM-Fehlern definiert:

'66 88' Verifizierung der kryptografischen Prüfsumme fehlgeschlagen,

'69 87' erwartete SM-Datenobjekte fehlen,

'69 88' SM-Datenobjekte inkorrekt.

CSM_027 Sendet die Kontrollgerätkarte Status-Bytes ohne SM-DO oder mit einem fehlerhaften SM-DO zurück, muss die FE den Vorgang abbrechen.

5.3. Algorithmus zur Berechnung der kryptografischen Prüfsummen

CSM_028 Kryptografische Prüfsummen werden unter Verwendung eines üblichen MAC gemäß ANSI X9.19 mit DES aufgebaut:

- Ausgangsstufe: Der Ausgangsprüfblock y_0 ist $E(K_a, SSC)$.
- Folgestufe: Unter Verwendung von K_a werden die Prüfböcke $y_1, \dots, y_n$ berechnet.
- Endstufe: Die kryptografische Prüfsumme wird aus dem letzten Prüfblock y_n wie folgt berechnet: $E(K_a, D(K_b, y_n))$.

$E()$ bedeutet Verschlüsselung mit DES, und $D()$ bedeutet Entschlüsselung mit DES.

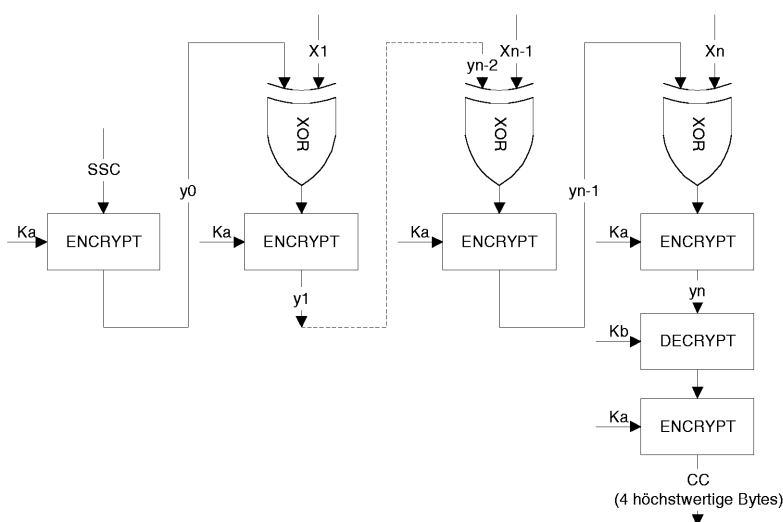
Die vier höchstwertigen Bytes der kryptografischen Prüfsumme werden übertragen.

CSM_029 Während der Schlüsselvereinbarung wird der 'Send Sequence Counter' (Sendesequenzzähler, SSC) wie folgt initialisiert:

Anfangs-SSC: Rnd3 (4 niedrigstwertige Bytes) || Rnd1 (4 niedrigstwertige Bytes).

CSM_030 Vor jeder Berechnung eines MAC wird der SSC um 1 erhöht (d. h. der SSC für den ersten Befehl ist Anfangs-SSC + 1, der SSC für die erste Antwort Anfangs-SSC + 2).

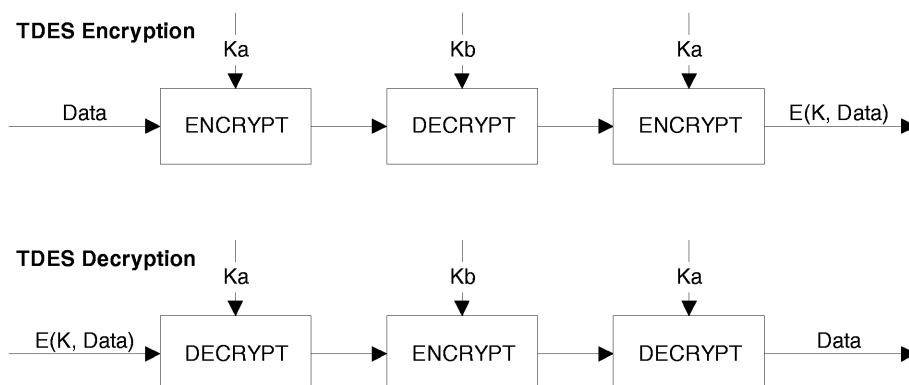
Die folgende Abbildung zeigt die Berechnung des MAC:



5.4. Algorithmus zur Berechnung von Kryptogrammen für Vertraulichkeits-DOs

CSM_031 Kryptogramme werden mit TDEA im Modus TCBC entsprechend den Referenzdokumenten TDES und TDES-OP sowie mit dem Nullvektor als Initial Value-Block berechnet.

Die folgende Abbildung zeigt die Anwendung von Schlüsseln in TDES:



6. DIGITALE SIGNATURMECHANISMEN BEIM HERUNTERLADEN VON DATEN

CSM_032 Das Intelligent Dedicated Equipment (IDE) speichert die von einem Gerät (FE oder Karte) während eines Übertragungsvorgangs empfangenen Daten in einer Datei ab. Diese Datei muss die Zertifikate MS_i.C und EQT.C enthalten. Die Datei enthält digitale Signaturen von Datenblöcken gemäß Anlage 7, Protokolle zum Herunterladen der Daten.

CSM_033 Für die digitalen Signaturen heruntergeladener Daten wird ein digitales Signatursystem mit Anhang verwendet, so dass die heruntergeladenen Daten auf Wunsch ohne Dechiffrierung lesbar sind.

6.1. Erzeugung der Signatur

CSM_034 Die Erzeugung der Datensignatur durch das Gerät folgt dem in Referenzdokument PKCS1 definierten digitalen Signatursystem mit Anhang und der Hash-Funktion SHA-1:

$$\text{Signatur} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel \text{PS} \parallel \text{'00'} \parallel \text{DER}(\text{SHA-1}(\text{Data}))]$$

PS = Füllstring von Oktetten mit Wert 'FF', so dass die Länge 128 beträgt.

DER(SHA-1(M)) ist die Kodierung des Algorithmus-ID für die Hash-Funktion und den Hash-Wert in einen ASN.1-Wert des Typs *DigestInfo* (Kodierungsregeln):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || Hash-Wert.

6.2. Verifizierung der Signatur

CSM_035 Die Verifizierung der Datensignatur bei heruntergeladenen Daten folgt dem in Referenzdokument PKCS1 definierten digitalen Signatursystem mit Anhang und der Hash-Funktion SHA-1.

Der europäische Schlüssel EUR.PK muss dem Prüfer von unabhängiger Seite her (für ihn verlässlich) bekannt sein.

Die folgende Tabelle veranschaulicht das Protokoll, das von einem IDE mit Kontrollkarte zur Verifizierung der Integrität von heruntergeladenen und in ESM (externen Speichermedien) gespeicherten Daten herangezogen werden kann. Die Kontrollkarte wird zur Dechiffrierung digitaler Signaturen verwendet. Diese Funktion kann in diesem Fall nicht im IDE implementiert sein.

Das Gerät, das die zu analysierenden Daten heruntergeladen und signiert hat, ist mit EQT bezeichnet.

