Rat der
Europäischen Union

Brüssel, den 14. März 2019
(OR. en)

7510/19
ADD 3

TRANS 199
DELACT 68

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	C(2019) 1789 final - Annex 3
Betr.:	ANHANG der Delegierten Verordnung der Kommission zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates im Hinblick auf die Einführung und den Betrieb kooperativer intelligenter Verkehrssysteme

Die Delegationen erhalten in der Anlage das Dokument C(2019) 1789 final - Annex 3.

Anl.: C(2019) 1789 final - Annex 3

EUROPÄISCHE
KOMMISSION

Brüssel, den 13.3.2019
C(2019) 1789 final

ANNEX 3

ANHANG

der

Delegierten Verordnung der Kommission

zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates im Hinblick auf die Einführung und den Betrieb kooperativer intelligenter Verkehrssysteme

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

INHALTSVERZEICHNIS

ANHANG III

1. EINLEITUNG

1.1. Überblick und Anwendungsbereich der Certificate Policy

In der vorliegenden Certificate Policy wird das europäische C-ITS Trust Model auf der Grundlage einer Public Key Infrastruktur (PKI) definiert, das in den Anwendungsbereich des Systems für das Management von Sicherheitsberechtigungsnachweisen von C-ITS-Diensten in der EU (EU C-ITS security credential management system, EU-CCMS) fällt. Festgelegt werden Anforderungen für das Management von Anträgen auf Public-Key-Zertifikate durch ausstellende Teilnehmer und deren Nutzung durch Endteilnehmer in Europa. Auf ihrer höchsten Ebene setzt sich eine PKI aus einer Reihe von Root-CA zusammen, die „aktiviert“ wurden, nachdem sie vom Trust List Manager (Manager der Liste vertrauenswürdiger Zertifikate, TLM) auf eine European Certificate Trust List (europäische Liste vertrauenswürdiger Zertifikate, ECTL) gesetzt wurden; diese Liste wird vom TLM der zentralen Teilnehmerstelle herausgegeben und veröffentlicht (siehe die Abschnitte 1.2 und 1.3).

Diese Certificate Policy ist für alle Teilnehmer verbindlich, die an dem vertrauenswürdigen C-ITS-System in Europa beteiligt sind. Sie hilft bei der Bewertung des Niveaus an Vertrauen, das Empfänger von durch ein Endteilnehmerzertifikat der PKI authentifizierten Nachrichten in die empfangenen Informationen setzen können. Um eine Bewertung der Vertrauenswürdigkeit der vom EU-CCMS zur Verfügung gestellten Zertifikate zu ermöglichen, legt die Certificate Policy verbindliche Anforderungen für den Betrieb des TLM der zentralen Teilnehmerstelle sowie für die Erstellung und Verwaltung der ECTL fest. Dementsprechend werden in diesem Dokument folgende Aspekte im Zusammenhang mit der ECTL behandelt:

- Identifizierung und Authentifizierung von Vollmachtgebern, die PKI-Funktionen für den TLM übernehmen, einschließlich der Erklärungen über die jeder Rolle zugewiesenen Rechte;
- Mindestanforderungen an die lokale Sicherheitspraxis für den TLM, einschließlich physischer, personeller und verfahrenstechnischer Kontrollen;
- Mindestanforderungen an die technische Sicherheitspraxis des TLM, einschließlich der Computersicherheit, der Netzsicherheit und der kryptografischen Module für die technischen Kontrollen;
- Mindestanforderungen für die betriebliche Praxis des TLM, einschließlich der Registrierung neuer Root-CA-Zertifikate, der vorübergehenden oder ständigen Abmeldung bestehender, eingeschlossener CA und der Veröffentlichung und Verbreitung von ECTL-Aktualisierungen;
- ein ECTL-Profil, einschließlich aller obligatorischen und optionalen Datenfelder der ECTL, der zu verwendenden kryptografischen Algorithmen, des genauen ECTL-Formats und der Empfehlungen für die Verarbeitung der ECTL;
- das Lebenszyklusmanagement von ECTL-Zertifikaten, einschließlich Verteilung, Aktivierung, Ablauf und Sperrung von ECTL-Zertifikaten;

- gegebenenfalls die Verwaltung von vertrauensbezogenen Sperrungen von Root-CA.

Da die Vertrauenswürdigkeit der ECTL nicht allein von der ECTL selbst abhängt, sondern weitgehend auch von den Root-CA und Sub-CA, aus denen sich die PKI zusammensetzt, werden in der vorliegenden Certificate Policy auch für alle teilnehmenden CA (Root-CA und Sub-CA) obligatorische Mindestanforderungen festgelegt. Es handelt sich um folgende Anforderungsgebiete:

- Identifizierung und Authentifizierung von Vollmachtgebern, die PKI-Funktionen für den TLM übernehmen (z. B. Sicherheitsbeauftragte, Datenschutzbeauftragte, Sicherheitsadministratoren, Verzeichnisadministratoren und Endnutzer), einschließlich einer Erklärung der Pflichten, Verantwortlichkeiten, Haftungen und Rechten, die mit den einzelnen Funktionen verbunden sind;
- Schlüsselmanagement einschließlich akzeptabler, obligatorischer Algorithmen für die Signatur von Zertifikaten, die Signatur von Daten und Gültigkeitszeiträume von Zertifikaten;
- Mindestanforderungen an lokale Sicherheitspraktiken, einschließlich physischer, personeller und verfahrenstechnischer Kontrollen;
- Mindestanforderungen an technische Sicherheitspraktiken wie Computersicherheit, Netzsicherheit und technische Kontrollen im Bereich der kryptografischen Module;
- Mindestanforderungen für die betriebliche Praxis der CA, EA, AA und Endteilnehmer, unter Einschluss von Aspekten der Registrierung, der Abmeldung (d. h. Streichung aus der Liste), Sperrung, Kompromittierung von Schlüsseln, Kündigung aus wichtigem Grund, Aktualisierung von Zertifikaten, Auditpraktiken und Nichtoffenlegung datenschutzbezogener Informationen;
- Zertifikat und CRL-Profil, unter Einschluss von Formaten, akzeptablen Algorithmen, obligatorischen und optionalen Datenfeldern sowie deren gültige Wertebereiche, sowie Angaben dazu, wie die Prüfer die Zertifikate bearbeiten sollen;
- regelmäßige Überwachung, Meldung, Warnung und Wiederherstellung der Aufgaben der Teilnehmer des C-ITS Trust Models, um auch im Fall von Fehlverhalten einen sicheren Betrieb zu gewährleisten.

Zusätzlich zu diesen Mindestanforderungen können die Stellen, die die Root-CA und Sub-CA betreiben, ihre eigenen, zusätzlichen Anforderungen beschließen und in den maßgeblichen Erklärungen zum Zertifizierungsbetrieb (CPS) darlegen, sofern diese nicht den in der Certificate Policy festgelegten Anforderungen widersprechen. Einzelheiten dazu, wie Erklärungen zum Zertifizierungsbetrieb geprüft und veröffentlicht werden, sind Abschnitt 1.5 zu entnehmen.

In der Certificate Policy werden auch die Zwecke genannt, zu denen die Root-CA, Sub-CA und deren herausgegebene Zertifikate eingesetzt werden können. Darin sind die Haftungen aufgeführt, die von folgenden Stellen übernommen werden:

- dem TLM;
- jeder Root-CA, deren Zertifikate in der ECTL aufgeführt sind;

- den Sub-CA der Root-CA (EA und AA);
- alle Mitglieder oder Organisationen, die für einen der Teilnehmer des C-ITS Trust Models verantwortlich sind oder diesen betreiben.

In der Certificate Policy sind auch verbindliche Verpflichtungen festgelegt, die für Folgendes gelten:

- den TLM;
- jeder Root-CA, deren Zertifikate in der ECTL aufgeführt sind;
- jede von einer Root-CA zertifizierte Sub-CA;
- alle Endteilnehmer;
- alle Mitgliedsorganisationen, die für einen der Teilnehmer des C-ITS Trust Models verantwortlich sind oder diesen betreiben.

Schließlich legt die Certificate Policy Anforderungen in Bezug auf die Dokumentation von Beschränkungen der Haftung und Verpflichtungen in der Erklärung zum Zertifizierungsbetrieb (CPS) jeder Root-CA fest, deren Zertifikate in der ECTL aufgeführt werden.

Die vorliegende Certificate Policy steht im Einklang mit dem von der Internet Engineering Task Force (IETF) angenommenen Rahmen für Zertifizierungsregeln und Zertifizierungsverfahren [3].

1.2. Begriffsbestimmungen und Abkürzungen

Es gelten die Begriffsbestimmungen in [2], [3] und [4].

AA	authorisation authority (Genehmigungsstelle)
AT	authorisation ticket (Berechtigungsticket)
CA	certification authority (Zertifizierungsstelle]
CP	Certificate Policy
CPA	C-ITS certificate policy authority (für die C-ITS Certificate Policy zuständige Stelle)
CPOC	C-ITS point of contact (C-ITS-Kontaktstelle)
CPS	certificate practice statement (Erklärung zum Zertifizierungsbetrieb)
CRL	certificate revocation list (Zertifikatssperrliste)
EA	enrolment authority (Enrollmentstelle)
EC	enrolment credential (Enrollment-Berechtigungsnachweis)
ECIES	elliptic curve integrated encryption scheme (Verschlüsselungsverfahren, dem elliptische Kurven zugrunde liegen)
EE	end-entity (Endteilnehmer (d.h. C-ITS-Station)

ECTL	European Certificate Trust List (Liste vertrauenswürdiger europäischer Zertifikate)
EU-CCMS	EU C-ITS security credential management system (EU-weites Managementsystem für Sicherheitsberechtigungsnachweise von C-ITS)
DSGVO	Datenschutz-Grundverordnung
HSM	Hardware-Sicherheitsmodul
PKI	Public-Key-Infrastruktur
RA	registration authority (Registrierungsstelle)
Sub-CA	EA und AA
TLM	Trust List Manager (Manager der Liste vertrauenswürdiger Zertifikate)

Glossar

Antragsteller	Die natürliche oder juristische Person, die ein Zertifikat (oder dessen Erneuerung) beantragt. Ist das Zertifikat einmal ausgestellt (Initialisierung), wird der Antragsteller als Abonnent bezeichnet. Bei für Geräte ausgestellten Zertifikaten ist der Abonnent (Antragsteller) die Stelle, die über den Endteilnehmer, an den das Zertifikat ausgestellt wird, Kontrolle ausübt bzw. ihn betreibt, auch wenn der Endteilnehmer den eigentlichen Antrag auf das Zertifikat sendet.
authorisation authority (Genehmigungs-stelle)	In diesem Dokument bezieht sich der Begriff „Genehmigungsstelle“ (AA) nicht nur auf die spezifische Funktion der AA, sondern auch auf die juristische und/oder operative Stelle, die sie verwaltet.
certification authority (Zertifizierungs-stelle)	Die Wurzelzertifizierungsstelle, die Enrollmentstelle und die Genehmigungsstelle werden zusammen als Zertifizierungsstelle (CA) bezeichnet.
C-ITS-Trust Model	Für die Herstellung eines Vertrauensverhältnisses zwischen C-ITS-Stationen ist das C-ITS Trust Model verantwortlich. Es wird durch die Verwendung einer PKI umgesetzt, die sich aus Root-CA, CPOC, TLM, EA, AA und einem sicheren Netz zusammensetzt.
Krypto-Agilität	Die Fähigkeit der Teilnehmer am C-ITS Trust Modell, die Certificate Policy an sich wandelnde Umfelder oder neue künftige Anforderungen anzupassen, beispielsweise durch im Laufe der Zeit vorgenommene Änderungen der kryptografischen Algorithmen und der Schlüssellänge.
kryptografisches Modul	Ein sicheres, auf Hardware basierenden Element, in dem Schlüssel generiert und/oder gespeichert, Zufallszahlen generiert und Daten signiert oder verschlüsselt werden.
enrolment authority (Enrollmentstelle)	In diesem Dokument bezieht sich der Begriff „Enrollmentstelle“ (EA) nicht nur auf die spezifische Funktion der EA, sondern auch auf die juristische und/oder operative Einrichtung, die sie verwaltet.
PKI-Teilnehmer	Die Teilnehmer des C-ITS Trust Models, d. h. der TLM, die Root-CA, EA, AA und die C-ITS-Stationen.
Schlüssel-erneuerung	Diese Unterkomponente dient zur Beschreibung bestimmter Elemente in Bezug auf einen Abonnenten oder sonstigen Teilnehmer, der ein neues Schlüsselpaar generiert und die Ausstellung eines neuen Zertifikats zur Zertifizierung des neuen öffentlichen Schlüssels beantragt, wie in [3] beschrieben.
Datenablage	Die Datenablage, die für die Speicherung der Zertifikate und der von den Teilnehmern des C-ITS Trust Models bereitgestellten Informationen über Zertifikate gemäß Definition in Abschnitt 2.3 genutzt wird.
Wurzel-zertifizierungs-stelle	In diesem Dokument bezieht sich der Begriff „Wurzelzertifizierungsstelle“(CA) nicht nur auf die spezifische Funktion der Zertifizierungsstelle, sondern auch auf die juristische und/oder operative Einrichtung, die sie verwaltet.
Subjekt	Die natürliche Person, das Gerät, das System, die Einheit oder die Rechtsperson, die bzw. das in einem Zertifikat als Subjekt genannt wird, d. h. entweder der Abonnent oder ein Gerät, das vom Abonnenten kontrolliert oder betrieben wird.
Abonnent	Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die rechtlich an einen Abonnentenvertrag oder eine Vereinbarung über Nutzungsbedingungen gebunden ist.

Abonnenten-vertrag	Ein Vertrag zwischen Wurzelzertifizierungsstelle und Antragsteller/Abonnent, in dem die Rechte und Verantwortlichkeiten der Vertragsparteien festgelegt werden.

1.3. PKI-Teilnehmer

1.3.1. Einleitung

Die PKI-Teilnehmer spielen in der durch die vorliegende Certificate Policy festgelegten PKI eine Rolle. Sofern dies nicht ausdrücklich untersagt ist, kann ein Teilnehmer gleichzeitig mehrere Funktionen übernehmen. Es kann ihm untersagt werden, bestimmte Funktionen gleichzeitig zu übernehmen, um Interessenkonflikte zu vermeiden oder eine Aufgabentrennung zu gewährleisten.

Im Rahmen eines Dienstleistungsvertrags können die Teilnehmer auch andere Teile ihrer Funktionen an andere Stellen übertragen. Wenn beispielsweise Angaben zum Sperrstatus mit Hilfe von CRL zur Verfügung gestellt werden, ist die Wurzelzertifizierungsstelle (CA) auch Herausgeberin der CRL, kann aber die Zuständigkeit für die Ausstellung der CRL an einen anderen Teilnehmer delegieren.

Bei PKI-Funktionen handelt es sich um:

- maßgebliche Funktionen, d. h. jede Funktion wird eindeutig instanziiert;
- betriebliche Funktionen, d. h. Funktionen, die bei einem oder mehreren Teilnehmern instanziiert werden können.

So kann eine Root-CA beispielsweise von einem gewerblichen Teilnehmer, einer gemeinsamen Interessengruppe, einer nationalen Organisation und/oder einer europäischen Organisation implementiert werden.

Abbildung 1 zeigt die Architektur des C-ITS Trust Models auf der Grundlage von [2]. Die Architektur wird an dieser Stelle kurz beschrieben, die Hauptelemente werden jedoch in den Abschnitten 1.3.2 bis 1.3.6 ausführlicher beschrieben.

Die CPA ernennt den TLM, der daher für alle PKI-Teilnehmer ein vertrauenswürdiger Teilnehmer ist. Die CPA genehmigt den Betrieb der Root-CA und bestätigt, dass der TLM der/den Root-CA vertrauen kann. Der TLM stellt die ECTL aus, die allen PKI-Teilnehmern Vertrauen in die genehmigten Root-CA vermittelt. Die Root-CA stellt der EA und AA Zertifikate aus und vermittelt so Vertrauen in deren Betrieb. Die EA stellt Enrollment-Zertifikate an die sendenden und weiterleitenden C-ITS-Stationen (als Endteilnehmern) aus und vermittelt so Vertrauen in deren Betrieb. Die AA stellt den C-ITS-Stationen auf der Grundlage des Vertrauens in die EA Berechtigungstickets (AT) aus.

Die empfangende und weiterleitende C-ITS-Station (als weiterleitende Partei) kann anderen C-ITS-Stationen vertrauen, weil die Berechtigungstickets (AT) von einer AA ausgestellt werden, der eine Root-CA vertraut, der wiederum TLM und CPA vertrauen.

Beachten Sie bitte, dass Abbildung 1 nur die Ebene der Root-CA im C-ITS Trust Model darstellt. Einzelheiten zu den unteren Ebenen werden in den nachfolgenden Abschnitten dieser Certificate Policy oder der Erklärung zum Zertifizierungsbetrieb (CPS) der spezifischen Root-CA aufgeführt.

Abbildung 2 vermittelt einen Überblick über die Informationsflüsse zwischen PKI-Teilnehmern. Die grünen Punkte zeigen Informationsflüsse, die eine Kommunikation

von Maschine zu Maschine erfordern. Für die Informationsflüsse in Rot bestehen festgelegte Sicherheitsanforderungen.

Das C-ITS Trust Model basiert auf einer multiplen Root-CA-Architektur, bei der die Root-CA-Zertifikate regelmäßig (wie im Folgenden beschrieben) der zentralen Kontaktstelle (CPOC) durch ein sicheres, von der CPOC festgelegtes Protokoll (z. B. Link-Zertifikate) übertragen werden.

Eine Root-CA kann von einer staatlichen oder privaten Stelle betrieben werden. Die Architektur für das C-ITS Trust Model enthält mindestens eine Root-CA (die EU Root-CA mit der gleichen Ebene wie die anderen Root-CA). Die EU Root-CA wird von allen am C-ITS Trust Model beteiligten Stellen, die nicht ihre eigene Root-CA gründen wollen, delegiert. Die zentrale Kontaktstelle (CPOC) übermittelt die empfangenen Root-CA-Zertifikate an den TLM, der dafür zuständig ist, die Liste der Root-CA-Zertifikate zu erfassen und zu signieren und sie an die CPOC zurückzusenden, die sie dann für alle öffentlich zugänglich macht (siehe unten).

Die Vertrauensbeziehungen zwischen den Teilnehmern am C-ITS Trust Model werden in den folgenden Abbildungen, Tabellen und Abschnitten beschrieben.

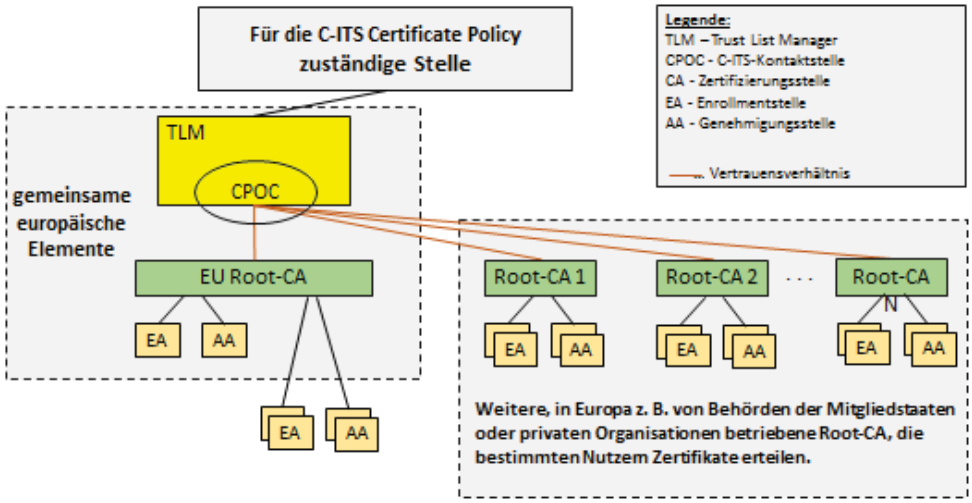

Abbildung 1: Architektur des C-ITS Trust Models

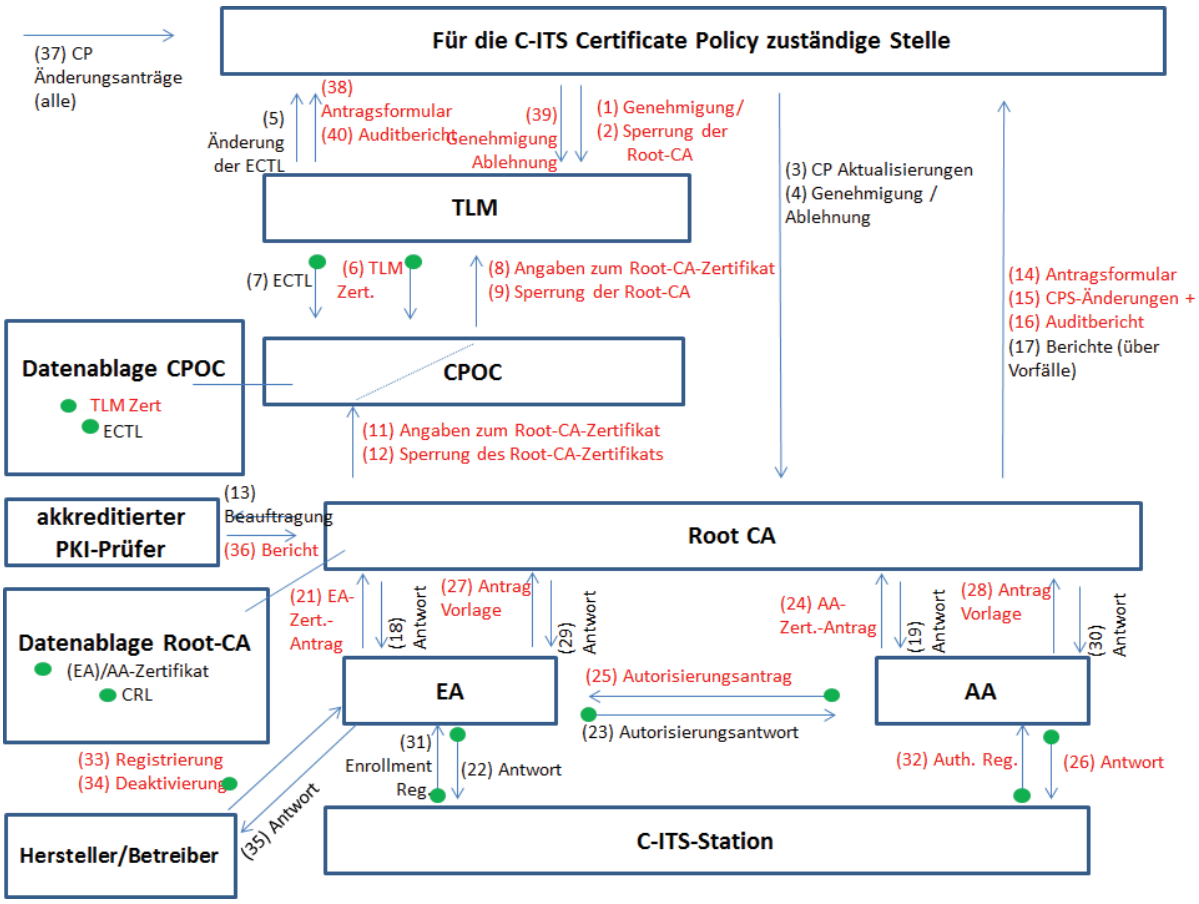

Abbildung 2: Informationsflüsse im C-ITS Trust Model

ID, Ablauf	Von	Zu	Inhalt	Referenz
(1).	CPA	TLM	Genehmigung des Root-CA-Antrags	8
(2).	CPA	TLM	Informationen über die Sperrung der Root-CA	8.5
(3).	CPA	Root-CA	Aktualisierungen der Certificate Policy	1.5
(4).	CPA	Root-CA	Genehmigung/Ablehnung des Antragsformulars der Root-CA oder des CPS-Änderungsantrags oder des Auditverfahrens	8.5, 8.6
(5).	TLM	CPA	Mitteilung einer ECTL-Änderung	4, 5.8.1
(6).	TLM	CPOC	TLM-Zertifikat	4.4.2
(7).	TLM	CPOC	ECTL	4.4.2
(8).	CPOC	TLM	Angaben zum Root-CA-Zertifikat	4.3.1.1
(9).	CPOC	TLM	Sperrung des Root-CA-Zertifikats	7.3
(10).	CPOC	alle Endteil-nehmer	TLM-Zertifikat	4.4.2
(11).	Root-CA	CPOC	Angaben zum Root-CA-Zertifikat	4.3.1.1
(12).	Root-CA	CPOC	Sperrung des Root-CA-Zertifikats	7.3
(13).	Root-CA	Prüfer	Prüfungsanordnung	8
(14).	Root-CA	CPA	Antragsformular für die Root-CA – Erstantrag	4.1.2.1
(15).	Root-CA	CPA	Antragsformular für Root-CA – CPS-Änderungen	1.5.1
(16).	Root-CA	CPA	Antragsformular für Root-CA – Auditbericht	8.6
(17).	Root-CA	CPA	Root-CA Störungsmeldungen, einschließlich Sperrung einer Sub-CA (EA, AA)	Anhang III, 7.3.1
(18).	Root-CA	EA	Antwort, EA-Zertifikat	4.2.2.3
(19).	Root-CA	AA	Antwort, AA-Zertifikat	4.2.2.3
(20).	Root-CA	Alle	EA/AA Zertifikat, CRL	4.4.2
(21).	EA	Root-CA	Antrag auf EA-Zertifikat	4.2.2.3
(22).	EA	C-ITS-Station	Antwort, Enrollment-Berechtigungsnachweis	4.3.1.4
(23).	EA	AA	Antwort, Genehmigung	4.2.2.5
(24).	AA	Root-CA	Antrag auf AA-Zertifikat	4.2.2.3
(25).	AA	EA	Antrag auf Genehmigung	4.2.2.5
(26).	AA	C-ITS-Station	Antwort, Berechtigungsticket	4.3.1.5
(27).	EA	Root-CA	Einreichung des Antrags	4.1.2.3
(28).	AA	Root-CA	Einreichung des Antrags	4.1.2.3

(29).	Root-CA	EA	Antwort	4.12 und 4.2.1
(30).	Root-CA	AA	Antwort	4.12 und 4.2.1
(31).	C-ITS-Station	EA	Antrag auf Enrollment-Berechtigungsnachweis	4.2.2.4
(32).	C-ITS-Station	AA	Antrag auf Berechtigungsticket	4.2.2.5
(33).	Hersteller/Betreiber	EA	Registrierung	4.2.1.4
(34).	Hersteller / Betreiber	EA	Deaktivierung	7.3
(35).	EA	Hersteller / Betreiber	Antwort	4.2.1.4
(36).	Prüfer	Root-CA	Bericht	8.1
(37).	alle	CPA	Anträge auf Änderungen der CP	1.5
(38).	TLM	CPA	Antragsformular	4.1.2.2
(39).	CPA	TLM	Annahme/Ablehnung	4.1.2.2
(40).	TLM	CPA	Auditbericht	4.1.2.2

Tabelle 1: Ausführliche Beschreibung der Informationsflüsse im C-ITS Trust Model

1.3.2. Für die C-ITS Certificate Policy zuständige Stelle

(1) Die für die C-ITS Certificate Policy zuständige Stelle (CPA) setzt sich aus Vertretern öffentlicher und privater Interessenträger (z. B. Mitgliedstaaten, Fahrzeughersteller usw.) zusammen, die am C-ITS Trust Model beteiligt sind. Die Stelle ist für zwei nachgeordnete Funktionen zuständig:

(1) Verwaltung der Certificate Policy, einschließlich:

- Genehmigung der vorliegenden Certificate Policy und künftiger Anträge auf Änderungen der Certificate Policy;
- Entscheidung über die Überprüfung von Änderungsanträgen und Empfehlungen, die von anderen PKI-Teilnehmern oder Organisationen eingereicht wurden;
- Entscheidung über die Freigabe neuer Fassungen der Certificate Policy;

(2) PKI-Bevollmächtigungsmanagement, einschließlich:

- Festlegung, Entscheidung und Veröffentlichung von Genehmigungen für Erklärungen zum Zertifizierungsbetrieb (CPS) und CA-Auditverfahren (im Folgenden zusammen als „CA-Genehmigungsverfahren“ bezeichnet);
- Ermächtigung der CPOC, regelmäßig tätig zu werden und darüber Bericht zu erstatten;
- Ermächtigung des TLM, regelmäßig tätig zu werden und Bericht zu erstatten;

- Genehmigung der CPS von Root-CA, wenn sie mit der gemeinsamen, gültigen Certificate Policy (CP) in Einklang stehen;
- Prüfung der Auditberichte des akkreditierten PKI-Prüfers für alle Root-CA;
- Benachrichtigung des TLM über die Liste genehmigter oder nicht genehmigter Root-CA und der zugehörigen Zertifikate auf der Grundlage eingegangener Genehmigungsberichte der Root-CA und regelmäßiger betrieblicher Berichte.

(2) Der Bevollmächtigte der CPA ist für die Authentifizierung des Bevollmächtigen des TLM und die Genehmigung des Antragsformulars für den TLM-Enrollment-Prozess zuständig. Die CPA ist dafür zuständig, das TLM zu bevollmächtigen, den Angaben in diesem Abschnitt entsprechend zu handeln.

1.3.3. Trust List Manager

(3) Der TLM ist eine von der CPA benannte einzige Stelle.

(4) Der TLM ist zuständig für:

- den Betrieb der ECTL im Einklang mit der gemeinsamen, gültigen Certificate Policy und die regelmäßige Übermittlung von Tätigkeitsberichten an die für die Certificate Policy zuständige Stelle (CPA), damit der Betrieb des C-ITS Trust Models insgesamt sicher verläuft;
- Empfang der CA-Zertifikate von der CPOC;
- Ein- oder Ausschluss von Root-CA-Zertifikaten in der ECTL nach entsprechender Benachrichtigung durch die CPA;
- Signieren der ECTL;
- die regelmäßige und rechtzeitige Übermittlung der ECTL an die CPOC.

1.3.4. Akkreditierter PKI-Prüfer

(5) Der akkreditierte PKI-Prüfer ist zuständig für:

- die Durchführung oder Organisation von Audits von Root-CA, TLM und Sub-CA;
- Weitergabe des Auditberichts (über einen erstmaligen oder regelmäßigen Audit) an die CPA im Einklang mit den Anforderungen in Abschnitt 8. Der Auditbericht muss Empfehlungen des akkreditierten PKI-Prüfers enthalten;
- Benachrichtigung der die Root-CA verwaltenden Stelle über die erfolgreiche oder nicht erfolgreiche Durchführung eines erstmaligen oder regelmäßigen Audits der Sub-CA;
- Bewertung der Konformität der Erklärungen zum Zertifizierungsbetrieb (CPS) mit der vorliegenden Certificate Policy.

1.3.5. C-ITS-Kontaktstelle (CPOC)

(6) Die CPOC ist eine von der CPA ernannte einzige Stelle. Der Bevollmächtigte der CPA ist für die Authentifizierung des Bevollmächtigten der CPOC und die

Genehmigung des Antragsformulars für den CPOC-Enrollment-Prozess zuständig. Die CPA ist dafür zuständig, die CPOC zu bevollmächtigen, den Angaben in diesem Abschnitt entsprechend zu handeln.

(7) Die CPOC ist zuständig für:

- Aufbau eines sicheren Kommunikationsaustausches zwischen allen Teilnehmern des C-ITS Trust Models auf effiziente, schnelle Art und Weise und die Leistung von Beiträgen hierzu;
- Überprüfung von Änderungsanträgen und Empfehlungen, die von anderen Teilnehmern des Trust Models (z. B. Root-CA) eingereicht wurden;
- Übermittlung von Root-CA-Zertifikaten an das TLM;
- Veröffentlichung des gemeinsamen Vertrauensankers (aktueller öffentlicher Schlüssel und Link-Zertifikat des TLM);
- Veröffentlichung der ECTL.

Die vollständigen Angaben zur ECTL sind in Abschnitt 7 zu finden.

1.3.6. Betriebliche Funktionen

(8) Die folgenden, in [2] definierten Stellen üben gemäß Festlegung in RFC 3647 eine betriebliche Funktion aus:

Funktionselement	Funktion der PKI ([3] und [4])	Funktion im Einzelnen ([2])
Wurzelzertifizierungsstelle	CA/RA (Registrierungsstelle)	Übermittelt EA und AA den Nachweis, dass sie EC oder AT ausstellen darf
Enrollmentstelle	Abonnent bei der Root-CA/Subjekt des EA-Zertifikats CA/RA	Authentifiziert eine C-ITS-Station und gewährt ihr Zugang zur ITS-Kommunikation
Genehmigungsstelle	Abonnent bei der Root-CA/Subjekt des AA-Zertifikats CA/RA	Übermittelt einer C-ITS-Station verlässliche Nachweise dafür, dass sie bestimmte ITS-Dienste nutzen darf
Sendende C-ITS-Station	Subjekt des Endteilnehmer (EE)-Zertifikats (EC)	Erwirbt von der EA Zugangsrechte zu ITS-Kommunikationen Erwirbt von der AA Rechte, ITS-Dienste aufzurufen Sendet Meldungen in Einzeletappen und weitergeleitete Funkmeldungen
Weiterleitende (Weiterleitung) C-ITS-Station	Weiterleitende Partei/ Subjekt des EE-Zertifikats	Empfängt Funkmeldungen von der sendenden C-ITS-Station und leitet sie erforderlichenfalls an die empfangende C-ITS-Station weiter
empfangende C-ITS-Station	weiterleitende Partei	Empfängt Funkmeldungen von einer sendenden oder weiterleitenden C-ITS-Station
Hersteller	Abonnent an die EA	Installiert während der Herstellung die erforderlichen Informationen für das Sicherheitsmanagement in der C-ITS-Station
Betreiber	Abonnent bei EA/AA	Installiert und aktualisiert während des Betriebs die erforderlichen Informationen für das Sicherheitsmanagement in der C-ITS-Station

Tabelle 2: Betriebliche Funktionen

Anmerkung: Im Einklang mit [4] werden in der vorliegenden Certification Policy unterschiedliche Begriffe für den „Abonnenten“, der mit der CA einen Vertrag über die Ausstellung von Zertifikaten schließt, und das „Subjekt“, auf das sich das Zertifikat bezieht, verwendet. Abonnenten sind stets Teilnehmer, die eine vertragliche Beziehung mit einer CA haben, Subjekte sind Teilnehmer, für die das Zertifikat gilt. EA/AA sind Abonnenten und Subjekte der Root-CA und können EA/AA-Zertifikate anfordern. C-ITS-Stationen sind Subjekte und können Endteilnehmer-Zertifikate anfordern.

(9) Registrierungsstellen:

Die EA hat die Aufgabe, die Funktion einer Registrierungsstelle für Endteilnehmer zu übernehmen. Nur authentifizierte und berechtigte Abonnenten können neue Endteilnehmer (C-ITS-Stationen) in einer Enrollment-Stelle (EA) registrieren lassen. Die maßgeblichen Root-CA haben die Funktion von Registrierungsstellen für EA und A zu erfüllen.

1.4. Verwendung von Zertifikaten

1.4.1. Anwendbare Verwendungsbereiche

(10) Im Rahmen der vorliegenden Certification Policy ausgestellte Zertifikate sind für die Validierung digitaler Signaturen im Kontext der kooperativen ITS-

Kommunikation vorgesehen, wobei die Referenzarchitektur von [2] einzuhalten ist.

(11) In den Zertifikatprofilen in [5] wird die Verwendung von Zertifikaten für TLM, Root-CA, EA, AA und Endteilnehmer bestimmt.

1.4.2. Zuständigkeitsgrenzen

(12) Zertifikate sind für folgende Verwendungszwecke weder bestimmt noch zulässig:

- Umstände, die geltendes Recht, Verordnungen (z. B. die DSGVO), Erlässe oder behördliche Anordnungen verletzen, gegen sie verstoßen oder ihnen zuwiderlaufen;
- Umstände, die gegen die Rechte Dritter verstoßen, ihnen zuwiderlaufen oder sie verletzen;
- Verstoß gegen die vorliegende Certificate Policy oder den maßgeblichen Abonnentenvertrag;
- Umstände, unter denen ihre Verwendung unmittelbar zu Todesfällen, Körperverletzungen oder schweren Umweltschäden führen könnte (z. B. Ausfall kerntechnischer Anlagen, der Navigation oder Kommunikation von Flugzeugen oder von Waffenkontrollsystemen);
- Umstände, die dem übergeordneten Ziel einer höheren Straßenverkehrssicherheit und eines effizienteren Straßenverkehrs in Europa zuwiderlaufen.

1.5. Verwaltung der Certificate Policy

1.5.1. Aktualisierung der CPS der in der ECTL aufgeführten CA

(13) Jede in der ECTL aufgeführte Root-CA veröffentlicht ihre eigene Erklärung zum Zertifizierungsbetrieb (CPS), die mit dieser Certificate Policy konform sein muss. Eine Root-CA kann zusätzliche Anforderungen hinzufügen, muss jedoch sicherstellen, dass jederzeit sämtliche Anforderungen dieser Certificate Policy erfüllt werden.

(14) Jede in der ECTL aufgeführte CA führt ein geeignetes Änderungsverfahren für ihr CPS-Dokument ein. Die wichtigsten Eigenschaften des Änderungsverfahrens werden im öffentlichen Teil der CPS dokumentiert.

(15) Mit dem Änderungsverfahren wird sichergestellt, dass alle Änderungen an der vorliegenden Certificate Policy (CP) sorgfältig analysiert werden; sofern dies zur Einhaltung der CP in der geänderten Form erforderlich ist, wird die CPS innerhalb des im Umsetzungsschritt des Änderungsverfahrens für die CP festgelegten Zeitrahmens aktualisiert. Das Änderungsverfahren beinhaltet insbesondere Dringlichkeitsverfahren für Änderungen, mit denen eine fristgerechte Umsetzung sicherheitsrelevanter Änderungen an der Certificate Policy (CP) sichergestellt wird.

(16) Das Änderungsverfahren umfasst geeignete Maßnahmen zur Verifizierung der Konformität mit der Certificate Policy aller Änderungen an der Erklärung zum Zertifizierungsbetrieb (CPS). Alle Änderungen an der CPS werden eindeutig dokumentiert. Bevor eine neue Fassung einer CPS umgesetzt wird, muss deren

Konformität mit der Certificate Policy von einem akkreditierten PKI-Prüfer bestätigt werden.

(17) Die Root-CA teilt der CPA jede Änderung an der CPS mit mindestens folgenden Angaben mit:

- einer genaue Beschreibung der Änderung;
- der Gründe für die Änderung;
- eine Bericht des akkreditierten PKI-Prüfers, in dem die Konformität mit der CP bestätigt wird;
- Kontaktangaben der für die CPS zuständigen Person;
- geplanter Zeitplan für die Umsetzung.

1.5.2. Verfahren zur Genehmigung von CPS

(18) Vor Beginn des Betriebs legt eine künftige Root-CA einem akkreditierten PKI-Prüfer ihre CPS im Rahmen eines Auftrags zur Konformitätsprüfung (Ablauf 13) sowie der CPA zur Genehmigung (Ablauf 15) vor.

(19) Eine Root-CA legt Änderungen an ihrer CPS einem akkreditierten PKI-Prüfer im Rahmen eines Auftrags zur Konformitätsprüfung (Ablauf 13) sowie der CPA zur Genehmigung (Ablauf 15) vor.

(20) Eine EA/AA legt ihre Erklärung zum Zertifizierungsbetrieb (CPS) oder Änderungen an ihrer CPS der Root-CA vor. Die Root-CA kann bei der für die Genehmigung der EA/AA gemäß Definition in den Abschnitten 4.1.2 und 8 zuständigen nationalen Instanz oder privatrechtlichen juristischen Person eine Konformitätsbescheinigung anfordern.

(21) Der akkreditierte PKI-Prüfer bewertet die CPS gemäß Abschnitt 8.

(22) Der akkreditierte PKI-Prüfer übermittelt die Ergebnisse der CPS-Bewertung als Teil des Auditberichts gemäß Darlegung in Abschnitt 8.1. Die CPS wird im Rahmen der Annahme oder Ablehnung des Auditberichts (siehe die Abschnitte 8.5 und 8.6 angenommen oder abgelehnt.

2. VERANTWORTLICHKEITEN FÜR VERÖFFENTLICHUNG UND DATENABLAGE (REPOSITORY)

2.1. Methoden für die Veröffentlichung von Informationen über Zertifikate

(23) Informationen über Zertifikate können wie in Abschnitt 2.5 beschrieben veröffentlicht werden, d. h.:

- regelmäßig oder periodisch;
- auf Antrag einer der beteiligten Stellen.

In jedem dieser Fälle gelten unterschiedliche Dringlichkeitsstufen für die Veröffentlichung und somit Zeitpläne, die Teilnehmer müssen jedoch auf beide Regelungsarten vorbereitet sein.

(24) Die regelmäßige Veröffentlichung der Informationen über Zertifikate ermöglicht es, eine maximale Frist zu bestimmen, innerhalb der Informationen über Zertifikate für alle Knotenpunkte des C-ITS-Netzes aktualisiert werden.

Die Häufigkeit der Veröffentlichung sämtlicher Informationen über Zertifikate wird in Abschnitt 2.2 festgelegt.

(25) Auf Antrag von Stellen, die am C-ITS-Netz beteiligt sind, können Teilnehmer jederzeit mit der Veröffentlichung von Informationen über Zertifikate beginnen und abhängig von ihrem Status einen aktuellen Satz an Informationen über Zertifikate anfordern, damit sie zu einem voll vertrauenswürdigen Knotenpunkt des C-ITS-Netzes werden können. Der Zweck dieser Veröffentlichung besteht vor allem darin, Teilnehmer auf den neusten allgemeinen Stand der Zertifikatinformationen im Netz zu bringen und sie in die Lage zu versetzen, bis zur nächsten regulären Veröffentlichung der Informationen auf Vertrauensbasis zu kommunizieren.

(26) Eine einzelne Root-CA kann ebenfalls jederzeit die Veröffentlichung von Informationen über Zertifikate einleiten, indem sie allen „abonnierten Mitgliedern“ des C-ITS-Netzes, die regelmäßig Informationen dieser Art erhalten, sind, einen aktualisieren Satz von Zertifikaten übermittelt. Dies unterstützt die Arbeit der CA und versetzt sie in die Lage, sich zwischen den regelmäßigen, geplanten Veröffentlichungsterminen der Zertifikate an die Mitglieder zu wenden.

(27) In Abschnitt 2.5 werden die Mechanismen und sämtliche Verfahren für die Veröffentlichung der Root-CA-Zertifikate und der ECTL dargelegt.

(28) Die zentrale Kontaktstelle (CPOC) veröffentlicht die (in der ECTL enthaltenen und für den öffentlichen Gebrauch bestimmten) Root-CA-Zertifikate, das TLM-Zertifikat und die ECTL, die sie herausgibt.

(29) Root-CA veröffentlichen ihre EA/AA-Zertifikate und CRL und sind in der Lage, alle drei an dieser Stelle genannten Mechanismen für deren Veröffentlichung bei ihren abonnierten Mitgliedern und Vertrauenden Dritten zu unterstützen, wobei sie alle erforderlichen Schritte zur Gewährleistung einer sicheren Übertragung gemäß Abschnitt 4 unternehmen.

2.2. Zeitpunkt oder Häufigkeit der Veröffentlichung

(30) Die Anforderungen an den Veröffentlichungszeitplan für Zertifikate und CRL müssen unter Berücksichtigung der verschiedenen einschränkenden Faktoren der einzelnen C-ITS-Knotenpunkte festgelegt werden, wobei das übergeordnete Ziel darin besteht, ein „vertrauenswürdiges Netz“ zu betreiben und Aktualisierungen so schnell wie möglich bei allen beteiligten C-ITS-Stationen zu veröffentlichen.

- Für die regelmäßige Veröffentlichung aktueller Informationen über Zertifikate (z. B. Änderungen an der Zusammensetzung der ECTL oder CRL) ist für den sicheren Betrieb des C-ITS-Netzes eine Frist von höchstens drei Monaten erforderlich.
- Root-CA veröffentlichen ihre CA-Zertifikate und CRL möglichst bald nach der Ausstellung.
- Für die Veröffentlichung der CRL wird die Datenablage (Repository) der Root-CA benutzt.

Darüber hinaus wird in der CPS für jede CA der Zeitraum angegeben, innerhalb dessen nach der Ausstellung eines Zertifikates durch die CA das betreffende Zertifikat veröffentlicht wird.

In diesem Abschnitt wird nur der Zeitpunkt oder die Häufigkeit der regelmäßigen Veröffentlichung festgelegt. Mittel zur Herstellung von Verbindungen zur Aktualisierung von C-ITS-Stationen mit den ECTL und CRL innerhalb einer Woche nach ihrer Veröffentlichung (unter normalen Betriebsbedingungen, z. B. Mobilfunkabdeckung, tatsächlicher Betrieb des Fahrzeugs usw.) werden den in im vorliegenden Dokument genannten Anforderungen entsprechend eingeführt.

2.3. Datenablagen

(31) Die Anforderungen an die Struktur der Datenablage zur Speicherung der Zertifikate und der von den Teilnehmern des C-ITS-Netzes zur Verfügung gestellten Informationen lauten für einzelne Teilnehmer wie folgt:

- im Allgemeinen sollte jede Root-CA eine Datenablage für Informationen über ihre eigenen, aktuell aktiven EA/AA-Zertifikate und CRL nutzen, um Zertifikate für die anderen PKI-Teilnehmer zu veröffentlichen (z. B. einen LDAP-gestützten Verzeichnisdienst). Die Datenablage jeder Root-CA unterstützt alle erforderlichen Zugangskontrollen (Abschnitt 2.4) und Übertragungszeiten (Abschnitt 2.2) für jede Verbreitungsmethode für Informationen im Zusammenhang mit C-ITS;
- die Datenablage des TLM (Trust List Manager) (in der beispielsweise die von der CPOC veröffentlichten ECTL und TLM-Zertifikate gespeichert werden) sollte sich auf ein Veröffentlichungsverfahren stützen, das für jede Verteilungsmethode die in Abschnitt 2.2 dargelegten Übertragungszeiten gewährleisten kann.

Die Anforderungen der AA sind nicht festgelegt, müssen jedoch die gleichen Sicherheitsstufen wie die anderen Teilnehmer unterstützen; diese müssen in ihrer CPS ausgewiesen sein.

2.4. Zugangskontrollen für Datenablagen (Repositories)

(32) Die Anforderungen an die Zugangskontrolle zu Datenablagen für Informationen über Zertifikate genügen mindestens den allgemeinen Standards für den sicheren Umgang mit Informationen gemäß ISO/IEC 27001 und den Anforderungen in Abschnitt 4. Darüber hinaus müssen sie die Prozesssicherheit widerspiegeln, die für die einzelnen Verfahrensschritte bei der Veröffentlichung der Zertifikatinformationen hergestellt werden muss.

- Dazu gehört auch die Implementierung der Datenablage für TLM-Zertifikate und ECTL bei dem TLM/der CPOC. Alle Zertifizierungsstellen (CA) oder Betreiber von Datenablagen implementieren in Bezug auf sämtliche C-ITS-Teilnehmer und externen Parteien Zugangskontrollen für mindestens drei verschiedene Ebenen (z. B. allgemein zugänglich, beschränkt auf C-ITS-Teilnehmer, Root-CA-Ebene), um zu verhindern, dass Unbefugte Einträge in der Datenablage ergänzen, ändern oder löschen können.
- Die genauen Zugangskontrollmechanismen der einzelnen Teilnehmer sollten Bestandteil der jeweiligen CPS sein.
- Bei jeder einzelnen Root-CA müssen die EA- und AA-Datenablagen die gleichen Anforderungen an die Zugangskontrollverfahren erfüllen, und

zwar unabhängig von dem Ort oder der vertraglichen Bindung an den Diensteanbieter, der die Datenablage betreibt.

Als Ausgangspunkt für die verschiedenen Ebenen der Zugangskontrolle sollten alle Root-CA oder Betreiber von Datenablagen mindestens drei verschiedene Ebenen (z. B. allgemein zugänglich, beschränkt auf C-ITS-Teilnehmer, Root-CA-Ebene) bereitstellen.

2.5. Veröffentlichung von Informationen über Zertifikate

2.5.1. Veröffentlichung von Informationen über das Zertifikat durch den TLM

(33) Der TLM im gemeinsamen europäischen C-ITS-Vertrauensbereich veröffentlicht die folgenden Informationen über die CPOC:

- alle derzeit gültigen TLM-Zertifikate für den nächsten Betriebszeitraum (aktuelle und Link-Zertifikate, sofern vorhanden);
- Informationen über die Zugangsstelle für die CPOC-Datenablage zur Bereitstellung der signierten Liste von Root-CA (ECTL);
- allgemeine Informationsstelle für die ECTL und den Einsatz der C-ITS.

2.5.2. Veröffentlichung von Informationen über Zertifikate durch CA

(34) Root-CA im gemeinsamen europäischen C-ITS-Vertrauensbereich veröffentlichen folgende Informationen:

- ausgestellte (derzeit gültige) Root-CA-Zertifikate (aktuelle Zertifikate und Zertifikate mit korrekt erneuertem Schlüssel, einschließlich eines Link-Zertifikats) in der in Abschnitt 2.3 genannten Datenablage;
- alle gültigen EA, AA-Teilnehmer mit Betreiber-ID und der geplanten Betriebsdauer;
- ausgestellte CA-Zertifikate in den in Abschnitt 2.3 genannten Datenablagen;
- die CRL für alle gesperrten CA-Zertifikate, die ihre nachgeordneten EA und AA abdecken;
- Angaben zur Zugangsstelle der CA zur CRL und zu CA-Informationen.

Alle Zertifikate sind in drei Vertraulichkeitsebenen einzustufen und für die allgemeine Öffentlichkeit bestimmte Dokumente müssen ohne Einschränkungen öffentlich zugänglich sein.

3. IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1. Namen

3.1.1. Arten von Namen

3.1.1.1. Namen für TLM, Root-CA, EA, AA

(35) Der Name im TLM-Zertifikat besteht aus einem einzelnen Attribut „subject_Name“ mit dem reservierten Wert „EU_TLM“.

(36) Der Name von Root-CA besteht aus einem einzelnen Attribute „subject_Name“ mit einem von der CPA zugewiesenen Wert. Die Eindeutigkeit von Namen liegt in der alleinigen Verantwortung der CPA und

der TLM muss das Register der Root-CA-Namen nach entsprechender Benachrichtigung durch die CPA pflegen (Genehmigung, Sperrung/Löschung einer Root-CA). Die Subjektnamen in Zertifikaten sind auf 32 Bytes beschränkt. Jede Root-CA schlägt der CPA ihren Namen in dem Antragsformular (Ablauf 14) vor. Die CPA ist für die Überprüfung der Eindeutigkeit von Namen zuständig. Ist der Name nicht eindeutig, wird das Antragsformular zurückgewiesen (Ablauf 4).

(37) Der Name in jedem EA/AA-Zertifikat kann aus einem einzelnen Attribut „subject_Name“ bestehen, das vom Aussteller des Zertifikats generiert wird. Die Eindeutigkeit von Namen liegt in der alleinigen Verantwortung der ausstellenden Root-CA.

(38) In den EA- und AA-Zertifikaten darf kein Name verwendet werden, der länger als 32 Byte ist, da der subject_Name in Zertifikaten auf 32 Bytes beschränkt ist.

(39) Die AT dürfen keinen Namen enthalten.

3.1.1.2. Namen für Endteilnehmer

(40) Jeder C-ITS-Station werden zwei Arten von eindeutigen Kennungen zugewiesen:

- eine kanonische ID, die bei der erstmaligen Registrierung der C-ITS-Station unter der Verantwortung des Herstellers gespeichert wird. Sie enthält eine Teilkette, aus der der Hersteller oder Betreiber hervorgeht, so dass diese Kennung eindeutig sein kann;
- einen „subject_name“ der Teil des Enrollment-Berechtigungsnachweises (EC) der C-ITS-Station sein kann und für den die EA verantwortlich ist.

3.1.1.3. Identifizierung der Zertifikate

(41) Zertifikate, die dem Format in [5] entsprechen, werden mittels Berechnung eines HasdId8-Werts gemäß Definition in [5] identifiziert.

3.1.2. Notwendigkeit der Aussagekraft von Namen

Keine Bestimmung vorgesehen.

3.1.3. Anonymität und Pseudonymität von Endteilnehmern

(42) Die AA stellt sicher, dass die Pseudonymität einer C-ITS-Station dadurch hergestellt wird, dass die C-ITS-Station mit AT versehen wird, die keine Namen oder Angaben enthalten, die eine Verbindung zwischen dem Subjekt und seiner wirklichen Identität herstellen könnten.

3.1.4. Regeln für die Auslegung verschiedener Namensformen

Keine Bestimmung vorgesehen.

3.1.5. Eindeutigkeit von Namen

(43) Die Namen für die TLM, Root-CA, EA, AA und kanonischen ID für C-ITS-Stationen müssen eindeutig sein.

(44) Der TLM stellt im Registrierungsprozess einer bestimmten Root-CA in der ECTL sicher, dass deren Zertifikatskennung (HaheudId8) eindeutig ist. Die Root-CA stellt im Ausstellungsprozess sicher, dass die Zertifikatskennung (HashedId8) jeder nachgeordneten CA eindeutig ist.

(45) Die HasheudId8 eines EC muss innerhalb der ausstellenden CA eindeutig sein. Die HasheudId8 eines AT muss nicht eindeutig sein.

3.2. Erstmalige Validierung der Identität

3.2.1. Methode zum Nachweis des Besitzes des privaten Schlüssels

(46) Die Root-CA muss nachweisen, dass sie den privaten Schlüssel, der dem öffentlichen Schlüssel im selbstunterzeichneten Zertifikat entspricht, rechtmäßig besitzt. Die CPOC überprüft diesen Nachweis.

(47) Die EA/AA muss nachweisen, dass sie den privaten Schlüssel, der dem im Zertifikat aufzuführenden öffentlichen Schlüssel entspricht, rechtmäßig besitzt. Die Root-CA überprüft diesen Nachweis.

(48) Der Besitz eines neuen privaten Schlüssels (zur Schlüsselerneuerung) wird mittels Signieren des Antrags mit dem neuen privaten Schlüssel (innere Signatur), gefolgt von der Generierung einer äußeren Signatur mit dem derzeit gültigen privaten Schlüssel über dem signierten Antrag nachgewiesen (als Garantie für die Authentizität des Antrags (Request)). Der Antragsteller reicht den unterzeichneten Zertifikatantrag über einen sicheren Kommunikationsweg bei der ausstellenden CA ein. Die ausstellende CA überprüft, ob die digitale Signatur des Antragstellers mit Hilfe des privaten Schlüssels erstellt wurde, der dem öffentlichen, dem Zertifikatantrag beigefügten Schlüssel entspricht. Die Root-CA gibt an, welche Zertifikatanträge und Antworten sie in ihrer CPS unterstützt.

3.2.2. Authentifizierung der Organisationsidentität

3.2.2.1. Authentifizierung der Organisationsidentität der Root-CA

(49) In einem Antragsformular an die CPA (d. h. Ablauf 14) übermittelt die Root-CA die Identität der Organisation und die Registrierungsinformationen, die sich wie folgt zusammensetzen:

- Name der Organisation;
- Postanschrift;
- E-Mailadresse;
- Name einer natürlichen Kontaktperson in der Organisation;
- (Telefonnummer;
- digitaler Fingerabdruck (d. h. SHA 256 Hash-Wert) des Zertifikates der Root-CA in gedruckter Form;
- kryptografische Informationen (d. h. kryptografische Algorithmen, Schlüssellängen) im Zertifikat der CA-Root;
- alle Genehmigungen, die die Root-CA nutzen und an Sub-CA weitergeben darf.

(50) Die CPA prüft die Identität der Organisation und der sonstigen Registrierungsinformationen, die vom Antragsteller auf Aufnahme eines Zertifikats der Root-CA in die ECTL bereitgestellt werden.

(51) Im Hinblick auf die Identität (z. B, den Namen) und gegebenenfalls hinsichtlich besonderer Attribute der Subjekte, denen ein Zertifikat ausgestellt

wird, erhebt die CPA entweder unmittelbare Nachweise oder sie beschafft eine Bestätigung einer geeigneten, berechtigten Quelle. Die Nachweise können in Papierform oder in elektronischer Form vorgelegt werden.

(52) Die Identität des Subjekts wird zum Zeitpunkt der Registrierung auf geeignete Weise und im Einklang mit der vorliegenden Certificate Policy verifiziert.

(53) Bei jedem Zertifikatantrag sind Nachweise für Folgendes zu erbringen:

- den vollständigen Namen der organisatorischen Einheit (private Organisation, staatliche Stelle oder nichtgewerbliche Einrichtung);
- eine national anerkannte Registrierung oder sonstige Attribute, die so weit wie möglich zur Unterscheidung der Organisationseinheit von anderen mit demselben Namen eingesetzt werden können.

Die vorstehenden Regeln beruhen auf TS 102 042 [4]: *Die CA stellt sicher, dass Nachweise für die Identifizierung von Abonnent und Subjekt sowie die Richtigkeit ihrer Namen und damit verbundenen Daten entweder im Rahmen des definierten Dienstes ordnungsgemäß geprüft oder gegebenenfalls mittels Prüfung von Bestätigungen geeigneter, berechtigte Quellen gefolgert werden; sie stellt ferner sicher, dass Anträge auf Zertifikate richtig, autorisiert und vollständig sind und den erhobenen Nachweisen oder Bestätigungen entsprechen.*

3.2.2.2. Authentifizierung der Identität der TLM-Organisation

(54) Die Organisation, die das TLM betreibt, muss Nachweise für die Identifizierung und die Richtigkeit des Namens und der damit verbundenen Daten erbringen, um eine angemessene Verifizierung der erstmaligen Erstellung und Schlüsselerneuerung des TLM-Zertifikats zu ermöglichen.

(55) Die Identität des Subjekts wird zum Zeitpunkt der Erstellung des Zertifikats oder der Schlüsselerneuerung mit geeigneten Mitteln und im Einklang mit der vorliegenden Certificate Policy (CP) verifiziert.

(56) Nachweise für die Organisation werden auf die gleiche Weise wie in Abschnitt 3.2.2.1 spezifiziert übermittelt.

3.2.2.3. Authentifizierung der Identität von Sub-CA-Organisationen

(57) Die Root-CA prüft die Identität der Organisation sowie weitere Registrierungsangaben, die von Antragstellern für Sub-CA-Zertifikate (EA/AA) vorgelegt werden.

(58) Die Root-CA muss mindestens:

- die Existenz der Organisation durch einen Identitätsprüfungsservice oder eine Identitätsprüfungsdatenbank eines Dritten oder alternativ durch entsprechende Organisationsdokumente feststellen, die von einer zuständigen staatlichen Stelle oder anerkannten Behörde ausgestellt oder bei ihr eingereicht wurden und die Existenz der Organisation bestätigen;
- mittels Briefpost oder eines vergleichbaren Verfahrens den Antragsteller auffordern, bestimmte Informationen über die Organisation zu bestätigen und ferner zu bestätigen, dass er den Antrag auf ein Zertifikat genehmigt hat und dass die Person, die den Antrag im Namen des Antragstellers einreicht, dazu berechtigt ist. Enthält ein Zertifikat den Namen einer natürlichen Person als Bevollmächtigter der Organisation, bestätigt er

außerdem, dass diese natürliche Person bei ihm beschäftigt ist und dass er sie bevollmächtigt hat, in seinem Namen zu handeln.

(59) Die Validierungsverfahren für die Ausstellung von CA-Zertifikaten werden in einer CPS der Root-CA dokumentiert.

3.2.2.4. Authentifizierung der Abonnentenorganisation von Endteilnehmern

(60) Bevor sich ein Abonnent von Endteilnehmern (Hersteller/Betreiber) bei einer vertrauenswürdigen EA anmelden kann, um seinen Endteilnehmern zu ermöglichen, Anträge auf EC-Zertifikate zu versenden, muss die EA

- die Identität der Abonnentenorganisation und andere vom Antragsteller bereitgestellte Registrierungsinformationen überprüfen;
- prüfen, ob der Typ der C-ITS-Station (d. h. das auf Marke, Modell und Version der C-ITS-Station basierende, konkrete Produkt) alle Kriterien für die Compliance-Bewertung erfüllt.

(61) Die EA muss mindestens:

- die Existenz der Organisation durch einen Identitätsprüfungsservice oder eine Identitätsprüfungsdatenbank eines Dritten oder alternativ durch entsprechende Organisationsdokumente feststellen, die von einer zuständigen staatlichen Stelle oder anerkannten Behörde ausgestellt oder bei ihr eingereicht wurden und die Existenz der Organisation bestätigen;
- mittels Briefpost oder eines vergleichbaren Verfahrens den Antragsteller auffordern, bestimmte Informationen über die Organisation zu bestätigen und ferner zu bestätigen, dass er den Antrag auf ein Zertifikat genehmigt hat und dass die Person, die den Antrag in seinem Namen einreicht, dazu berechtigt ist. Enthält ein Zertifikat den Namen einer natürlichen Person als Bevollmächtigter der Organisation, bestätigt er außerdem, dass diese natürliche Person bei ihm beschäftigt ist und dass er sie bevollmächtigt hat, in seinem Namen zu handeln.

(62) Die Validierungsverfahren für die Registrierung einer C-ITS-Station durch ihren Abonnenten werden in einer CPS der EA dokumentiert.

3.2.3. Authentifizierung einzelner Teilnehmer

3.2.3.1. Authentifizierung des einzelnen TLM/CA-Teilnehmers

(63) Für die Authentifizierung eines einzelnen Teilnehmers (natürliche Person), die in Verbindung mit einer juristischen Person oder einer organisatorischen Einheit (z. B. dem Abonnenten) identifiziert wurde, sind Nachweise über Folgendes vorzulegen:

- vollständiger Name des Subjekts (einschließlich des Nachnamens und der Vornamen, im Einklang mit geltendem Recht und den nationalen Verfahren zur Feststellung der Personalien);
- Geburtsdatum und Geburtsort, Verweis auf ein national anerkanntes Ausweisdokument oder andere Attribute des Abonnenten, die so weit wie möglich verwendet werden können, um die Person von anderen mit demselben Namen zu unterscheiden;
- vollständiger Name und Rechtsform der verbundenen juristischen Person oder einer anderen Organisationseinheit (z. B. der Abonnent);

- alle einschlägigen Registrierungsinformationen (z. B. die Firmenregistrierung) der verbundenen juristischen Person oder einer anderen Organisationseinheit;
- Nachweis, dass das Subjekt mit der juristischen Person oder einer anderen Organisationseinheit verbunden ist.

Die Nachweise können in Papierform oder in elektronischer Form vorgelegt werden.

(64) Zur Überprüfung seiner Identität legt der Bevollmächtigte einer Root-CA, EA, AA oder eines Abonnenten Unterlagen vor, aus denen hervorgeht, dass er für die Organisation arbeitet (Vollmachtsurkunde). Er muss außerdem einen amtlichen Ausweis vorlegen.

(65) Beim Verfahren des erstmaligen Enrollments (Ablauf 31/32) übermittelt ein Vertreter der EA/AA der entsprechenden Root-CA alle erforderlichen Informationen (siehe Abschnitt 4.1.2).

(66) Das Personal der Root-CA überprüft die Identität des Vertreters des Zertifikatantragstellers und alle zugehörigen Unterlagen, wobei es die Anforderungen für „vertrauenswürdiges Personal“ gemäß Abschnitt 5.2.1 anwendet. (Das Verfahren zur Validierung der Antragsdaten und zur Erstellung des Zertifikats durch die CA erfolgt durch „vertrauenswürdige Personen“ bei der Root-CA, die mindestens einer doppelten Aufsicht unterliegen, da es sich um sensible Vorgänge im Sinne von Abschnitt 5.2.2 handelt).

3.2.3.2. Authentifizierung der Identität der Abonnenten von C-ITS-Stationen

(67) Abonnenten werden durch autorisierte Endnutzer in der Organisation vertreten, die bei der ausstellenden EA und AA registriert sind. Diese Endnutzer, die von Organisationen (Herstellern oder Betreibern) benannt wurden, müssen ihre Identität und Authentizität nachweisen, bevor

- sie den Endteilnehmer (EE) bei seiner entsprechenden EA einschließlich seines kanonischen öffentlichen Schlüssels, der kanonischen ID (eindeutige Kennung) und der dem EE entsprechenden Genehmigungen registrieren;
- sich bei der AA anmelden und den Nachweis eines Abonnentenvertrags beschaffen, der an die EA übermittelt werden kann.

3.2.3.3. Authentifizierung der Identität von C-ITS-Stationen

(68) Endteilnehmer-Subjekte von EC authentifizieren sich bei der Beantragung von EC (Ablauf 31) selbst, indem sie ihren kanonischen Privatschlüssel für die erstmalige Authentifizierung verwenden. Die EA prüft die Authentifizierung anhand des kanonischen öffentlichen Schlüssels, der dem EE entspricht. Die kanonischen öffentlichen Schlüssel der EE werden der EA vor der Ausführung des ursprünglichen Antrags auf einem sicheren Kanal zwischen dem Hersteller oder Betreiber der C-ITS-Station und der EA übergeben (Ablauf 33).

(69) Die Endteilnehmer-Subjekte von AT authentifizieren sich bei der Beantragung von AT (Ablauf 32) selbst, indem sie ihren eindeutigen privaten Enrollment-Schlüssel verwenden. Die AA leitet die Signatur zur Validierung an die EA weiter (Ablauf 25); die EA validiert diese und bestätigt das Ergebnis der AA gegenüber (Ablauf 23).

3.2.4. Nicht verifizierte Angaben zu Abonnenten

Keine Bestimmung vorgesehen.

3.2.5. Validierung der Zertifizierungsstelle

3.2.5.1. Validierung von TLM, Root-CA, EA, AA

(70) Jede Organisation muss in der CPS mindestens einen Vertreter (z. B. einen Sicherheitsbeauftragten) benennen, der für die Beantragung neuer Zertifikate und Erneuerungen zuständig ist. Es gelten die Namensgebungsregeln in Abschnitt 3.2.3.

3.2.5.2. Validierung des Abonnenten der C-ITS-Station

(71) Mindestens eine natürliche Person, die für die Registrierung der C-ITS-Stationen bei einer EA verantwortlich ist (z. B. Sicherheitsbeauftragter) muss der EA bekannt und von ihr zugelassen sein (siehe Abschnitt 3.2.3).

3.2.5.3. Validierung von C-ITS-Stationen

(72) Ein Abonnent einer C-ITS-Station kann C-ITS-Stationen in einem bestimmten EA (Ablauf 33) registrieren lassen, sofern er von dieser EA authentifiziert wird.

Wird die C-ITS-Station mit einer eindeutigen kanonischen ID und einem kanonischen öffentlichen Schlüssel bei einer EA registriert, kann sie mittels eines Antrags, der mit dem kanonischen Privatschlüssel, der mit dem zuvor registrierten, kanonischen öffentlichen Schlüssel verbunden ist, signiert wurde, einen Enrollment-Berechtigungsnachweis (EC) beantragen.

3.2.6. Kriterien für die Interoperabilität

(73) Für die Kommunikation zwischen C-ITS-Stationen und EA (oder AA) muss die C-ITS-Station in der Lage sein, eine sichere Kommunikation mit EA (oder AA) herzustellen, d. h. Authentifizierungs-, Vertrauens- und Integritätsfunktionen gemäß Spezifikation in [1] zu implementieren Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist. Die EA und AA unterstützen diese sichere Kommunikation.

(74) Die EA und AA unterstützen Zertifikatanträge und Antworten, die konform mit [1] sind; dort ist ein sicheres Protokoll für die Beantragung/Beantwortung von AT vorgesehen, das die Anonymität des Antragstellers gegenüber der AA und die Aufgabentrennung zwischen AA und EA unterstützt. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist. Um eine Offenlegung der langfristigen Identität von C-ITS-Stationen zu verhindern, muss die Kommunikation zwischen einer mobilen C-ITS-Station und einer EA vertraulich sein (z. B. werden die Kommunikationsdaten durchgehend verschlüsselt „end-to-end“).

(75) Die AA übermittelt für jeden Auftrag auf Bevollmächtigung, den sie von einem Subjekt eines EE-Zertifikats erhält, ein Ersuchen um Validierung der Bevollmächtigung (Ablauf 25). Die EA validiert dieses Ersuchen in Bezug auf

- den Status der EE bei der EA;
- die Gültigkeit der Signatur;

- die beantragten ITS-Anwendungs-ID (ITS-AID) und -Berechtigungen;
- der Stand der Dienstleistungserbringung seitens AA gegenüber dem Abonnenten.

3.3. Identifizierung und Authentifizierung von Schlüsselerneuerungsanträgen (Re-Key)

3.3.1. Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerungsanträge

3.3.1.1. TLM-Zertifikate

(76) Der TLM generiert ein Schlüsselpaar und zwei Zertifikate: ein selbstsigniertes Zertifikat und ein Link-Zertifikat gemäß Abschnitt 7.

3.3.1.2. Root-CA-Zertifikate

Entfällt.

3.3.1.3. EA/AA-Zertifikatserneuerung oder Schlüsselerneuerung

(77) Bevor ein EA/AA-Zertifikat abläuft, beantragt die EA/AA ein neues Zertifikat (Ablauf 21/Ablauf 24), um die Kontinuität der Zertifikatsnutzung aufrechtzuerhalten. Die EA/AA generiert ein neues Schlüsselpaar zum Ersatz des ablaufenden Schlüsselpaars und signiert den Antrag auf Schlüsselerneuerung, der den neuen öffentlichen Schlüssel enthält, mit dem derzeit gültigen privaten Schlüssel („Schlüsselerneuerung“). Die EA oder AA generiert ein neues Schlüsselpaar und signiert den Antrag mit dem neuen privaten Schlüssel (innere Signatur) als Nachweis für den Besitz des neuen privaten Schlüssels. Der gesamte Antrag wird (gegengezeichnet) mit dem derzeit gültigen privaten Schlüssel (äußere Signatur) signiert, um die Integrität und Authentizität des Antrags zu gewährleisten. Wird ein Schlüsselpaar zur Ver- und Entschlüsselung verwendet, wird der Besitz privater Entschülsselungsschlüssel nachgewiesen (eine ausführliche Beschreibung der Schlüsselerneuerung ist Abschnitt 4.7.3.3 zu entnehmen).

(78) Die Identifizierungs- und Authentifizierungsmethode für routinemäßige Schlüsselerneuerungen entspricht der Methode für die Validierung der erstmaligen Ausstellung eines erstmaligen Root-CA-Zertifikats gemäß Abschnitt 3.2.2.

3.3.1.4. Berechtigungsnachweise von Endteilnehmern für das Enrollment (Anmeldung)

(79) Bevor ein bestehender EC (Berechtigungsnachweis) abläuft, beantragt der Endteilnehmer (EE) ein neues Zertifikat (Ablauf 31), um die Kontinuität der Zertifikatsnutzung aufrechtzuerhalten. Der EE generiert ein neues Schlüsselpaar, um das auslaufenden Schlüsselpaar zu ersetzen, und beantragt mit dem neuen öffentlichen Schlüssel ein neues Zertifikat; der Antrag wird mit dem derzeit gültigen privaten Schlüssel des EC signiert.

(80) Der EE (Endteilnehmer) kann den Antrag mit dem neu geschaffenen privaten Schlüssel (innere Signatur) unterzeichnen, um den Besitz des neuen privaten Schlüssels zu belegen. Anschließend wird der gesamte Antrag mit dem derzeit gültigen privaten Schlüssel signiert (gegengezeichnet) (äußere Signatur) und der empfangenden EA gegenüber gemäß Spezifikation in [1] verschlüsselt, um die Vertraulichkeit, Integrität und Authentizität des Antrags zu gewährleisten.

Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

3.3.1.5. Berechtigungstickets von Endteilnehmern

(81) Die Schlüsselerneuerung für Zertifikate für AT beruht auf demselben Verfahren wie die erstmalige Bevollmächtigung gemäß Definition in [1]. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

3.3.2. Identifizierung und Authentifizierung bei Schlüsselerneuerungsanträgen nach Zertifikatssperrung

3.3.2.1. CA-Zertifikate

(82) Die Authentifizierung einer CA-Organisation zur Schlüsselerneuerung für Root-CA-, EA- und AA-Zertifikate nach einer Sperrung wird in der gleichen Weise gehandhabt wie die erstmalige Ausstellung eines CA-Zertifikats gemäß Abschnitt 3.2.2.

3.3.2.2. Berechtigungsnachweise von Endteilnehmern für das Enrollment (Anmeldung)

(83) Die Authentifizierung eines EE (Endteilnehmers) zur Schlüsselerneuerung für ein EC-Zertifikat nach einer Sperrung wird in der gleichen Weise gehandhabt wie die erstmalige Ausstellung eines EE-Zertifikats gemäß Abschnitt 3.2.2.

3.3.2.3. Berechtigungsanträge von Endteilnehmern

Entfällt, da AT nicht gesperrt werden.

3.4. Identifizierung und Authentifizierung für Sperrungsantrag

3.4.1. Root-CA/EA/AA-Zertifikate

(84) Anträge auf Streichung eines Root-CA-Zertifikats aus der ECTL werden von der Root-CA dem TLM gegenüber authentifiziert (Abläufe 12 und 9). Anträge auf Sperrung eines EA/AA-Zertifikats werden von der maßgeblichen Root-CA und Sub-CA selbst authentifiziert.

(85) Zulässige Verfahren für die Authentifizierung von Sperranträgen eines Abonnenten sind unter anderem:

- eine schriftliche, unterschriebene Nachricht des Abonnenten auf dessen Firmenbriefpapier, mit der er unter Nennung des zu sperrenden Zertifikats die Sperrung beantragt;
- Kommunikation mit dem Abonnenten, der hinreichende Garantien dafür bietet, dass die Person oder Organisation, die die Sperrung beantragt, tatsächlich der Abonnent ist. Je nach Umständen kann eine solche Kommunikation einen oder mehrere folgender Wege beinhalten: E-Mail, Briefpost oder Kurierdienst.

3.4.2. Enrollment-Berechtigungsnachweise von C-ITS-Stationen

(86) Der Abonnent der C-ITS-Station kann den Enrollment-Berechtigungsnachweis (EC) einer zuvor registrierten C-ITS-Station bei einer EA sperren lassen (Ablauf 34). Der antragstellende Abonnent erstellt einen Antrag auf Sperrung einer bestimmten C-ITS-Station oder Liste von C-ITS-Stationen. Die EA authentifiziert den Sperrantrag vor der Verarbeitung und bestätigt die Sperrung der C-ITS-Stationen und ihrer Enrollment-Berechtigungsnachweise (EC).

(87) Die EA kann den EC einer C-ITS-Station im Einklang mit Abschnitt 7.3 sperren.

3.4.3. Berechtigungstickets von C-ITS-Stationen

(88) Da Berechtigungstickets (AT) nicht gesperrt werden, wird ihre Gültigkeit auf einen bestimmten Zeitraum begrenzt. Der Umfang zulässiger Gültigkeitszeiträume in der vorliegenden Certificate Policy wird in Abschnitt 7 spezifiziert.

4. BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

4.1. Zertifikatantrag

(89) In diesem Abschnitt werden die Anforderungen an einen Erstantrag auf Ausstellung eines Zertifikats dargelegt.

(90) Der Begriff „Zertifikatantrag“ bezieht sich auf folgende Vorgänge:

- Registrierung und Aufbau eines Vertrauensverhältnisses zwischen dem TLM und der CPA;
- Registrierung und Aufbau eines Vertrauensverhältnisses zwischen der Root-CA, der CPA und dem TLM, einschließlich der Aufnahme des ersten Root-CA-Zertifikats in die ECTL (Liste vertrauenswürdiger europäischer Zertifikate);
- Registrierung und Aufbau von Vertrauensverhältnissen zwischen der EA/AA und der Root-CA, einschließlich der Ausstellung eines neuen EA-/AA-Zertifikats;
- Registrierung der C-ITS-Station bei der EA durch den Hersteller/Betreiber;
- Antrag der C-ITS-Stelle auf EC/AT.

4.1.1. Wer kann einen Zertifikatantrag einreichen?

4.1.1.1. *Root-CA*

(91) Root-CA generieren ihre eigenen Schlüsselpaare und stellen ihr Wurzelzertifikat selbst aus. Eine Root-CA kann einen Zertifikatantrag durch ihren benannten Vertreter einreichen (Ablauf 14).

4.1.1.2. *TLM*

(92) Der TLM generiert seine eigenen Schlüsselpaare und stellt seine Zertifikate selbst aus. Die erstmalige Erstellung des TLM-Zertifikats wird von einem Vertreter der TLM-Organisation unter der Kontrolle der CPA verarbeitet.

4.1.1.3. EA und AA

(93) Die Anforderung eines Zertifikatantrags der Sub-CA (EA und/oder AA) kann von einem Bevollmächtigten der EA oder AA beim Bevollmächtigten der maßgeblichen Root-CA eingereicht werden (Ablauf 27/28).

4.1.1.4. C-ITS-Station

(94) Abonnenten registrieren im Einklang mit Abschnitt 3.2.5.3 jede C-ITS-Station bei der EA.

(95) Jede bei der EA registrierte C-ITS-Station kann Anträge auf Enrollment-Berechtigungsnachweise (EC) versenden (Ablauf 31).

(96) Jede C-ITS-Station kann Anträge auf Berechtigungstickets (AT) versenden (Ablauf 32), ohne Interaktionen mit Abonnenten anzufordern. Bevor eine C-ITS-Station einen AT beantragt, muss sie über einen EC verfügen.

4.1.2. Enrollment-Prozess und Verantwortlichkeiten

(97) Genehmigungen, dass Root-CA und Sub-CA Zertifikate für bestimmte (behördliche) Zwecke ausstellen dürfen (d. h. besondere mobile und ortsfeste C-ITS-Stationen), können nur von den Mitgliedstaaten erteilt werden, in denen die Organisationen ansässig sind.

4.1.2.1. *Root-CA*

(98) Nach ihrem Audit (Ablauf 13 und 36, Abschnitt 8) können Root-CA bei der CPA die Aufnahme ihres Zertifikats bzw. ihrer Zertifikate in die ECTL beantragen (Ablauf 14). Der Enrollment-Prozess basiert auf einem unterschriebenen, von Hand ausgefüllten Antragsformular, das der CPA vom Bevollmächtigten der Root-CA physisch übergeben wird und mindestens die in den Abschnitten 3.2.2.1, 3.2.3 und 3.2.5.1 genannten Angaben enthält.

(99) Das Antragsformular der CA wird von deren Bevollmächtigten unterzeichnet.

(100) Zusätzlich zum Antragsformular legt der Bevollmächtigte der Root-CA der CPA eine Kopie der Erklärung zum Zertifizierungsbetrieb (CPS) der Root-CA (Ablauf 15) und ihren Auditbericht zur Genehmigung vor (Ablauf 16). Im Falle eines positiven Bescheids generiert und versendet die CPA eine Konformitätsbescheinigung an die CPOC/den TLM und die entsprechende Root-CA.

(101) Anschließend übermittelt der Bevollmächtigte der Root-CA sein Antragsformular (mit dem „Fingerprint“ (Fingerabdruck) des selbstsignierten Zertifikats), die amtliche ID und einen Nachweis seiner Berechtigung an die CPOC/den TLM. Das selbstsignierte Zertifikat wird der CPOC/dem TLM elektronisch zugestellt. CPOC/TLM überprüfen alle Unterlagen und das selbstsignierte Zertifikat.

(102) Verlaufen die Überprüfungen positiv, fügt der TLM das Zertifikat der Root-CA auf der Grundlage der Benachrichtigung von der CPA (Abläufe 1 und 2) der ECTL hinzu. Der detaillierte Prozess wird in der CPS des TLM beschrieben.

(103) Ein zusätzliches Verfahren zur Einholung einer Genehmigung der CPS und des Auditberichts einer Root-CA bei einer nationalen Einrichtungen bestimmter Länder sollte möglich sein.

4.1.2.2. *TLM*

(104) Nach seinem Audit kann sich der TLM bei der CPA anmelden (Enrollment). Der Vorgang des Enrollments basiert auf einem unterschriebenen, von Hand ausgefüllten Antragsformular, das der CPA (Ablauf 38) vom Bevollmächtigten des TLM physisch übergeben wird und mindestens die in den Abschnitten 3.2.2.2 und 3.2.3 genannten Angaben enthält.

(105) Das Antragsformular des TLM wird von dessen Bevollmächtigten unterzeichnet.

(106) Der TIM generiert zunächst sein selbstsigniertes Zertifikat und übermittelt es sicher an die CPA. Anschließend übergibt der TLM sein Antragsformular (mit dem Fingerabdruck des selbstsignierten Zertifikats), eine Kopie seiner CPS, eine amtliche ID, einen Nachweis der Bevollmächtigung und seinen Auditbericht der CPA (Ablauf 40). Die CPA prüft alle Dokumente und das selbstsignierte Zertifikat. Verläuft die Überprüfung sämtlicher Dokumente, des selbstsignierten Zertifikats und des Fingerabdrucks positiv, bestätigt die CPA den Enrollment-Prozess, indem sie dem TLM und der CPOC ihre Genehmigung übermittelt (Ablauf 39). Die vom TLM übermittelten Antragsinformationen werden von der CPA gespeichert. Anschließend wird das TLM-Zertifikat über die CPOC ausgestellt.

4.1.2.3. EA und AA

(107) Im Zuge des Enrollment-Prozesses übermitteln die EA/AA der entsprechenden Root-CA die maßgeblichen Dokumente (z. B. die CPS und den Auditbericht) zur Genehmigung (Ablauf 27/28). Im Falle einer positiven Prüfung der Unterlagen erteilt die Root-CA den entsprechenden Sub-CA die Genehmigung (Ablauf 29/30). Die Sub-CA (EA oder AA) übermitteln anschließend ihren signierten Antrag elektronisch und stellen ihr Antragsformular (gemäß Abschnitt 3.2.2.1), den Bevollmächtigungsnachweis und das ID-Dokument der entsprechenden Root-CA physisch zu. Die Root-CA überprüft den Antrag und die eingegangenen Dokumente (Antragsformular mit dem Fingerabdruck, d.h. dem SHA 256 hashvalue des Antrags der Sub-CA, den Bevollmächtigungsnachweis und das ID-Dokument). Führen alle Prüfungen zu einem positiven Ergebnis, stellt die Root-CA das entsprechende Sub-CA-Zertifikat aus. Ausführliche Informationen darüber, wie ein erstmaliger Antrag erfolgt, wird in der spezifischen CPS beschrieben.

(108) Der Bevollmächtigte der Sub-CA fügt dem Antragsformular der Sub-CA an die Root-CA zusätzlich eine Kopie der CPS bei.

(109) Ein akkreditierter PKI-Prüfer erhält die Informationen zur Prüfung gemäß Abschnitt 8.

(110) Befindet sich eine Sub-CA im Besitz eines anderen Teilnehmers als des Teilnehmers, der Eigentümer der Root-CA ist, unterzeichnet der Teilnehmer der Sub-CA vor der Ausstellung eines Antrags auf ein Sub-CA-Zertifikat einen Vertrag über den Dienst der Root-CA.

4.1.2.4. C-ITS-Station

(111) Die erstmalige Registrierung der Subjekte von Endteilnehmern (C-ITS-Stationen) wird vom verantwortlichen Abonnenten (Hersteller/Betreiber) bei der EA durchgeführt (Abläufe 33 und 35) und erfolgt nach der erfolgreichen Authentifizierung der Organisation des Abonnenten und eines seiner Vertreter gemäß den Abschnitten 3.2.2.4 und 3.2.5.2.

(112) Eine C-ITS-Station kann ein EC-Schlüsselpaar generieren (siehe Abschnitt 6.1) und einen signierten EC-Antrag gemäß [1] erstellen. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(113) Bei der Registrierung einer normalen C-ITS-Station (im Gegensatz zu einer speziellen mobilen oder ortsfesten C-ITS-Station) muss die EA prüfen, ob die Genehmigungen im erstmaligen Auftrag nicht für behördliche Zwecke

bestimmt sind. Die Genehmigungen für behördliche Zwecke werden von den entsprechenden Mitgliedstaaten festgelegt. Das ausführliche Registrierungs- und Beantwortungsverfahren der EA bezüglich des Herstellers/Betreibers (Abläufe 33 und 35) wird in der entsprechenden CPS der EA dargelegt.

(114) Das Enrollment einer C-ITS-Station bei einer EA (Abschnitt 3.2.5.3) erfolgt gemäß [1] mittels Übermittlung ihres erstmaligen EC-Antrags.

(115) Nach der erstmaligen Registrierung durch einen authentifizierten Abonnentenvertreter genehmigt die EA die AT, die das Subjekt des Endteilnehmers (d. h. die C-ITS-Station) erwirken kann. Darüber hinaus wird jedem Endteilnehmer eine Vertrauenszusicherungsebene zugewiesen, die mit der Zertifizierung des Endteilnehmers nach einem der in Abschnitt 6.1.5.2 aufgeführten Schutzprofile zusammenhängt

(116) Reguläre Fahrzeuge müssen nur über eine C-ITS-Station verfügen, die bei einer EA registriert ist. Sonderfahrzeuge (wie Polizeiwagen und andere Sonderfahrzeuge mit besonderen Rechten) können bei einer zusätzlichen EA registriert werden oder verfügen über eine zusätzliche C-ITS-Station für Autorisierungen innerhalb des Geltungsbereichs ihres besonderen Zwecks. Die Fahrzeuge, für die eine solche Ausnahme gilt, werden von den zuständigen Mitgliedstaaten festgelegt. Die Genehmigungen für spezielle mobile und ortsfeste C-ITS-Stationen werden nur von den zuständigen Mitgliedstaaten erteilt. In den CPS der Root-CA oder Sub-CA, die Zertifikate für derartige Fahrzeuge in den betreffenden Mitgliedstaaten ausstellen, wird festgelegt, in welcher Weise der Zertifizierungsprozess für derartige Fahrzeuge zutrifft.

(117) Durchläuft der Abonnent gerade einen Prozess zur Migration einer C-ITS-Station von einer EA zu einer anderen EA, kann die C-ITS bei zwei (ähnlichen) EA registriert werden.

(118) Eine C-ITS-Station generiert ein AT-Schlüsselpaar (siehe Abschnitt 6.1) und erstellt einen signierten AT-Antrag gemäß [1]. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(119) Die C-ITS-Stationen senden einen Antrag auf Autorisierung an die URL der AA (Abläufe 32 und 26), indem sie mindestens die in Abschnitt 3.2.3.3 genannten, erforderlichen Informationen übermitteln. Die AA und EA validieren die Autorisierung für jeden Antrag gemäß den Abschnitten 3.2.6 und 4.2.2.5.

4.2. Bearbeitung von Zertifikatanträgen

4.2.1. Durchführung von Identifikations- und Authentifizierungsaufgaben

4.2.1.1. Identifizierung und Authentifizierung von Root-CA

(120) Der Bevollmächtigte der CPA ist für die Authentifizierung des Bevollmächtigten der Root-CA und die Genehmigung von dessen Enrollment-Prozess nach Abschnitt 3 zuständig.

4.2.1.2. Identifizierung und Authentifizierung des TLM

(121) Der Bevollmächtigte der CPA ist für die Authentifizierung des Bevollmächtigten des TLM und die Genehmigung von dessen im Rahmen des Enrollment-Prozesses nach Abschnitt 3 eingereichten Antragsformular nach Abschnitt 3 zuständig.

4.2.1.3. Identifizierung und Authentifizierung von EA und AA

(122) Die entsprechende Root-CA ist für die Authentifizierung des Bevollmächtigten der EA/AA und die Genehmigung von dessen im Rahmen des Enrollment-Prozesses eingereichten Antragsformular nach Abschnitt 3 zuständig.

(123) Die Root-CA bestätigt die positive Validierung des Antragsformulars bei der EA/AA. Die EA/AA kann anschließend einen Antrag auf Erteilung eines Zertifikats an die Root-CA richten (Ablauf 21/24), die Zertifikate für die entsprechende EA/AA ausstellt (Ablauf 18/19).

4.2.1.4. Identifizierung und Authentifizierung des EE-Abonnenten

(124) Bevor eine C-ITS-Station einen Antrag auf Ausstellung eines EC-Zertifikats stellen kann, muss der EE-Abonnent der EA die Angaben zur Kennung der C-ITS-Station sicher übermitteln (Ablauf 33). Die EA prüft den Antrag und trägt im Fall einer positiv verlaufenen Überprüfung die Angaben zur C-ITS-Station in ihre Datenbank ein und bestätigt dies dem EE-Abonnenten gegenüber (Ablauf 35). Dieser Vorgang wird für jede C-ITS-Station nur einmal durch den Hersteller oder Betreiber durchgeführt. Sobald eine C-ITS-Station bei einer EA registriert wird, kann sie jeweils ein einzelnes, von ihr benötigtes EC-Zertifikat beantragen (Ablauf 31). Die EA authentifiziert und verifiziert, ob die Angaben im EG-Zertifikatantrag für die betreffende C-ITS-Station gültig sind.

4.2.1.5. Berechtigungstickets

(125) Im Zuge von Autorisierungsanträgen (Ablauf 32) nach [1] muss die AA die EA authentifizieren, von der die C-ITS-Station ihren Enrollment-Berechtigungsnachweis (EC) erhalten hat. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist. Ist die AA nicht in der Lage, die EA zu authentifizieren, wird der Antrag abgelehnt (Ablauf 26). Es gilt die Anforderung, dass sich das EA-Zertifikat zur Authentifizierung der EA und zur Verifizierung ihrer Antworten im Besitz der AA befinden muss (Abläufe 25 und 23, Abschnitt 3.2.5.3).

(126) Die EA authentifiziert die C-ITS-Station, die ein Berechtigungsticket (AT) anfordert, indem sie deren EC verifiziert (Abläufe 25 und 23).

4.2.2. Genehmigung oder Ablehnung von Zertifikatanträgen

4.2.2.1. Genehmigung oder Ablehnung von Root-CA-Zertifikaten

(127) Der TLM trägt im Einklang mit der Genehmigung der CPA die Root-CA-Zertifikate in die ECTL ein bzw. entfernt sie daraus (Ablauf 1/2).

(128) Der TLM sollte nach dem Empfang der Genehmigung durch die CPA (Ablauf 1) die Signatur, die Informationen und die Verschlüsselung der Root-CA-Zertifikate verifizieren. Nach positiv verlaufener Validierung und Genehmigung durch die CPA setzt der TLM das entsprechende Wurzelzertifikat auf die ECTL und benachrichtigt die CPA (Ablauf 5).

4.2.2.2. *Genehmigung oder Ablehnung von TLM-Zertifikaten*

(129) Die CPA ist für die Genehmigung oder Ablehnung von TLM-Zertifikaten zuständig.

4.2.2.3. *Genehmigung oder Ablehnung von EA- und AA-Zertifikaten*

(130) Die Root-CA überprüft die Zertifikatanträge der Sub-CA (Ablauf 21/24) und die maßgeblichen (von einem akkreditierten PKI-Prüfer herausgegebenen) Berichte (Ablauf 36, Abschnitt 8), sobald sie diese von den entsprechenden Sub-CA der Root-CA erhalten hat. Führt die Prüfung des Antrags zu einem positiven Ergebnis, stellt die entsprechende Root-CA der antragstellenden EA/AA ein Zertifikat aus (Ablauf 18/19); andernfalls wird der Antrag abgelehnt, und der EA/AA wird kein Zertifikat ausgestellt.

4.2.2.4. Genehmigung oder Ablehnung von EC

(131) Die EA überprüft und validiert EC-Anträge im Einklang mit den Abschnitten 3.2.3.2 und 3.2.5.3.

(132) Ist der Zertifikatantrag nach [1] korrekt und gültig, generiert die EA das beantragte Zertifikat.

(133) Ist der Zertifikatantrag nicht gültig, lehnt die EA (Enrollment-Stelle) ihn ab und übermittelt eine Antwort, in der sie den Grund für die Ablehnung gemäß [1] darlegt. Wünscht eine C-ITS-Station weiterhin einen EC, kann sie einen neuen Zertifikatantrag stellen. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

4.2.2.5. Genehmigung oder Ablehnung von AT

(134) Der Zertifikatantrag wird durch die EA geprüft. Die AA kommuniziert zur Validierung des Antrags mit der EA (Ablauf 25). Die Enrollment-Stelle (EA) authentifiziert die antragstellende C-ITS-Station und validiert, ob sie zum Empfang des beantragten Berechtigungstickets (AT) berechtigt ist, dabei folgt sie der Certificate Policy (CP) (z. B. mittels Prüfung des Sperrungsstatus und Validierung der zeitlichen/regionalen Gültigkeit des Zertifikats, der Zulassungen, der Vertrauenszusicherungsebene usw.). Die EA sendet eine Validierungsantwort (Ablauf 23); ist die Antwort positiv, generiert die AA das beantragte Zertifikat und übermittelt es an die C-ITS-Station. Ist der AT-Antrag nicht korrekt oder ist die Validierungsantwort der EA negativ, lehnt die AA den Antrag ab. Benötigt eine C-ITS-Station weiterhin ein Berechtigungsticket (AT), stellt sie einen neuen Antrag auf Autorisierung.

4.2.3. Bearbeitungsdauer von Zertifikatanträgen

4.2.3.1. Antrag auf Root-CA-Zertifikat

(135) Die Bearbeitungszeit für den Identifizierungs- und Authentisierungsprozess eines Zertifikatantrags liegt innerhalb eines Arbeitstags und unterliegt einer maximalen Frist, die in der Erklärung zum Zertifizierungsbetrieb (CPS) der Root-CA festgelegt ist.

4.2.3.2. *Antrag auf TLM-Zertifikat*

(136) Für die Bearbeitung des TLM-Zertifikatantrags gilt eine in der CPS des TLM festgelegte Höchstdauer.

4.2.3.3. *Antrag auf EA- und AA-Zertifikate*

(137) Die Bearbeitungszeit für den Identifizierungs- und Authentisierungsprozess eines Zertifikatantrags liegt im Einklang mi der Vereinbarung und dem Vertrag zwischen der Root-CA von Mitgliedstaat/privater Organisation und der Sub-

CA innerhalb eines Arbeitstags. Für die Bearbeitung von Anträgen auf Sub-CA-Zertifikate gilt eine maximale Frist, die in der Erklärung zum Zertifizierungsbetrieb (CPS) der Sub-CA festgelegt ist.

4.2.3.4. *EC-Antrag*

(138) Für die Bearbeitung von EC-Anträgen (Enrollment-Berechtigungsnachweis) gilt eine maximale Frist, die in der Erklärung zum Zertifizierungsbetrieb (CPS) der Enrollment-Stelle (EA) festgelegt ist.

4.2.3.5. *AT-Antrag*

(139) Für die Bearbeitung von AT-Anträgen (Berechtigungsticket) gilt eine maximale Frist, die in der Erklärung zum Zertifizierungsbetrieb (CPS) der AA festgelegt ist.

4.3. Zertifikatsausstellung

4.3.1. Maßnahmen der Wurzelzertifizierungsstelle während der Ausstellung von Zertifikaten

4.3.1.1. Ausstellung von Zertifikaten für die Root-CA

(140) Root-CA stellen ihre eigenen, selbstsignierten Root-CA-Zertifikate, Link-Zertifikate, Sub-CA-Zertifikate und CRL aus.

(141) Nach der Genehmigung durch die CPA (Ablauf 4) sendet die Root-CA ihr Zertifikat über die CPOC zur Aufnahme in die ECTL an dem TLM (Abläufe 11 und 8) (siehe Abschnitt 4.1.2.1). Der TLM prüft, ob die CPA das Zertifikat genehmigt hat (Ablauf 1).

4.3.1.2. *Ausstellung von TLM Zertifikaten*

(142) Der TLM stellt seine eigenen selbstsignierten TLM- und Link-Zertifikate aus und sendet sie an die CPOC (Ablauf 6).

4.3.1.3. Ausstellung von EA- und AA-Zertifikaten

(143) Die Sub-CA generieren einen signierten Zertifikatantrag und übermitteln ihn an die entsprechende Root-CA (Abläufe 21 und 24). Die Root-CA überprüft den Antrag und stellt der antragstellenden Sub-CA gemäß [5] sobald wie möglich, d. h. den in der CPS für die übliche betriebliche Praxis festgelegten Bestimmungen entsprechend, spätestens aber fünf Arbeitstage nach Eingang des Antrags, ein Zertifikat aus.

(144) Die Root-CA aktualisiert die Datenablage, die die Zertifikate der Sub-CA enthält.

4.3.1.4. Ausstellung von EC

(145) Die C-ITS-Station übermittelt der EA einen Antrag auf einen Enrollment-Berechtigungsnachweis (EC) gemäß [1]. Die EA authentifiziert und überprüft, ob die im Zertifikatantrag enthaltenen Informationen für eine C-ITS-Station gültig sind. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(146) Im Falle einer positiven Validierung stellt die EA ein der Registrierung der C-ITS-Station (siehe 4.2.1.4) entsprechendes Zertifikat aus und sendet es mittels einer EC-Antwortnachricht nach [1] an die C-ITS-Station. Andere Protokolle

können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(147) Besteht keine Registrierung, generiert die EA einen Fehlercode und sendet ihn mittels einer EC-Antwortnachricht nach [1] an die C-ITS-Station. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(148) EC-Anträge und EC-Antworten werden zur Wahrung der Vertraulichkeit verschlüsselt und zur Gewährleistung der Authentifizierung und Integrität signiert.

4.3.1.5. Ausstellung von AT

(149) Die C-ITS-Station übermittelt der AA eine Nachricht mit einem Antrag auf ein Berechtigungsticket (AT) gemäß [1]. Die AA übermittelt der EA ein AT-Validierungsersuchen gemäß [1]. Die EA übermittelt der AA eine Antwort zur AT-Validierung. Ist die Antwort positiv, generiert die AA ein Berechtigungsticket (AT) und sendet es mittels einer AT-Antwortnachricht nach [1] an die C-ITS-Station. Ist die Antwort negativ, generiert die AA einen Fehlercode und sendet ihn mittels einer AT-Antwortnachricht nach [1] an die C-ITS-Station. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(150) AT-Anträge und AT-Antworten werden zur Wahrung der Vertraulichkeit verschlüsselt (nur bei mobilen C-ITS-Stationen erforderlich) und zur Gewährleistung der Authentifizierung und Integrität signiert.

4.3.2. Benachrichtigung des Abonnenten über die Ausstellung von Zertifikaten durch die Zertifizierungsstelle

Entfällt.

4.4. Annahme der Zertifikate

4.4.1. Durchführung der Annahme von Zertifikaten

4.4.1.1. *Root-CA*

Entfällt.

4.4.1.2. *TLM*

Entfällt.

4.4.1.3. EA und AA

(151) Die EA/AA überprüft die Art des Zertifikats, die Signatur und die im empfangenen Zertifikat enthaltenen Angaben. Die EA/AA verwirft alle EA/AA-Zertifikate, die nicht als korrekt verifiziert wurden, und stellt einen neuen Antrag.

4.4.1.4. C-ITS-Station

(152) Die C-ITS-Station überprüft die EC/AT-Antwort, die sie von der EA/AA erhalten hat, anhand ihres ursprünglichen Antrags unter Einschluss der Signatur und der Zertifikatkette. Sie verwirft alle EC/AT-Antworten, die nicht als korrekt verifiziert wurden. In diesen Fällen sollte sie einen neuen EC/AT-Antrag übermittelt.

4.4.2. Veröffentlichung des Zertifikats

(153) TLM-Zertifikate und die zugehörigen Link-Zertifikate werden allen Teilnehmern über die CPOC zur Verfügung gestellt.

(154) Root-CA-Zertifikate werden vom CPOC über die ECTL veröffentlicht, die vom TLM signiert wird.

(155) Die Zertifikate von Sub-CA (EA und AA) werden von der Root-CA veröffentlicht.

(156) EC und AT werden nicht veröffentlicht.

4.4.3. Benachrichtigung über die Zertifikatsausstellung

Es gibt keine Benachrichtigungen über die Ausstellung.

4.5. Verwendung des Schlüsselpaars und des Zertifikats

*4.5.1. **Nutzung des privaten Schlüssels und des Zertifikats***

4.5.1.1. Nutzung privater Schlüssel und Zertifikate für TLM

(157) Der TLM nutzt seine privaten Schlüssel zur Signierung seiner eigenen (TLM- und Link-) Zertifikate und der ECTL.

(158) Das TLM-Zertifikat wird von den PKI-Teilnehmern für die Überprüfung des ECTL und die Authentifizierung des TLM verwendet.

4.5.1.2. Nutzung privater Schlüssel und Zertifikate für Root-CA

(159) Root-CA nutzen ihre privaten Schlüssel zur Signierung ihrer eigenen Zertifikate, CRL, Link-Zertifikate und der EA/AA-Zertifikate.

(160) Root-CA-Zertifikate werden von den PKI-Teilnehmern für die Überprüfung der zugehörigen AA und EA-Zertifikate, der Link-Zertifikate und der CRL verwendet.

4.5.1.3. Nutzung privater Schlüssel und Zertifikats für EA und AA

(161) EA nutzen ihre privaten Schlüssel zur Signierung von EC und Entschlüsselung von Enrollment-Anträgen.

(162) EA-Zertifikate werden zur Verifizierung der Signatur zugehöriger EC und zur Verschlüsselung von EC- und AT-Anträgen durch EE gemäß Definition in [1]verwendet.

(163) AA nutzen ihre privaten Schlüssel zur Signierung von AT und zur Entschlüsselung von Anträgen auf AT (Berechtigungstickets).

(164) AA-Zertifikate werden von Endteilnehmern (EE) zur Verifizierung zugehöriger AT und zur Verschlüsselung von AT-Anträgen gemäß Definition in [1] verwendet.

4.5.1.4. Nutzung privater Schlüssel und Zertifikate für Endteilnehmer

(165) Endteilnehmer (EE) nutzen den einem gültigen EC (Enrollment-Berechtigungsnachweis) entsprechenden privaten Schlüssel zur Signierung eines neuen Enrollment-Antrags gemäß Definition in [1]. Der neue private Schlüssel wird zum Aufbau der inneren Signatur im Antrag verwendet, um den Besitz des privaten Schlüssels zu belegen, der dem neuen öffentlichen EC-Schlüssel entspricht.

(166) Endteilnehmer (EE) nutzen den einem gültigen EC (Enrollment-Berechtigungsnachweis) entsprechenden privaten Schlüssel zur Signierung eines Autorisierungsantrags gemäß Definition in [1]. Der dem neuen AT (Berechtigungsticket) entsprechende private Schlüssel wird zum Aufbau der inneren Signatur im Antrag verwendet, um den Besitz des privaten Schlüssels zu belegen, der dem neuen öffentlichen AT-Schlüssel entspricht.

(167) Endteilnehmer (EE) nutzen den einem ordnungsgemäßen AT entsprechenden privaten Schlüssel zum Signieren von C-ITS-Nachrichten gemäß Definition in [5].

4.5.2. ***Nutzung öffentlicher Schlüssel und Zertifikate durch Vertrauende Dritte***

(168) Vertrauende Dritte nutzen den vertrauenswürdigen Zertifizierungspfad und die zugehörigen öffentlichen Schlüssel zu den in den Zertifikaten genannten Zwecken und zur Authentifizierung der vertrauenswürdigen gemeinsamen Identität von EC und AT.

(169) Root-CA- EA- und AA-Zertifikate sowie EC und AT dürfen ohne eine Vorabprüfung durch einen Vertrauenden Dritten nicht verwendet werden.

4.6. Zertifikatserneuerung

Nicht zulässig.

4.7. Schlüsselerneuerung von Zertifikaten (Re-Key)

4.7.1. Umstände für eine Schlüsselerneuerung

(170) Schlüsselerneuerungen von Zertifikaten werden bearbeitet, wenn ein Zertifikat das Ende seiner Laufzeit erreicht oder wenn bei einem privaten Schlüssel die betriebliche Nutzung endet, das Vertrauensverhältnis mit der Wurzelzertifizierungsstelle (CA) aber noch besteht. Ein neues Schlüsselpaar und das entsprechende Zertifikat werden in allen Fällen generiert und ausgestellt.

4.7.2. Wer darf eine Schlüsselerneuerung beantragen?

4.7.2.1. *Root-CA*

(171) Die Root-CA beantragt keine Schlüsselerneuerung. Der Schlüsselerneuerungsprozess stellt für die Root-CA einen internen Vorgang dar, weil ihr Zertifikat von ihr selbst signiert wird. Die Root-CA führt Schlüsselerneuerungen entweder mit Link-Zertifikaten oder Neuausstellungen durch (siehe Abschnitt 4.3.1.1).

4.7.2.2. *TLM*

(172) Der TLM beantragt keine Schlüsselerneuerung. Der Schlüsselerneuerungsprozess stellt für den TLM einen internen Vorgang dar, weil das TLM-Zertifikat von ihm selbst signiert wird.

4.7.2.3. EA und AA

(173) Der Zertifikatantrag von Sub-CA muss rechtzeitig eingereicht werden, um sicher sein zu können, dass ein neues Sub-CA-Zertifikat und ein funktionsfähiges Sub-CA-Schlüsselpaar vorliegt, bevor der aktuelle private Schlüssel der Sub-CA abläuft. Hinsichtlich des Datums der Einreichung muss auch die für die Genehmigung benötigte Zeit berücksichtigt werden.

4.7.2.4. C-ITS-Station

Entfällt.

4.7.3. Schlüsselerneuerungsprozess

4.7.3.1. TLM-Zertifikat

(174) Der TLM entscheidet auf der Grundlage der in den Abschnitten 6.1 und 7.2 aufgeführten Anforderungen über eine Schlüsselerneuerung. Der Prozess wird in seiner Erklärung zum Zertifizierungsbetrieb (CPS) ausführlich beschrieben.

(175) Der TLM führt den Prozess der Schlüsselerneuerung so rechtzeitig durch, dass die Verteilung des neuen TLM-Zertifikats und des Link-Zertifikats an alle Teilnehmer möglich ist, bevor das derzeitige TLM-Zertifikat abläuft.

(176) Der TLM verwendet für die Schlüsselerneuerung und zur Gewährleistung des Vertrauensverhältnisses des neuen, selbstsignierten Zertifikats Link-Zertifikate. Das neu generierte TLM- und Link-Zertifikat wird an die zentrale Kontaktstelle (CPOC) übertragen.

4.7.3.2. Root-CA-Zertifikat

(177) Die Root-CA entscheidet auf der Grundlage der in den Abschnitten 6.15 und 7.2 aufgeführten Anforderungen über eine Schlüsselerneuerung. Der Prozess in seinen Einzelheiten sollte in ihrer Erklärung zum Zertifizierungsbetrieb (CPS) festgelegt werden.

(178) Die Root-CA führt den Schlüsselerneuerungsprozess so rechtzeitig (bevor das Root-CA-Zertifikat abläuft) durch, dass das neue Zertifikat in die ECTL aufgenommen werden kann, bevor das Zertifikat der Root-CA gültig wird (siehe Abschnitt 5.6.2). Der Schlüsselerneuerungsprozess erfolgt entweder über Link-Zertifikate oder wie ein erstmaliger Antrag.

4.7.3.3. EA- und AA-Zertifikate

(179) Die EA oder AA beantragt ein neues Zertifikat wie folgt:

Schritt	**Angabe**	**Antrag auf Schlüsselerneuerung**
1	**Generierung eines Schlüsselpaars**	Die Sub-CA (EA und AA) generieren gemäß Abschnitt 6.1 neue Schlüsselpaare.
2	**Generierung des Zertifikatantrags und der inneren Signatur**	Die Sub-CA generiert aus dem neu generierten öffentlichen Schlüssel einen Zertifikatantrag und berücksichtigt dabei das Benennungsschema (subject_info) in Abschnitt 3, den Signaturalgorithmus, die SSP und optionale zusätzliche Parameter; ferner generiert sie mit dem entsprechenden neuen privaten Schlüssel die innere Signatur. Ist ein Verschlüsselungsschlüssel erforderlich, muss die Sub-CA auch den Besitz des entsprechenden privaten Entschlüsselungsschlüssels nachweisen.
3	**Äußere Signatur generieren**	Der gesamte Antrag wird zur Gewährleistung der Authentizität des signierten Antrags mit dem derzeit gültigen privaten Schlüssel signiert.
4	**Antrag an Root-CA versenden**	Der unterzeichnete Antrag wird bei der entsprechenden Root-CA eingereicht.
5	**Prüfung des Antrags**	Die entsprechende Root-CA überprüft die Integrität und Authentizität (Echtheit) des Antrags. Zunächst überprüft sie die äußere Signatur. Verläuft die Prüfung positiv, überprüft sie die innere Signatur. Liegt

		ein Nachweis für den Besitz des privaten Entschlüsselungsschlüssels vor, überprüft sie auch diesen Nachweis.
6	**Antrag annehmen oder ablehnen**	Wenn alle Kontrollen zu einem positiven Ergebnis führen, nimmt die Root-CA den Antrag an; andernfalls wird er abgelehnt.
7	**Zertifikat generieren und ausstellen**	Die Root-CA generiert ein neues Zertifikat und verteilt es an die antragstellenden Sub-CA.
8	**Antwort senden**	Die Sub-CA sendet der Root-CA eine Statusmeldung (bezüglich dessen, ob das Zertifikat eingegangen ist oder nicht).

Tabelle 3: Schlüsselerneuerungsprozess für EA und AA

(180) Bei einer automatischen Schlüsselerneuerung für Sub-CA stellt die Root-CA sicher, dass der Antragsteller tatsächlich im Besitz seines privaten Schlüssels ist. Es werden geeignete Protokolle für den Besitznachweis für private Entschlüsselungsschlüssel angewendet, beispielsweise die in RFC 4210 und 4211 definierten Protokolle. Für private Signaturschlüssel sollte die innere Signatur verwendet werden.

4.7.3.4. C-ITS-Stationszertifikate

Trifft für Berechtigungstickets (AT) nicht zu.

4.8. Änderung von Zertifikaten

Nicht zulässig.

4.9. Sperrung und Suspendierung von Zertifikaten

Siehe Abschnitt 7.

4.10. Statusauskunftsdienste von Zertifikaten

4.10.1. Betriebseigenschaften

Entfällt.

4.10.2. Verfügbarkeit des Dienstes

Entfällt.

4.10.3. Optionale Funktionen

Entfällt.

4.11. Beendigung des Vertragsverhältnisses

Entfällt.

4.12. Schlüsselhinterlegung und Wiederherstellung

4.12.1. Teilnehmer

4.12.1.1. Welches Schlüsselpaar kann hinterlegt werden?

Entfällt.

4.12.1.2. Wer kann einen Wiederherstellungsantrag stellen?

Entfällt.

4.12.1.3. Wiederherstellungsprozess und Verantwortlichkeiten

Entfällt.

4.12.1.4. Identifizierung und Authentifizierung

Entfällt.

4.12.1.5. Genehmigung oder Ablehnung von Wiederherstellungsanträgen

Entfällt.

4.12.1.6. KEA und KRA bei der Wiederherstellung von Schlüsselpaaren

Entfällt.

4.12.1.7. Verfügbarkeit von KEA und KRA

Entfällt.

4.12.2. Sitzungsschlüsselkapselung und Richtlinien und Praktiken für die Wiederherstellung

Entfällt.

5. EINRICHTUNGS-, VERWALTUNGS- UND BETRIEBSKONTROLLEN

(181) Die PKI besteht aus der Root-CA, den EA/AA, der CPOC und dem TLM, einschließlich ihrer IKT-Komponenten (z. B. Netze und Server).

(182) In diesem Abschnitt wird die für einen Bestandteil der PKI verantwortliche Stelle durch das Element selbst bestimmt. Mit anderen Worten: der Satz „die CA ist für die Durchführung der Prüfung zuständig“ ist gleichbedeutend mit „zuständig für die Durchführung ... ist die Stelle oder das Personal, die oder das die CA verwaltet“.

(183) Der Begriff „Elemente des C-ITS Trust Models“ umfasst die Root-CA, den TLM, die EA/AA, die CPOC und das sichere Netz.

5.1. Physische Kontrollen

(184) Alle Vorgänge im Rahmen des C-ITS Trust Models werden in einem physisch geschützten Umfeld durchgeführt, das vor der unbefugten Nutzung sensibler Informationen und Systeme, dem Zugang dazu oder vor deren Offenlegung abschreckt, diese verhindert und aufdeckt. Elemente des C-ITS Trust Models nutzen physische Sicherheitskontrollen im Einklang mit ISO 27001 und ISO 27005.

(185) Die Stellen, die die Elemente für die C-ITS-Vertrauenselemente verwalten, beschreiben die physischen, verfahrenstechnischen und personellen Sicherheitskontrollen in ihren CPS. Insbesondere müssen die CPS Informationen über den Standort und die Bauweise der Einrichtungen und ihre physischen Sicherheitskontrollen umfassen, die den kontrollierten Zugang zu allen Räumen gewährleisten, die in Einrichtungen der für das C-ITS Trust Model zuständigen Stellen genutzt werden.

5.1.1. Standort und Bauweise

5.1.1.1. Root-CA, CPOC, TLM

(186) Standort und Bauweise der Einrichtung, in der die Geräte und Daten von Root-CA, CPOC und TLM untergebracht sind (HSM, Aktivierungsdaten, Backup von Schlüsselpaaren, Rechner, Log, Skript des Schlüsselgenerierungsverfahrens (Key Ceremony), Zertifikatanträge usw.), entsprechen Einrichtungen, die für die Unterbringung sensibler Informationen

von hohem Wert genutzt werden. Die Root-CA wird in einem speziell dafür bestimmten Bereich betrieben, der von physischen Bereichen anderer PKI-Komponenten getrennt ist.

(187) Die Root-CA, die CPOC und der TLM führen Richtlinien und Verfahren zur Sicherstellung dessen ein, dass in der physischen Umgebung, in der die Geräte der Root-CA untergebracht sind, ein hohes Maß an Sicherheit gewährleistet ist; damit soll garantiert werden, dass

- es von Netzen außerhalb des Trust Models getrennt ist;
- es in eine Reihe von (mindestens zwei) physischen Perimetern mit schrittweise höheren Sicherheitsstufen unterteilt ist;
- sensible Daten (HSM, Schlüsselpaar-Backup, Aktivierungsdaten usw.) in einem dafür vorgesehenen Safe in einem speziell dafür bestimmten Bereich unter mehrfacher Zugangskontrolle gespeichert werden.

(188) Die eingesetzten Sicherheitstechniken müssen darauf ausgelegt sein, gegen eine große Anzahl und Kombination verschiedener Angriffsformen Widerstand zu leisten. Die verwendeten Mechanismen müssen mindestens Folgendes umfassen:

- perimetrische Warnanlagen, Videoüberwachungssysteme, verstärkte Mauern und Bewegungsmelder;
- zwei-Faktoren-Authentifizierung (z. B. Smartcard und PIN) für jede Person und einen Zugangsausweis zum Betreten und Verlassen der Einrichtungen der Root-CA und des sicheren, physisch abgesicherten Bereichs.

(189) Die Root-CA, die CPOC und der TLM setzen befugtes Personal zur ständigen Überwachung (7x24x365-Basis) der Einrichtung ein, in der Geräte untergebracht sind. Das Betriebsumfeld (z. B. die physische Einrichtung) darf nie unbeaufsichtigt sein. Das Personal aus dem betrieblichen Umfeld darf nur dann Zutritt zu gesicherten Bereichen von Root-CA oder Sub-CA erhalten, wenn es dazu befugt ist.

5.1.1.2. *EA/AA*

(190) Es gelten die gleichen Bestimmungen wie in Abschnitt 5.1.1.1.

5.1.2. Physischer Zugang

5.1.2.1. Root-CA, CPOC, TLM

(191) Geräte und Daten (HSM, Aktivierungsdaten, Backup von Schlüsselpaaren, Rechner, Logs, Skript des Schlüsselgenerierungsverfahrens (Key Ceremony), Zertifikatanträge usw.) sind stets vor unbefugtem Zugang zu schützen. Die Mechanismen für die physische Sicherheit der Geräte müssen mindestens:

- eine ständige manuelle oder elektronische Überwachung auf unbefugtes Eindringen leisten;
- sicherstellen, dass kein unbefugter Zugang zur Hardware und zu den Aktivierungsdaten zugelassen wird;

- sicherstellen, dass alle transportablen Medien und Dokumente, die sensible Informationen in Klartext enthalten, in einem sicheren Behältnis aufbewahrt werden;
- sicherstellen, dass jede Person, die sichere Bereiche betritt und über keine dauernde Befugnis verfügt, stets unter der Aufsicht durch einen bevollmächtigten Mitarbeiter der Einrichtungen von Root-CA, CPOC oder TLM steht;
- sicherstellen, dass ein Zugangsprotokoll geführt und in regelmäßigen Abständen überprüft wird;
- mindestens zwei Ebenen schrittweise höherer Sicherheitsstufen bereitstellen, z. B. auf den Ebenen Grundstücksgrenze, Gebäude und Betriebsraum;
- zwei Vertrauensfunktionen erfüllende, physische Zugangskontrollen für das kryptografische Hardware-Sicherheitsmodul (HSM) und die Aktivierungsdaten vorschreiben.

(192) Am Gebäude, in dem Geräte untergerbacht sind, ist eine Sicherheitskontrolle durchzuführen, wenn dieses unbeaufsichtigt gelassen werden soll. Bei der Kontrolle wird zumindest überprüft, ob

- sich die Geräte in einem Zustand befinden, der für die derzeitige Betriebsweise geeignet ist;
- bei Offline-Komponenten alle Geräte abgeschaltet sind;
- Sicherheitsbehältnisse (manipulationssicherer Umschlag, Safe usw.) ordnungsgemäß versiegelt sind;
- die Systeme der physischen Sicherheit (z. B. Türschlösser, Lüftungsabdeckungen, Strom) ordnungsgemäß funktionieren;
- der Bereich gegen unbefugten Zutritt gesichert ist.

(193) Transportable kryptografische Module müssen vor der Lagerung deaktiviert werden. Befinden sich diese Module nicht im Einsatz, werden sie und die zugehörigen Zugangs- oder Aktivierungsdaten in einem Safe untergebracht. Aktivierungsdaten werden entweder auswendig gelernt oder in einer Weise aufgezeichnet und gespeichert, die der dem kryptografischen Modul zugeordneten Sicherheitsstufe entspricht. Sie werden nicht zusammen mit dem kryptografischen Modul gespeichert, um zu verhindern, dass nur eine Person Zugang zum privaten Schlüssel hat.

(194) Personen oder Gruppen mit Vertrauensfunktionen wird ausdrücklich die Verantwortung für die Durchführung solcher Kontrollen übertragen. Ist eine Personengruppe verantwortlich, so ist ein Protokoll zu führen, in dem die Person genannt wird, die die jeweilige Kontrolle ausführt. Ist die Einrichtung nicht ständig besetzt, zeichnet die Person, die die Einrichtung als letzte verlässt, einen Abmeldebogen ab, in dem Datum und Uhrzeit angegeben werden und bestätigt wird, dass alle erforderlichen physischen Schutzmechanismen vorhanden und aktiviert sind.

5.1.2.2. *EA/AA*

(195) Es gelten die gleichen Bestimmungen wie in Abschnitt 5.1.2.1.

5.1.3. Stromversorgung und Klimatisierung

(196) Sichere Einrichtungen für die Elemente des C-ITS Trust Models (Root-CA, CPOC, TLM, EA und AA) müssen mit einem zuverlässigen Zugang zu elektrischer Energie ausgestattet sein, damit auch bei vollständigem oder kurzzeitigem Stromausfall der Betrieb sichergestellt werden kann. Für den Fall eines Ausfalls der externen Stromversorgung und für eine reibungslose Abschaltung der Geräte des C-ITS Trust Models bei Energiemangel sind primäre Versorgungsanlagen und Backup-Installationen erforderlich. Einrichtungen des C-ITS Trust Models sind mit Heizungs-/Belüftungs-/Klimatisierungsanlagen auszustatten, mit denen die Temperatur und relative Luftfeuchtigkeit der Geräte des C-ITS Trust Models im Rahmen der Betriebsbedingungen gehalten werden können. Die Erklärung zum Zertifizierungsbetrieb (CPS) des Elements des C-ITS Trust Models enthält eine ausführliche Beschreibung des Plans und der Prozesse zur Umsetzung dieser Anforderungen.

5.1.4. Gefährdungen durch Wasser

(197) Sichere Einrichtungen für die Elemente des C-ITS Trust Models (Root-CA, CPOC, TLM, EA und AA) sollten so geschützt werden, dass die Auswirkungen durch Wassereinwirkung so gering wie möglich gehalten werden. Aus diesem Grund müssen Wasser- und Abflussleitungen vermieden werden. Die Erklärung zum Zertifizierungsbetrieb (CPS) eines Elements des C-ITS Trust Models enthält eine ausführliche Beschreibung des Plans und der Prozesse zur Umsetzung dieser Anforderungen.

5.1.5. Brandschutz

(198) Um eine schädigende Belastung durch Flammen oder Rauch zu vermeiden, werden die sicheren Einrichtungen von Elementen des C-ITS Trust Models (Root-CA, CPOC, TLM, EA und AA) entsprechend gebaut und ausgestattet und es werden Verfahren zur Bewältigung von Bedrohungen im Zusammenhang mit Feuer umgesetzt. Die Speichermedien sollten in geeigneten Behältern gegen Feuer geschützt werden.

(199) Die Elemente des C-ITS Trust Models schützen physische Medien, die Backups kritischer Systemdaten oder andere sensible Informationen enthalten, vor Umweltgefahren sowie der unbefugten Nutzung solcher Medien, dem Zugang zu ihnen oder deren Offenlegung. Die Erklärung zum Zertifizierungsbetrieb (CPS) des Elements des C-ITS Trust Models enthält eine ausführliche Beschreibung des Plans und der Prozesse zur Umsetzung dieser Anforderungen.

5.1.6. Medienmanagement

(200) Die im Rahmen des C-ITS Trust Models verwendeten Medien (Root-CA, CPOC, TLM, EA und AA) werden auf sichere Weise gehandhabt um sie vor Beschädigung, Diebstahl und unbefugtem Zugang zu schützen. Es werden Medienmanagementverfahren zum Schutz gegen Überalterung und Verschleiß von Medien während des Zeitraums, in dem Aufzeichnungen aufbewahrt werden müssen, umgesetzt.

(201) Sensible Daten werden vor dem Zugriff infolge einer Wiederverwendung von Speicherobjekten (z. B. gelöschten Dateien), durch die sensible Daten für unbefugt Nutzer zugänglich gemacht werden können, geschützt.

(202) Es wird ein Bestandsverzeichnis sämtlicher Informationsgüter geführt und es werden Anforderungen an den Schutz dieser Güter festgelegt, die im Einklang mit der Risikoanalyse stehen. Die Erklärung zum Zertifizierungsbetrieb (CPS) des Elements des C-ITS Trust Models enthält eine ausführliche Beschreibung des Plans und der Prozesse zur Umsetzung dieser Anforderungen.

5.1.7. Abfallentsorgung

(203) Die Elemente des C-ITS Trust Models (Root-CA, CPOC, TLM, EA und AA) führen Verfahren zur sicheren und irreversiblen Beseitigung von Abfällen (Papier, Medien oder andere Abfälle) durch, um die unbefugte Nutzung von Abfällen, die vertrauliche oder persönliche Informationen enthalten, sowie den unbefugten Zugang zu solchen Informationen oder deren Offenlegung zu verhindern. Alle Medien, die für die Speicherung sensibler Informationen wie Schlüsseln, Aktivierungsdaten oder Dateien verwendet werden, werden vor der Freigabe zur Entsorgung zerstört. Die Erklärung zum Zertifizierungsbetrieb (CPS) des Elements des C-ITS Trust Models enthält eine ausführliche Beschreibung des Plans und der Prozesse zur Umsetzung dieser Anforderungen.

5.1.8. Externe Sicherung

5.1.8.1. Root-CA, CPOC und TLM

(204) Nach einem Einsatz von Root-CA, CPOC und TLM sowie nach jeder Generierung neuer Schlüsselpaare werden vollständige Backups der Komponenten von Root-CA, CPOC und TLM erstellt, die für eine Wiederherstellung nach einem Systemausfall ausreichen. Es werden regelmäßig Sicherungskopien wesentlicher Unternehmensinformationen (Schlüsselpaar und CRL) sowie der Software erstellt. Es werden adäquate Backup-Einrichtungen bereitgestellt, damit eine Wiederherstellung aller wesentlichen Unternehmensinformationen und der Software nach einer Havarie oder einem Medienausfall sichergestellt ist. Back-up-Mechanismen für einzelne Systeme werden regelmäßig geprüft, um sicherzustellen, dass sie die Anforderungen des Plan zur Aufrechterhaltung des Geschäftsbetriebs erfüllen. Mindestens eine vollständige Backup-Kopie wird an einem externen Standort (Datenwiederherstellung im Falle eines Systemabsturzes, Disaster Recovery) gespeichert. Die Sicherungskopie wird an einem Ort mit physischen und verfahrenstechnischen Kontrollen gespeichert, die der des operativen PKI-Systems entsprechen.

(205) Die Backup-Daten unterliegen den gleichen Zugangsanforderungen wie die operativen Daten. Backup-Daten werden verschlüsselt und extern gespeichert. Bei einem vollständigen Datenverlust werden die Informationen, die erforderlich sind, um Root-CA, CPOC und TLM wieder in Betrieb zu setzen, vollständig aus den Backup-Daten wiederhergestellt.

(206) Privatschlüsselmaterial von Root-CA, CPOC und TLM darf nicht mit Hilfe von Standard-Backupmechanismen gesichert werden; stattdessen wird die Backup-Funktion des kryptografischen Moduls genutzt.

5.1.8.2. *EA/AA*

(207) Für diesen Abschnitt gelten die in Abschnitt 5.1.8.1 beschriebenen Prozesse.

5.2. Verfahrenskontrollen

In diesem Abschnitt werden die Aufgaben, die Pflichten und die Identifizierung des Personals beschrieben.

5.2.1. Vertrauensfunktionen

(208) Mitarbeiter, Auftragnehmer und Berater, denen eine Vertrauensfunktion zugewiesen wurde, gelten als „vertrauenswürdige Personen“. Personen, die die Anerkennung als vertrauenswürdige Personen anstreben, indem sie eine Vertrauensstellung beziehen, müssen die Screening-Anforderungen der vorliegenden Certificate Policy erfüllen.

(209) Vertrauenswürdige Personen haben Zugang zu Authentifizierungs- oder kryptografischen Operationen, die Folgendes wesentlich beeinflussen können:

- die Validierung von Informationen in Zertifikatanträgen;
- die Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatanträgen, Sperrungs- oder Erneuerungsanträgen;
- die Ausstellung oder die Sperrung von Zertifikaten unter Einschluss von Personal, das Zugang zu Beschränkungen unterliegenden Teilen der Datenablage oder zur Handhabung von Informationen über Abonnenten bzw. Anträgen hat.

(210) Zu den Vertrauensfunktionen gehören u. a.:

- der Kundenservice;
- die Systemadministration;
- ausgewiesene Technik (Designated Engineering);
- Führungskräfte, die mit der Verwaltung der Vertrauenswürdigkeit der Infrastruktur beauftragt sind.

(211) Die CA vermittelt in ihrer Erklärung zum Zertifizierungsbetrieb (CPS) klare Beschreibungen aller Vertrauensfunktionen.

5.2.2. Anzahl der pro Aufgabe erforderlichen Personen

(212) Die Elemente des C-ITS Trust Models richten zur Gewährleistung einer Aufgabentrennung auf der Grundlage von Vertrauensfunktionen strenge Kontrollverfahren ein, erhalten diese aufrecht und setzen sie durch; diese Verfahren stellen auch sicher, dass für die Durchführung sensibler Aufgaben mehrere vertrauenswürdige Personen erforderlich sind. Die Elemente des C-ITS Trust Models (TLM, CPOC, Root-CA, EA und AA) sollten [4] und die Anforderungen der folgenden Absätze einhalten.

(213) Es bestehen Richtlinien und Kontrollverfahren zur Gewährleistung einer Aufgabentrennung auf der Grundlage der beruflichen Zuständigkeiten. Für die sensibelsten Aufgaben wie dem Zugang zu und der Verwaltung von CA-Verschlüsselungshardware (HSM) und zugehörigen Schlüsselmaterials muss die Autorisierung mehrerer vertrauenswürdiger Personen vorgeschrieben sein.

(214) Diese internen Kontrollverfahren müssen so konzipiert sein, dass für den physischen oder logischen Zugang zu dem Gerät mindestens zwei vertrauenswürdige Personen erforderlich sind. Die Zugangsbeschränkungen zur CA-Verschlüsselungshardware müssen während des gesamten

Lebenszyklus, vom Empfang über die Kontrolle bis zur logischen und/oder physischen Zerstörung am Ende, von mehreren vertrauenswürdigen Personen streng durchgesetzt werden. Sobald ein Modul mit funktionsfähigen Schlüsseln aktiviert wird, werden weitere Zugangskontrollen aufgerufen, damit eine getrennte Kontrolle über den physischen und logischen Zugang zu Gerät aufrechterhalten wird.

5.2.3. Identifizierung und Authentifizierung der einzelnen Funktionen

(215) Alle Personen, denen der Beschreibung in dieser Certificate Policy (CP) entsprechend eine Funktion zugewiesen wird, werden einer Identifizierung und Authentifizierung unterzogen, damit gewährleistet ist, dass die betreffende Funktion ihnen ermöglicht, ihre PKI-Pflichten zu erfüllen.

(216) Elemente des C-ITS Trust Modells überprüfen und bestätigen die Identität und Autorisierung aller Mitarbeiter, die die Anerkennung als vertrauenswürde Person anstreben, bevor:

- ihnen ihre Zugangsgeräte ausgehändigt werden und sie Zugang zu den erforderlichen Einrichtungen erhalten;
- ihnen elektronische Berechtigungsnachweise für den Zugang zu CA-Systemen und die Durchführung spezieller Aufgaben übergeben werden.

(217) In der Erklärung zum Zertifizierungsbetrieb (CPS) werden die Mechanismen beschrieben, die für die Identifizierung und Authentifizierung natürlicher Personen eingesetzt werden.

5.2.4. Funktionen, die eine Aufgabentrennung erfordern

(218) Zu den Aufgaben, für die eine Aufgabentrennung erforderlich ist, gehören unter anderem:

- die Annahme, Ablehnung und Sperrung von Anträgen sowie die anderweitige Bearbeitung von CA-Zertifikatanträgen;
- die Generierung, Ausstellung und Vernichtung eines CA-Zertifikats.

(219) Die Aufgabentrennung kann mit Hilfe von PKI-Geräten, Verfahren oder beidem durchgesetzt werden. Keiner Person darf mehr als eine Identität zugewiesen werden, sofern dies nicht von der Root-CA genehmigt wurde.

(220) Der Teil der Root-CA und CA, der mit der Verwaltung der Generierung und Sperrung von Zertifikaten befasst ist, muss hinsichtlich seiner Entscheidungen in Bezug auf die Einrichtung, Bereitstellung, Aufrechterhaltung und Suspendierung von Dienstleistungen gemäß geltenden Certificate Policies von anderen Organisationen unabhängig sein. Insbesondere stehen die Geschäftsleitung, das leitende Personal und das Personal mit Vertrauensfunktionen unter keinerlei geschäftlichem, finanziellem oder sonstigem Druck, der das Vertrauen in die von ihm erbrachten Dienstleistungen nachteilig beeinflussen könnten.

(221) Die EA und AA, die mobile C-ITS-Stationen betreuen, müssen getrennte operative Einheiten mit getrennten IT-Infrastrukturen und IT-Managementteams sein. Der Datenschutz-Grundverordnung entsprechend tauschen EA und AA nur für die Genehmigung von AT-Anträgen (Berechtigungstickets) personenbezogene Daten aus. Daten bezüglich der Genehmigung von AT-Anträgen übertragen sie nur über eine speziell dafür

vorgesehene, sichere Schnittstelle mittels des in [1] genannten Protokolls zur Berechtigungsvalidierung. Andere Protokolle können unter der Voraussetzung verwendet werden, dass [1] umgesetzt worden ist.

(222) Die von der EA und AA gespeicherten Logdateien dürfen ausschließlich zum Zweck der Sperrung von Fehlverhalten aufweisenden EC auf der Grundlage von abgefangenen bösartigen CAM/DENM-Benachrichtigungen genutzt werden. Nachdem eine CAM/DENM-Benachrichtigung als „bösartig" eingestuft wurde, wird die AA den Verifizierungsschlüssel des Berechtigungstickets (AT) in ihren Ausstellungsprotokollen aufsuchen und bei der EA einen Sperrungsantrag mit der verschlüsselten Signatur unter dem privaten EC-Schlüssel, der bei der Ausstellung des AT verwendet wurde, einreichen. Alle Logdateien müssen angemessen gegen den Zugang unbefugter Parteien geschützt sein und dürfen nicht an andere Stellen oder Behörden weitergegeben werden.

Anmerkung: Zum Zeitpunkt der Erstellung der vorliegenden Fassung der Certificate Policy war die Ausgestaltung der Fehlverhalten aufweisenden Funktion noch nicht definiert. Es ist geplant, die Fehlverhalten aufweisende Funktion bei künftigen Überarbeitungen der Certificate Policy in ihrer Ausgestaltung darzustellen.

5.3. Personalkontrollen

5.3.1. Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

(223) Die Elemente des C-ITS Trust Models beschäftigen in ausreichender Zahl Personal mit dem Fachwissen, den Erfahrungen und den Qualifikationen, die für die Aufgaben am Arbeitsplatz und die angebotenen Dienste erforderlich sind. Das PKI-Personal erfüllt diese Anforderungen durch eine formelle Ausbildung und entsprechende Zeugnisse, praktische Erfahrung oder eine Kombination aus beidem. Vertrauensfunktionen und Verantwortlichkeiten gemäß Spezifikation in der Erklärung zum Zertifizierungsbetrieb (CPS) werden in den Stellenbeschreibungen dokumentiert und eindeutig benannt. Für das PKI-Personal von Subunternehmern werden Stellenbeschreibungen festgelegt, die eine Trennung der Pflichten und Rechte sicherstellen; zudem wird auf der Grundlage von Pflichten und Zugangsebenen, Sicherheitsüberprüfungen und der Schulung und Sensibilisierung der Mitarbeiter die Sensibilität der jeweiligen Stelle bestimmt.

5.3.2. Verfahren zur Zuverlässigkeitsüberprüfung

(224) Die Elemente des C-ITS Trust Models führen für Personal, das eine Anerkennung als vertrauenswürde Peron anstrebt, Zuverlässigkeitsüberprüfungen durch. Die Zuverlässigkeitsüberprüfungen sind bei Personal, das Vertrauensstellungen innehat, mindestens alle fünf Jahre zu wiederholen.

(225) Die bei einer Zuverlässigkeitsüberprüfung ermittelten Faktoren, die als Gründe für die Ablehnung von Bewerbern für Vertrauensstellungen oder für Maßnahmen gegen eine bestehende vertrauenswürdige Person betrachtet werden können, umfassen unter anderem Folgendes:

- Falschdarstellungen durch den Bewerber oder die vertrauenswürdige Person;

- sehr ungünstige oder unzuverlässige berufliche Zeugnisse;
- bestimmte strafrechtliche Verurteilungen;
- Hinweise auf einen Mangel an finanziellem Verantwortungsbewusstsein.

(226) Berichte, die derartige Informationen enthalten, werden vom Personal der HR-Abteilung bewertet, das in Anbetracht der Art, der Größenordnung und der Häufigkeit des durch die Zuverlässigkeitsüberprüfung aufgedeckten Verhaltens angemessene Maßnahmen zu treffen hat. Die kann Maßnahmen bis einschließlich Aufhebungsangeboten an Bewerber für Vertrauensstellungen oder die Kündigung bestehender vertrauenswürdiger Personen umfassen. Die Verwendung von Informationen, die bei einer Zuverlässigkeitsüberprüfung als Grundlage für eine solche Maßnahme ermittelt wurden, unterliegt geltendem Recht.

(227) Hintergrundüberprüfungen von Personen, die die Anerkennung als vertrauenswürdige Person anstreben, umfassen unter anderem Folgendes:

- Bestätigung der früheren Beschäftigung;
- eine Überprüfung der beruflichen Zeugnisse, die ihre Beschäftigung über einen Zeitraum von mindestens fünf Jahren abdecken;
- Bestätigung des höchsten oder relevantesten Bildungsabschlusses;
- Abfrage der Strafregister.

5.3.3. Schulungsanforderungen

(228) Die Elemente des C-ITS Trust Models stellen ihren Mitarbeitern die erforderliche Schulung zur Verfügung, damit sie ihre Aufgaben im Zusammenhang mit den CA-Operationen sachkundig und zufriedenstellend erfüllen können.

(229) Die Ausbildungsprogramme werden regelmäßig überprüft; in der Ausbildung der Mitarbeiter werden Fragen behandelt, die für die von ihnen wahrgenommenen Funktionen relevant sind.

(230) Die Ausbildungsprogramme betreffen Angelegenheiten, die für das besondere Umfeld der Ausbildungsteilnehmer relevant sind, unter anderem:

- Sicherheitsgrundsätze und -mechanismen der Elemente des C-ITS Trust Models;
- die verwendeten Hard- und Softwareversionen;
- alle Pflichten, deren Erfüllung von der betreffenden Person erwartet wird, sowie interne und externe Berichtsverfahren und Sequenzen;
- PKI-Geschäftsprozesse und Arbeitsabläufe;
- Meldung und Handhabung von Zwischenfällen und Kompromittierungen;
- Verfahren zur Datenwiederherstellung im Falle eines Systemabsturzes und zur Aufrechterhaltung des Geschäftsbetriebs;
- ausreichende IT-Kenntnisse.

5.3.4. Nachschulungsintervalle und -anforderungen

(231) Die Personen, denen Vertrauensfunktionen zugewiesen wurden, müssen ihre während der Ausbildung erworbenen Kenntnisse fortlaufend unter Nutzung eines Schulungsumfelds auffrischen. Die Schulung ist immer dann zu wiederholen, wenn dies für erforderlich gehalten wird, mindestens jedoch alle zwei Jahre.

(232) Elemente des C-ITS Trust Models bieten ihrem Personal in dem Umfang und mit der Häufigkeit Auffrischungsschulungen und Aktualisierungen an, die zur Aufrechterhaltung des Kenntnisstandes erforderlich ist, den sie für die kompetente, zufriedenstellende Erfüllung der Verantwortlichkeiten an ihrem Arbeitsplatz benötigen.

(233) Personen mit Vertrauensfunktionen müssen eventuelle Änderungen im PKI-Betrieb kennen. Wesentliche Änderungen im Betrieb werden von einem Schulungs- bzw. Sensibilisierungsplan begleitet und die Durchführung des Plans wird dokumentiert.

5.3.5. Häufigkeit und Abfolge der Arbeitsplatzrotation

(234) Keine Vorgabe, solange die technischen Fähigkeiten, Erfahrungen und Zugangsrechte gewährleistet sind. Die Administratoren der Elemente des C-ITS Trust Models stellen sicher, dass personelle Veränderungen die Sicherheit des Systems nicht beeinträchtigen.

5.3.6. Sanktionen bei unbefugten Handlungen

(235) Jedes Element des C-ITS Trust Models muss ein förmliches Disziplinarverfahren entwickeln, damit die angemessene Sanktionierung unbefugter Handlungen gewährleistet ist. In schweren Fällen müssen Funktionszuweisungen und die entsprechenden Rechte entzogen werden.

5.3.7. Anforderungen an unabhängige Auftragnehmer

(236) Die Elemente des C-ITS Trust Models können selbständigen Unternehmern oder Beratern nur in dem Umfang den Erwerb der Anerkennung als vertrauenswürdige Personen gestatten, der mit klar umrissenen Beziehungen im Rahmen einer Auslagerung von Aufgabenbereichen in Einklang zu bringen ist; ferner gilt die Voraussetzung, dass die betreffende Stelle den Auftragnehmern oder Beratern im gleichen Maße vertraut wie Mitarbeitern und dass die Auftragnehmer und Berater die für Beschäftigte geltenden Anforderungen erfüllen.

(237) Ist dies nicht der Fall, erhalten selbständige Unternehmer und Berater nur Zugang zu PKI-sicheren C-ITS-Einrichtungen, wenn sie von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.3.8. Dem Personal bereitgestellte Dokumentation

(238) Elemente des C-ITS Trust Models bieten ihrem Personal die erforderliche Schulung und den Zugang zu den Unterlagen, die sie benötigen, um ihre Aufgaben kompetent und zufriedenstellend zu erfüllen.

5.4. Verfahren für die Protokollierung von Audits

(239) In diesem Abschnitt werden die Anforderungen hinsichtlich der Arten von aufzuzeichnenden Ereignissen und das Management von Auditprotokollen festgelegt.

5.4.1. Von jeder CA aufzuzeichnende und zu meldende Ereignisarten

(240) Ein Vertreter der Wurzelzertifizierungsstelle (CA) überprüft die Protokolle, Ereignisse und Verfahren der CA regelmäßig.

(241) Elemente des C-ITS Trust Models zeichnen folgende Arten von Auditereignissen auf (falls zutreffend):

- physischer Zugang zu Einrichtungen – der Zugang natürlicher Personen zu den Einrichtungen wird mittels Speicherung der Zugangsanfragen durch Smartcards aufgezeichnet. Jedes Mal, wenn ein Datensatz angelegt wird, wird ein Ereignis angelegt;
- Verwaltung der Vertrauensfunktionen – jede Änderung der Definition und der Zugangsebene der verschiedenen Funktionen wird einschließlich der Änderungen an Attributen der Funktionen aufgezeichnet. Jedes Mal, wenn ein Datensatz angelegt wird, wird ein Ereignis angelegt;
- logischer Zugang – es wird ein Ereignis angelegt, wenn ein Teilnehmer (z. B. ein Programm) Zugang zu sensiblen Bereichen (d. h. Netzen und Servern) hat;
- Backup-Management – jedes Mal, wenn ein Backup erfolgreich oder erfolglos abgeschlossen wird, wird ein Ereignis angelegt;
- Protokollmanagement – Protokolle werden gespeichert. Wenn die Größe des Protokolls eine bestimmte Größe überschreitet, wird ein Ereignis angelegt;
- Daten aus dem Authentisierungsprozess für Abonnenten und Elemente des C-ITS Trust Models – für jede Authentifizierungsanfrage durch Abonnenten und Elemente des C-ITS Trust Models wird ein Ereignis generiert;
- Annahme und Ablehnung von Zertifikatanträgen, einschließlich der Ausstellung und Erneuerung von Zertifikaten – es wird regelmäßig ein Ereignis mit einer Liste der in den vorangegangenen sieben Tagen angenommenen und abgelehnten Zertifikatanträgen generiert;
- Herstellerregistrierung – wenn ein Hersteller registriert wird, wird ein Ereignis angelegt;
- Registrierung der C-ITS-Station – ein Ereignis wird angelegt, wenn eine C-ITS-Station registriert wird;
- HSM-Management – ein Ereignis wird angelegt, wenn eine HSM-Sicherheitsverletzung aufgezeichnet wird;
- IT und Netzmanagement, soweit sie die PKI-Systeme betreffen – ein Ereignis wird angelegt, wenn ein PKI-Server abgeschaltet oder neu gestartet wird;

- Sicherheitsmanagement (erfolgreiche und erfolglose Zugangsversuche zum PKI-System, durchgeführte Aktionen an und durch PKI- und sonstige(n) sicherheitsrelevante(n) Systeme(n), Änderungen am Sicherheitsprofil, Systemabstürze, Hardware-Ausfälle und andere Anomalien, Firewall- und Router-Aktivitäten; sowie Zutritt zu und Verlassen von Einrichtungen des PKI-Systems);
- ereignisbezogene Daten werden mindestens fünf Jahre lang gespeichert, sofern keine zusätzlichen nationalen Vorschriften gelten.

(242) Im Einklang mit der Datenschutz-Grundverordnung (DSGVO) erlauben die Audit-Protokolle in Bezug auf Privatfahrzeuge an C-ITS-Stationen keinen Zugriff auf Daten, die die Privatsphäre betreffen.

(243) Die Protokolle von Sicherheitsaudits werden nach Möglichkeit automatisch erfasst. Ist dies nicht möglich, so ist ein Logbuch, ein Papierformular oder ein sonstiger physischer Mechanismus zu verwenden. Alle elektronischen und nicht elektronischen Protokolle von Sicherheitsaudits müssen aufbewahrt und bei Konformitätsprüfungen zur Verfügung gestellt werden.

(244) Jedes mit dem Lebenszyklus eines Zertifikats zusammenhängende Ereignis wird so in einem Protokoll erfasst, dass es der durchführenden Person zugeordnet werden kann. Alle Daten im Zusammenhang mit einer persönlichen Identität werden verschlüsselt und gegen unbefugten Zugriff geschützt.

(245) Audit-Protokolle umfassen mindestens folgende (automatisch oder manuell für jedes prüfbare Ereignis aufgezeichnete) Angaben:

- Art des Ereignisses (aus der vorstehenden Aufzählung);
- vertrauenswürdiges Datum und vertrauenswürdige Uhrzeit des Eintritts des Ereignisses;
- Ergebnis des Ereignisses – Erfolg oder Misserfolg, sofern angemessen;
- gegebenenfalls die Identität der Stelle und/oder des Betreibers, die bzw. der das Ereignis ausgelöst hat;
- Identität der Stelle, an die sich das Ereignis richtet.

5.4.2. Häufigkeit der Bearbeitung von Protokollen

(246) Die Überprüfung von Audit-Protokollen wird durch Alarmmeldungen auf der Grundlage von Unregelmäßigkeiten und Vorfällen innerhalb der CA-Systeme ausgelöst und darüber hinaus in regelmäßigen jährlichen Abständen durchgeführt.

(247) Die Bearbeitung von Audit-Protokollen besteht in einer Überprüfung der Audit-Protokolle und der Dokumentierung der Gründe für alle bedeutenden Ereignisse in einer Zusammenfassung der Audit-Protokolle. Im Rahmen der Überprüfungen von Audit-Protokollen wird verifiziert, dass das Protokoll nicht manipuliert wurde; ferner werden alle Protokolleinträge kontrolliert und Alarmmeldungen oder Unregelmäßigkeiten in den Protokollen werden untersucht. Auf der Grundlage von Überprüfungen der Audit-Protokolle getroffene Maßnahmen werden dokumentiert.

(248) Das Audit-Protokoll wird mindestens einmal wöchentlich archiviert. Administratoren archivieren das Protokoll manuell, wenn der freie

Speicherplatz für das Audit-Protokoll kleiner ist als die Menge an Audit-Protokolldaten, die für die betreffende Woche erwartet werden.

5.4.3. Aufbewahrungszeitraum für Audit-Protokolle

(249) Protokoll-Datensätze, die sich auf die Lebenszyklen von Zertifikaten beziehen, werden mindestens fünf Jahre nach dem Ablauf des entsprechenden Zertifikats aufbewahrt.

5.4.4. Schutz der Audit-Protokolle

(250) Die Integrität und Vertraulichkeit des Audit-Protokolls wird durch einen auf Funktionen basierenden Zugriffskontrollmechanismus gewährleistet. Die internen Audit-Protokolle sind nur für Administratoren zugänglich; Audit-Protokolle im Zusammenhang mit dem Lebenszyklus von Zertifikaten sind über einer Webseite mit Nutzer-Login auch Nutzern mit entsprechender Autorisierung zugänglich. Der Zugang ist mit einer Authentifizierung mit mehreren Nutzern (mindestens zwei Nutzern) auf mindestens zwei Ebenen zu gewähren. Es muss technisch gewährleistet sein, dass die Nutzer nicht auf ihre eigenen Logdateien zugreifen können.

(251) Alle Protokolleinträge müssen unter Verwendung von Schlüsselmaterial der Verschlüsselungshardware HSM signiert werden.

(252) Ereignisprotokolle, die zur persönlichen Identifizierung führen können, beispielsweise über ein privates Fahrzeug, werden so verschlüsselt, dass nur befugte Personen sie lesen können.

(253) Ereignisse werden in einer Weise protokolliert, dass sie innerhalb der Frist, in der die Protokolle beibehalten werden müssen nicht ohne Weiteres gelöscht oder zerstört werden können (außer bei Übertragungen auf Langzeitmedien).

(254) Die Ereignisprotokolle sind so geschützt, dass sie für die Dauer ihrer Speicherfrist lesbar bleiben.

5.4.5. Sicherungsverfahren für Audit-Protokolle

(255) Audit-Protokolle und Audit-Zusammenfassungen werden mittels unternehmensinterner Sicherungsmechanismus unter Aufsicht von Inhabern autorisierter Vertrauensfunktionen getrennt von der Quellkomponente für ihre Erzeugung gesichert (Backup). Backups von Audit-Protokollen werden mit dem gleichen Vertrauensniveau geschützt, das auch für die ursprünglichen Protokolle gilt.

5.4.6. Audit-Erfassungssystem (intern oder extern)

(256) Die Geräte der Elemente des C-ITS Trust Models aktivieren die Auditprozesse beim Einschalten des Systems und deaktivieren sie erst beim Abschalten des Systems. Stehen keine Auditprozesse zur Verfügung, stellt das Element des C-ITS Trust Models seinen Betrieb vorübergehend ein.

(257) Am Ende eines jeden Betriebszeitraums sowie bei der Schlüsselerneuerung für Zertifikate ist dem Betriebsleiter und dem Leitungsorgan des Betriebs des jeweiligen PKI-Elements der kollektive Gerätestatus zu melden.

5.4.7. Benachrichtigung des ereignisauslösenden Subjekts

(258) Protokolliert das Audit-Erfassungssystem ein Ereignis, gewährleistet es die Verknüpfung des Ereignisses mit einer Vertrauensfunktion.

5.4.8. Schwachstellenbewertung

(259) Der für die Durchführung von Audits zuständige Aufgabenbereich und die für die Realisierung des Betriebs des PKI-Systems in den Elementen des C-ITS Trust Models zuständigen Aufgabenbereiche erläutern alle bedeutenden Ereignis in einer Audit-Protokollzusammenfassung. Im Rahmen solcher Überprüfungen wird verifiziert, dass die Protokolle nicht manipuliert wurden und dass bei den Auditdaten keine Unterbrechungen oder sonstige Verluste vorliegen; anschließend werden sämtliche Protokolleinträge kurz kontrolliert, wobei Alarmmeldungen oder Unregelmäßigkeiten in den Protokollen einer gründlicheren Untersuchung unterzogen werden. Die infolge dieser Überprüfungen getroffenen Maßnahmen werden dokumentiert.

(260) Die Elemente des C-ITS Trust Models

- führen unter der Leitung der Elemente des C-ITS Trust Modells organisatorische und/oder technische Aufdeckungs- und Präventionskontrollen durch, um PKI-Systeme vor Viren und Schadsoftware zu schützen;
- dokumentieren und befolgen einen Prozess zur Beseitigung von Schwachstellen, der sich mit der Ermittlung, Prüfung, Beantwortung und Behebung von Schwachstellen befasst;
- durchlaufen eine Schwachstellenüberprüfung (Vulnerability Scan) oder führen diese wie folgt durch:
    - nach Wechseln von Systemen oder Netzen, die von den Elementen des C-ITS Trust Models als bedeutend für PKI-Komponenten eingestuft werden und
    - mindestens einmal im Monat auf öffentlichen und privaten IP-Adressen, die von der CA und der CPOC als zum PKI-System gehörend gekennzeichnet wurden,
- durchlaufen mindestens auf jährlicher Basis und nach Aktualisierungen oder Änderungen von Infrastrukturen oder Anwendungen, die von den Elementen des C-ITS Trust Models als für die PKI-Komponente einer Wurzelzertifizierungsstelle (CA) bedeutend gekennzeichnet wurden, einen Penetrationstest;
- bei Online-Systemen werden Nachweise erfasst, dass jede(r) einzelne Schwachstellenüberprüfung und Penetrationstest von einer Person oder Stelle (bzw. kollektiven Gruppe aus beiden) durchgeführt wurde, die über die Kompetenzen, Instrumente und Kenntnisse sowie den Ethikkodex und die Unabhängigkeit verfügt, die zur Erbringung eines verlässlichen Schwachstellen- oder Penetrationstests erforderlich sind;
- verfolgen und beheben Schwachstellen im Einklang mit den Strategien für die Cybersicherheit von Unternehmen und der Methode zur Risikominderung.

5.5. Archivierung von Aufzeichnungen

5.5.1. Art der archivierten Aufzeichnungen

(261) Die Elemente des C-ITS Trust Models archivieren Aufzeichnungen hinreichend detailliert, damit die Gültigkeit einer Signatur und der ordnungsgemäße Betrieb der PKI festgestellt werden können. Es werden mindestens folgende Aufzeichnungen mit PKI-Ereignisses archiviert (falls zutreffend):

- Protokoll über den physischen Zugang zu Einrichtungen von Elementen des C-ITS Trust Models (mindestens ein Jahr);
- Managementprotokoll der Vertrauensfunktion für Elemente des C-ITS Trust Models (mindestens 10 Jahre);
- Protokoll über den IT-Zugang für Elemente des C-ITS Trust Models (mindestens fünf Jahre);
- Protokoll über die Generierung, Nutzung und Vernichtung von CA-Schlüsseln (mindestens fünf Jahre) (nicht für TLM und CPOC);
- Protokoll über die Generierung, Nutzung und Vernichtung von Zertifikaten (mindestens zwei Jahre);
- Protokoll über CPA-Anträge (mindestens zwei Jahre);
- Protokoll über das Aktivierungsdatenmanagement für Elemente des C-ITS Trust Models (mindestens fünf Jahre);
- IT- und Netzprotokoll für Elemente des C-ITS Trust Models (mindestens fünf Jahre);
- PKI-Unterlagen für Elemente des C-ITS Trust Models (mindestens fünf Jahre);
- Bericht über Sicherheitsvorfälle und Audits für Elemente des C-ITS Trust Models (mindestens zehn Jahre);
- Geräte, Software und Konfiguration des Systems (mindestens fünf Jahre).

(262) Die Elemente des C-ITS Trust Models müssen folgende Unterlagen, die sich auf Zertifikatanträge und deren Verifizierung beziehen, sowie alle Zertifikate von TLM, Root-CA und CA und deren CRL mindestens sieben Jahre, nachdem ein Zertifikat auf der Grundlage dieser Unterlagen ungültig wird, aufbewahren:

- von Elementen des C-ITS Trust Models aufbewahrte PKI-Auditunterlagen;
- von Elementen des C-ITS Trust Models aufbewahrte CPS-Unterlagen;
- von Elementen des C-ITS Trust Models aufbewahrte Verträge zwischen der CPA und anderen Stellen;
- von CA und TLM aufbewahrte Zertifikate (oder andere Informationen über Sperrungen);
- Aufzeichnungen über Zertifikatanträge im System der Root-CA (gilt nicht für den TLM);

- sonstige Daten oder Anwendungen, die ausreichen, um den Inhalt des Archivs zu verifizieren;
- alle Arbeiten im Zusammenhang mit oder von Elementen des C-ITS Trust Models und Konformitätsprüfern.

(263) Die CA-Stelle bewahrt sämtliche Unterlagen, die sich auf Zertifikatanträge und deren Verifizierung beziehen, sowie sämtliche Zertifikate und Unterlagen über deren Sperrung mindestens sieben Jahre, nachdem auf diesen Unterlagen basierende Zertifikate ungültig werden, auf.

5.5.2. Aufbewahrungszeitraum für Archive

(264) Elemente des C-ITS Trust Models bewahren sämtliche Aufzeichnungen mindestens fünf Jahre, nachdem das entsprechende Zertifikat abgelaufen ist, auf; Verordnungen, die eine längere Archivierungszeit vorschreiben, bleiben hiervon unberührt.

5.5.3. Schutz von Archiven

(265) Elemente des C-ITS Trust Models speichern das Aufzeichnungsarchiv in einer sicheren, geschützten Speichereinrichtung getrennt von Geräten der CA und mit physischen und verfahrenstechnischen Sicherheitskontrollen, die denen der PKI gleichwertig oder besser als diese sind.

(266) Das Archiv ist mittels Speicherung in einem vertrauenswürdigen System vor unbefugter Einsichtnahme, Änderung, Löschung oder sonstiger Manipulation zu schützen.

(267) Die Medien, in denen die Archivdaten aufbewahrt werden, und die für deren Verarbeitung erforderlichen Anwendungen werden in einer Weise gepflegt, die sicherstellt, dass während des in der vorliegenden Certificate Policy festgelegten Zeitraums auf sie zugegriffen werden kann.

5.5.4. Systemarchiv und Speicherung

(268) Die Elemente des C-ITS Trust Models führen schrittweise Sicherungen der Systemarchive für Informationen dieser Art täglich und vollständige Sicherungen (Backups) wöchentlich durch. Kopien von Aufzeichnungen in Papierform werden in einer gesicherten Einrichtung außerhalb des Standorts aufbewahrt.

5.5.5. Anforderungen an Zeitstempel von Aufzeichnungen

(269) Die Elemente des C-ITS Trust Models, die eine Datenbank für Sperrungen verwalten, stellen sicher, dass die Aufzeichnungen Angaben zur Uhrzeit und zum Datum der Erstellung von Sperraufzeichnungen enthalten. Die Integrität dieser Informationen wird mithilfe kryptografischer Lösungen gesichert.

5.5.6. Archiverfassungssystem (intern oder extern)

(270) Das Archiverfassungssystem ist intern.

5.5.7. Verfahren zur Beschaffung und Verifizierung von Archivinformationen

(271) Sämtliche Elemente des C-ITS Trust Models erlauben ausschließlich bevollmächtigten, vertrauenswürdigen Personen den Zugang zum Archiv. Root-CA und CA beschreiben in ihrer Erklärung zum Zertifizierungsbetrieb

(CPS) die Verfahren für die Erstellung, Verifizierung, Packung, Übertragung und Speicherung von Archivinformationen.

(272) Die Geräte von Root-CA und CA überprüfen vor der erneuten Speicherung die Integrität der Informationen.

5.6. Schlüsselwechsel für Elemente des C-ITS Trust Models

(273) Bei folgenden Elementen des C-ITS Trust Models bestehen besondere Anforderungen an Schlüsselwechsel: TLM-, Root-CA- und EA/A-/AA-Zertifikate.

*5.6.1. **TLM***

(274) Der TLM löscht seinen privaten Schlüssel, wenn das entsprechende Zertifikat abläuft. Vor der Deaktivierung des derzeit gültigen privaten Schlüssels generiert er ein neues Schlüsselpaar und das entsprechende TLM-Zertifikat. Dabei sorgt er dafür. dass das neue (Link-)Zertifikat so rechtzeitig in die ECTL aufgenommen wird, dass es vor seinem Gültigwerden an alle C-ITS-Stationen verteilt werden kann. Das Link-Zertifikat und das neue selbstsignierte Zertifikat werden an die zentrale Kontaktstelle (CPOC) übertragen.

5.6.2. Root-CA

(275) Die Root-CA deaktiviert und löscht den derzeitigen privaten Schlüssel (einschließlich der Backup-Schlüssel), so dass sie keine EA/AA Zertifikate mit einer über die Gültigkeit des Root-CA-Zertifikats hinausgehenden Gültigkeit ausstellen kann.

(276) Die Root-CA generiert vor der Deaktivierung des derzeitigen privaten Schlüssels (einschließlich der Backup-Schlüssel) ein neues Schlüsselpaar und ein entsprechendes Root-CA- und Link-Zertifikat und übermittelt es an den TLM zur Aufnahme in die ECTL (Liste vertrauenswürdiger europäischer Zertifikate). Die Gültigkeitsdauer des neuen Root-CA-Zertifikats beginnt mit der geplanten Deaktivierung des derzeitigen privaten Schlüssels. Die Root-CA sorgt dafür, dass das neue Zertifikat so rechtzeitig in die ECTL aufgenommen wird, dass es vor seinem Gültigwerden an alle C-ITS-Stationen verteilt werden kann.

(277) Die Root-CA aktiviert den neuen privaten Schlüssel, sobald das entsprechende Zertifikat der Root-CA gültig wird.

5.6.3. EA/AA-Zertifikat

(278) Die EA/AA deaktiviert den derzeitigen privaten Schlüssel, so dass sie keine EC/AT mit einer über die Gültigkeit des EA/AA-Zertifikats hinausgehenden Gültigkeit ausstellen kann.

(279) Die EA/AA generiert vor der Deaktivierung des derzeitigen privaten Schlüssels ein neues Schlüsselpaar und fordert das entsprechende EA/AA-Zertifikat an. Die Gültigkeitsdauer des neuen EA/AA-Zertifikats für die beginnt mit der geplanten Deaktivierung des derzeitigen privaten Schlüssels. Die EA/AA sorgt dafür, dass das neue Zertifikat so rechtzeitig veröffentlicht werden kann, dass es vor seinem Gültigwerden an alle C-ITS-Stationen verteilt werden kann.

(280) Die EA/AA aktiviert den neuen privaten Schlüssel, sobald das entsprechende EA/AA-Zertifikat gültig wird.

5.6.4. Prüfer

Keine Regelung.

5.7. Kompromittierung und Datenwiederherstellung im Falle eines Systemabsturzes (Disaster Recovery)

5.7.1. Umgang mit Störungen und Kompromittierungen

(281) Die Elemente des C-ITS Trust Models überwachen ihre Geräte fortlaufend, so dass potenzielle Hackerversuche oder andere Formen von Kompromittierungen aufgedeckt werden. In einem solchen Fall führen sie Untersuchungen zur Ermittlung der Art und des Umfangs der Schäden durch.

(282) Entdeckt das für das Management der Root-CA oder des TLM zuständige Personal einen potenziellen Hackerversuch oder eine andere Form der Kompromittierung, führt es Untersuchungen zur Ermittlung der Art und des Umfangs der Schäden durch. Bei einer Kompromittierung des private Schlüssels wird das Root-CA-Zertifikat gesperrt. Die IT-Sicherheitsexperten der CPA bewerten den Umfang des potenziellen Schadens, um festzustellen, ob die PKI neu aufgebaut werden muss, ob nur einige Zertifikate gesperrt werden müssen und/oder ob die PKI kompromittiert wurde. Darüber hinaus bestimmt die CPA im Einklang mit ihrem Plan zur Aufrechterhaltung des Geschäftsbetriebs, welche Dienste beizubehalten sind (Sperrung und Information über den Zertifikatsstatus) und wie dies erfolgen soll.

(283) In der Erklärung zum Zertifizierungsbetrieb (CPS) werden Zwischenfälle, Kompromittierungen und die Aufrechterhaltung des Geschäftsbetriebs behandelt, wobei sie sich zu ihrer Umsetzung auch auf andere Ressourcen und Pläne des Unternehmens stützen kann.

(284) Entdeckt das für das Management der EA/AA/CPOC zuständige Personal einen potenziellen Hackerversuch oder eine andere Form der Kompromittierung, führt es Untersuchungen zur Ermittlung der Art und des Umfangs der Schäden durch. Das für das Management der CA- oder der CPOC-Stelle verantwortliche Personal bewertet den Umfang des potenziellen Schadens, um festzustellen, ob die PKI-Komponenten neu aufgebaut werden müssen, ob nur einige Zertifikate gesperrt werden müssen und/oder ob die PKI-Komponente kompromittiert wurde. Darüber hinaus bestimmt die Sub-CA-Stelle im Einklang mit ihrem Plan zur Aufrechterhaltung des Geschäftsbetriebs, welche Dienste beizubehalten sind und wie dies erfolgen soll. Wird eine PKI-Komponente kompromittiert, warnt die CA-Stelle ihre eigene Root-CA und den TLM über die CPOC.

(285) Zwischenfälle, Kompromittierungen und die Aufrechterhaltung des Geschäftsbetriebs werden in der Erklärung zum Zertifizierungsbetrieb (CPS) der Root-CA oder des TLM behandelt (bzw. anderen relevanten Unterlagen, wenn es sich um die CPOC handelt), wobei sich die CPOC zu deren Umsetzung auch auf andere Ressourcen und Pläne des Unternehmens stützen kann.

(286) Die Root-CA und die CA alarmieren alle Vertreter von Mitgliedstaaten und Root-CA, mit denen sie eine Vereinbarung im Zusammenhang mit kooperativen intelligenten Verkehrssystemen (C-ITS) geschlossen haben, und übermitteln ihnen genaue Informationen über die Folgen des Zwischenfalls, damit diese ihre eigenen Störungsmanagementpläne aktivieren können.

5.7.2. Beschädigung von Rechnerressourcen, Software und/oder Daten

(287) Wird eine Havarie festgestellt, die den ordnungsgemäßen Betrieb eines Elements des C-ITS Trust Models verhindert, so setzt dieses Element seinen Betrieb aus und prüft, ob der private Schlüssel kompromittiert wurde (mit Ausnahme der CPOC). Defekte Hardware wird so schnell wie möglich ersetzt und es gelten die in den Abschnitten 5.7.3 und 5.7.4 beschriebenen Verfahren.

(288) Die Beschädigung von Rechnerressourcen, Software und/oder Daten wird der Root-CA bei den höchsten Risikostufen innerhalb von 24 Stunden gemeldet. Alle anderen Ereignisse müssen in den regelmäßigen Bericht der Root-CA, EA und AA aufgenommen werden.

5.7.3. Verfahren bei der Kompromittierung von privaten Schlüsseln

(289) Wenn der private Schlüssel einer Root-CA kompromittiert ist, verloren geht oder zerstört wird oder der Verdacht seiner Kompromittierung besteht, muss die Root-CA:

- ihren Betrieb aussetzen;
- den Plan zur Datenwiederherstellung im Falle eines Systemabsturzes und den Migrationsplan in Gang setzen;
- ihr Root-CA-Zertifikat sperren;
- das „Schlüsselproblem“ ermitteln, das die Kompromittierung hervorrief, und die CPA benachrichtigen, die über den TLM das Root-CA-Zertifikat sperrt (siehe Abschnitt 7);
- alle Abonnenten, mit denen sie eine Vereinbarung geschlossen hat, warnen.

(290) Wenn der private Schlüssel einer EA/AA kompromittiert ist, verloren geht oder zerstört wird oder der Verdacht seiner Kompromittierung besteht, muss die EA/AA:

- ihren Betrieb aussetzen;
- ihr eigenes Zertifikat sperren;
- das „Schlüsselproblem“ ermitteln und die Root-CA benachrichtigen;
- Abonnenten, mit denen eine Vereinbarung besteht, warnen.

(291) Wenn der EC- oder AT-Schlüssel einer C-ITS-Station kompromittiert ist, verloren geht oder zerstört wird oder der Verdacht seiner Kompromittierung besteht, muss die EA/AA, bei der die C-ITS-Station ein Abonnement hat, Folgendes veranlassen:

- Sperrung des Enrollment-Berechtigungsnachweises (EC) des betroffenen ITS;
- Ermittlung des „Schlüsselproblems“ und Benachrichtigung der Root-CA;
- Warnung der Abonnenten, mit denen sie eine Vereinbarung geschlossen hat.

(292) Reichen von der Root-CA und/oder CA oder C-ITS-Stationen verwendete Algorithmen oder zugehörige Parameter für ihren verbleibenden Verwendungszweck nicht mehr aus, informiert die CPA (mit entsprechender

Empfehlung kryptografischer Experten) die Root-CA-Stelle, mit der sie eine Vereinbarung geschlossen hat, und ändert die verwendeten Algorithmen. (Einzelheiten sind Abschnitt 6 und den CPS der Root-CA und Sub-CA zu entnehmen.)

5.7.4. Fähigkeiten zur Aufrechterhaltung des Geschäftsbetriebs nach einem Systemabsturz

(293) Die sichere Einrichtungen für CA-Operationen betreibenden Elemente des C-ITS Trust Models entwickeln, testen, pflegen und implementieren einen Plan zur Datenwiederherstellung im Falle eines Systemabsturzes, der darauf ausgelegt ist, die Auswirkungen von Naturkatastrophen oder von Menschen verursachten Katastrophen zu mildern. Diese Pläne behandeln die Wiederherstellung von Diensten der Informationssysteme und Schlüsselfunktionen des Unternehmens.

(294) Nach einem Zwischenfall einer bestimmten Risikostufe muss die kompromittierte CA von einem akkreditieren PKI-Prüfer erneut geprüft werden (siehe Abschnitt 8).

(295) Kann eine kompromittierte CA nicht mehr arbeiten (z. B. nach einem schweren Zwischenfall), muss ein Migrationsplan für die Übertragung ihrer Funktionen auf eine andere Root-CA erstellt werden. Für die Unterstützung des Migrationsplans muss zumindest die Root-CA der EU zur Verfügung stehen. Die kompromittierte CA stellt ihre Funktion ein.

(296) Die Root-CA nehmen den Plan zu Datenwiederherstellung im Falle eines Systemabsturzes und den Migrationsplan in die Erklärung zum Zertifizierungsbetrieb (CPS) auf.

5.8. Beendigung und Übertragung

*5.8.1. **TLM***

(297) Der TLM beendet seinen Betrieb nicht, aber eine den TLM verwaltende Stelle kann eine andere Stelle übernehmen.

(298) Im Falle eines Wechsels der Verwaltungsstelle:

- beantragt sie die Genehmigung der CPA für den Wechsel des TLM-Managements von der alten auf die neue Stelle;
- die CPA genehmigt den Wechsel des TLM-Managements;
- sämtliche Audit-Protokolle und archivierten Aufzeichnungen werden von der alten Managementstelle an die neue Stelle übertragen.

5.8.2. Root-CA

(299) Die Root-CA beendet/beginnt ihren Betrieb nicht ohne die Erstellung eines Migrationsplans (in der maßgeblichen CPS festgelegt), der den laufenden Betrieb für alle Abonnenten gewährleistet.

(300) Im Falle der Beendigung des Root-CA-Dienstes veranlasst die Root-CA Folgendes:

- Benachrichtigung der CPA;
- Benachrichtigung des TLM, damit dieser das Zertifikat der Root-CA von der ECTL streichen kann;

- Sperrung der entsprechenden Root-CA mittels Ausstellung einer Zertifikatsperrliste (CRL), in der sie selbst enthalten ist;
- Warnung der Root-CA, mit denen sie eine Vereinbarung über die Erneuerung von EA/AA-Zertifikaten geschlossen hat;
- Vernichtung des privaten Schlüssels der Root-CA;
- Übermittlung der letzten Informationen über den Sperrstatus an den Vertrauenden Dritten (von der Root-CA signierte CRL) mit dem deutlichen Hinweis, dass es sich um die letzte Information über Sperrungen handelt;
- Archivierung aller Audit-Protokolle und sonstiger Aufzeichnungen vor der Beendigung der PKI;
- Übermittlung archivierter Aufzeichnungen an eine geeignete Behörde.

(301) Der TLM streicht das entsprechende Root-CA-Zertifikat von der ECTL.

5.8.3. ***EA/AA***

(302) Wird der EA/AA-Dienst beendet, übermittelt die EA/AA-Stelle vor der Beendigung entsprechende Benachrichtigungen. Eine EA oder AA beendet/beginnt ihren Betrieb nicht ohne die Erstellung eines Migrationsplans (in der maßgeblichen CPS festgelegt), der den laufenden Betrieb für alle Abonnenten gewährleistet. Die EA/AA

- informiert die Root-CA per Einschreiben;
- zerstört den privaten Schlüssel der CA;
- überträgt ihre Datenbank an die von der Root-CA benannte Stelle;
- stellt die Ausstellung von Zertifikaten ein;
- während ihre Datenbank übertragen wird und bis die Datenbank an einer neuen Stelle voll funktionsfähig ist, erhält sie Kapazitäten zur Genehmigung von Anträgen der zuständigen Datenschutzbehörde aufrecht;
- wurde eine Sub-CA kompromittiert, sperrt die Root-CA die Sub-CA und gibt eine neue CRL mit einem Verzeichnis gesperrter Sub-CA heraus;
- archiviert vor der Beendigung der PKI alle Audit-Protokolle und sonstigen Aufzeichnungen;
- überträgt archivierte Aufzeichnungen an eine von der Root-CA benannte Stelle.

(303) Im Falle der Beendigung der Dienste der CA ist die CA dafür verantwortlich, alle für die Erfordernisse von CA- und PKI-Komponenten relevanten Aufzeichnungen zu führen.

6. TECHNISCHE SICHERHEITSKONTROLLEN

6.1. Generierung und Installation von Schlüsselpaaren

6.1.1. TLM, Root-CA, EA, AA

(304) Der Prozess der Generierung von Schlüsselpaaren erfüllt folgende Anforderungen:

- jeder Teilnehmer muss in der Lage sein, im Einklang mit den Abschnitten 6.1.4 und 6.1.5 seine eigenen Schlüsselpaare zu generieren;
- der Prozess der Ableitung symmetrischer Verschlüsselungsschlüssel und eines MAC-Schlüssels für Zertifikatanträge (ECIES) wird gemäß [1] und [5] durchgeführt;
- im Schlüsselgenerierungsprozess werden die in den Abschnitten 6.1.4.1 und 6.1.4.2 beschriebenen Algorithmen und Schlüssellängen verwendet;
- für den Prozess der Generierung von Schlüsselpaaren gelten die Anforderungen für die „sichere Speicherung privater Schlüssel“ (siehe Abschnitt 6.1.5);
- die Root-CA und deren Abonnenten (Sub-CA) stellen sicher, dass die Integrität und Authentizität ihrer öffentlichen Schlüssel und damit verbundener Parameter während der Verteilung an die registrierten Stellen der Sub-CA erhalten bleiben.

6.1.2. EE – mobile C-ITS-Station

(305) Jede mobile C-ITS-Station generiert ihre eigenen Schlüsselpaare gemäß den Abschnitten 6.1.4 und 6.1.5.

(306) Der Prozess der Ableitung symmetrischer Verschlüsselungsschlüssel und eines MAC-Schlüssels für Zertifikatanträge (ECIES) wird gemäß [1] und [5] durchgeführt;

(307) Bei den Schlüsselgenerierungsprozessen werden die in den Abschnitten 6.1.4.1 und 6.1.4.2 beschriebenen Algorithmen und Schlüssellängen verwendet.

(308) Für die Prozesse der Generierung von Schlüsselpaaren gelten die Anforderungen für die „sichere Speicherung privater Schlüssel“ (siehe Abschnitt 6.1.5);

6.1.3. EE – ortsfeste C-ITS-Station

(309) Jede ortsfeste C-ITS-Station generiert ihr eigenes Schlüsselpaar gemäß den Abschnitten 6.1.4 und 6.1.5.

(310) Bei den Schlüsselgenerierungsprozessen werden die in den Abschnitten 6.1.4.1 und 6.1.4.2 beschriebenen Algorithmen und Schlüssellängen verwendet.

(311) Für die Prozesse der Generierung von Schlüsselpaaren gelten die Anforderungen für die „sichere Speicherung privater Schlüssel“ (siehe Abschnitt 6.1.5).

6.1.4. Kryptografische Anforderungen

(312) PKI-Teilnehmer müssen hinsichtlich des Signaturalgorithmus, der Schlüssellänge, des Zufallszahlengenerators und der Link-Zertifikate die in den folgenden Absätzen dargelegten kryptografischen Anforderungen erfüllen.

6.1.4.1. *Algorithmus und Schlüssellänge – Signaturalgorithmen*

(313) Spätestens zwei Jahre nach dem Inkrafttreten dieser Verordnung müssen alle PKI-Teilnehmer (TLM, Root-CA, EA, AA und C-ITS-Stationen) in der Lage sein, gemäß Tabelle 4 Schlüsselpaare zu generieren und den privaten Schlüssel mit ausgewählten Algorithmen für Signaturvorgänge zu nutzen.

(314) Sämtliche PKI-Teilnehmer, die ihrer Funktion gemäß Definition in Abschnitt 1.3.6 entsprechend die Integrität der ECTL, der Zertifikate und/oder der signierten Nachrichten kontrollieren müssen, unterstützen die entsprechenden, in Tabelle 5 aufgeführten Algorithmen für die Verifizierung. Insbesondere müssen die C-ITS-Stationen in der Lage sein, die Integrität der ECTL zu überprüfen.

	TLM	Root-CA	EA	AA	C-ITS-Station
ECDSA_nistP256_ung_SHA 256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	-	-
X kennzeichnet die verbindliche Unterstützung					

Tabelle 4: Generierung von Schlüsselpaaren und Nutzung des privaten Schlüssels für Signaturvorgänge

	TLM	Root-CA	EA	AA	C-ITS-Station
ECDSA_nistP256_ung_SHA 256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	X	X
X kennzeichnet die verbindliche Unterstützung					

Tabelle 5: Überblick über Verifizierungen

(315) Wenn die CPA dies auf der Grundlage neu festgestellter kryptografischer Schwachstellen entscheidet, müssen alle C-ITS-Stationen so bald wie möglich zu einem der beiden Algorithmen (ECDSA_nistP256_with_SHA 256 oder ECDSA_brainpoolP256_with_SHA 256) wechseln können. Der/die tatsächlich verwendete(n) Algorithmus/Algorithmen werden in der Erklärung zum Zertifizierungsbetrieb (CPS) der CA festgelegt, die im Einklang mit der vorliegenden Certificate Policy (CP) das Zertifikat für den entsprechenden öffentlichen Schlüssel ausstellt.

6.1.4.2. *Algorithmus und Schlüssellänge – Verschlüsselungsalgorithmen für Enrollment und Berechtigung*

(316) Spätestens zwei Jahre nach dem Inkrafttreten dieser Verordnung müssen alle PKI-Teilnehmer (TLM, EA, AA und C-ITS-Stationen) in der Lage sein, gemäß Tabelle 6 öffentliche Schlüssel für die Verschlüsselung von Enrollment- und Berechtigungsanträgen und den Antworten darauf mit ausgewählten Algorithmen zu nutzen. Der/die tatsächlich verwendete(n) Algorithmus/Algorithmen werden in der Erklärung zum Zertifizierungsbetrieb (CPS) der CA festgelegt, die im Einklang mit der vorliegenden Certificate Policy (CP) das Zertifikat für den entsprechenden öffentlichen Schlüssel ausstellt.

(317) Die in Tabelle 6 benannten Algorithmen geben die Länge der Schlüssel und die Länge der Hash-Algorithmen an und sind gemäß [5] zu implementieren.

	TLM	Root-CA	EA	AA	C-ITS-Station
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X kennzeichnet die verbindliche Unterstützung					

Tabelle 6: Verwendung öffentlicher Schlüssel für die Verschlüsselung von Enrollment- und Berechtigungsanträgen/Antworten

(318) Spätestens zwei Jahre nach dem Inkrafttreten dieser Verordnung müssen alle PKI-Teilnehmer (EA, AA und C-ITS-Stationen) in der Lage sein, gemäß Tabelle 7 Schlüsselpaare zu generieren und den privaten Schlüssel zur Entschlüsselung von Enrollment- und Berechtigungsanträgen und den Antworten darauf zu nutzen:

	TLM	Root-CA	EA	AA	C-ITS-Station
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X kennzeichnet die verbindliche Unterstützung					

Tabelle 7: Generierung von Schlüsselpaaren und Nutzung des privaten Schlüssels für die Entschlüsselung von Enrollment- und Berechtigungsanträgen und den Antworten darauf

6.1.4.3. *Krypto-Agilität*

(319) Die Anforderungen an Schlüssellängen und Algorithmen müssen im Zeitablauf geändert werden, damit ein angemessenes Sicherheitsniveau aufrechterhalten wird. Die CPA überwacht die Notwendigkeit solcher Änderungen unter Berücksichtigung tatsächlicher Gefährdungen und der neusten Entwicklungen in der Kryptografie. Sie wird eine Aktualisierung dieser Certificate Policy entwerfen, genehmigen und veröffentlichen, wenn sie beschließt, dass die kryptografischen Algorithmen aktualisiert werden sollten. Wird mit einer neuen Ausgabe dieser Certificate Policy (CP) eine Änderung des Algorithmus und/oder der Schlüssellänge angekündigt, führt die CPA eine Migrationsstrategie mit Übergangsfristen ein, während der die alten Algorithmen und Schlüssellängen weiter unterstützt werden müssen.

(320) Um die Übertragung auf neue Algorithmen und/oder Schlüssellängen zu ermöglichen und zu erleichtern, wird empfohlen, dass alle PKI-Teilnehmer Hardware und/oder Software implementieren, die zu einer Umstellung der Schlüssellängen und Algorithmen in der Lage ist.

(321) Änderungen der Wurzel- und TLM-Zertifikate werden mit Hilfe von Link-Zertifikaten (siehe Abschnitt 4.6) unterstützt und durchgeführt; Link-Zertifikate werden zur Überbrückung des Übergangszeitraums zwischen alten und neuen Wurzelzertifikaten genutzt („Migration des Trust Models“).

6.1.5. Sichere Speicherung privater Schlüssel

In diesem Abschnitt werden die Anforderungen an die sichere Speicherung und Generierung von Schlüsselpaaren und Zufallsnummern für CA und Endteilnehmer beschrieben. Diese Anforderungen werden für kryptografische Module festgelegt und in den folgenden Unterabschnitten beschrieben.

6.1.5.1. *Root-CA-, Sub-CA- und TLM-Ebene*

(322) Ein kryptografisches Modul ist für Folgendes zu verwenden:

- Generierung, Nutzung, Verwaltung und Speicherung privater Schlüssel;

- Generierung und Verwendung von Zufallszahlen (die Bewertung der Funktion zur Generierung von Zufallszahlen ist Bestandteil der Sicherheitsevaluierung und -zertifizierung);
- Erstellung von Sicherungen (Backups) privater Schlüssel gemäß Abschnitt 6.1.6;
- Löschung privater Schlüssel.

Das kryptografische Modul wird mit einem der folgenden Schutzprofile (PP) zertifiziert, wobei die Vertrauenszusicherungsebene EAL-4 oder höher ist:

- Schutzprofile für HSM:
  - CEN EN 419 221-2: Schutzprofile für die kryptografischen Module von TSP – Teil 2: Kryptografisches Modul für CSP-Signaturvorgänge mit Backup;
  - CEN EN 419 221-4: Schutzprofile für die kryptografischen Module von TSP – Teil 4: Kryptografisches Modul für CSP-Signaturvorgänge ohne Backup;
  - CEN EN 419 221-5: Schutzprofile für die kryptografischen Module von TSP – Teil 5: Kryptografisches Modul für Vertrauensdienste;
- Schutzprofile für Smartcards:
  - CEN EN 419 211-2: Schutzprofile für sichere Signaturerstellungseinheiten – Teil 2: Gerät mit Schlüsselgenerierung;
  - CEN EN 419 211-3: Schutzprofile für sichere Signaturerstellungseinheiten – Teil 3: Gerät mit Schlüsselimport.

Für den manuellen Zugriff auf das kryptografische Modul ist eine zwei-Faktoren-Authentifizierung vom Administrator erforderlich. Darüber hinaus ist die Beteiligung von zwei berechtigten Personen erforderlich.

Mit der Implementierung eines kryptografischen Moduls wird sichergestellt, dass außerhalb des kryptografischen Moduls kein Zugang zu Schlüsseln möglich ist. Das kryptografische Modul umfasst einen Zugangskontrollmechanismus zur Verhinderung einer unbefugten Nutzung privater Schlüssel.

6.1.5.2. *Endteilnehmer*

(323) Ein kryptografisches Modul für Endteilnehmer (EE) ist für Folgendes zu verwenden:

- Generierung, Nutzung, Verwaltung und Speicherung privater Schlüssel;
- Generierung und Verwendung von Zufallszahlen (die Bewertung der Funktion zur Generierung von Zufallszahlen ist Bestandteil der Sicherheitsevaluierung und -zertifizierung);
- sichere Löschung eines privaten Schlüssels.

(324) Das kryptografische Modul ist vor unbefugter Entfernung, Ersetzung und Änderung zu schützen. Sämtliche Schutzprofile und zugehörigen Unterlagen, die für die Sicherheitszertifizierung des kryptografischen Moduls gelten,

werden nach ISO 15408 bewertet, validiert und zertifiziert, wobei die Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten der Gruppe Hoher Beamter für Informationssicherheit (SOG-IS) oder ein gleichwertiges europäisches System für die Cybersicherheitszertifizierung innerhalb des einschlägigen europäischen Cybersicherheitsrahmens anzuwenden ist.

(325) Da es wichtig ist, das höchstmögliche Sicherheitsniveau aufrechtzuerhalten, werden Sicherheitszertifikate für das kryptografische Modul im Rahmen der Regelung zur Zertifizierung nach gemeinsamen Kriterien (Common Criteria) (ISO 15408) ausgestellt von einer Konformitätsbewertungsstelle, die vom Managementausschuss im Rahmen der SOG-IS-Abkommen anerkannt wird, oder von einer Konformitätsbewertungsstelle, die bei einer nationalen Cybersicherheitszertifizierungsbehörde eines Mitgliedstaats akkreditiert ist. Eine solche Konformitätsbewertungsstelle muss Bedingungen für die Sicherheitsevaluierung erfüllen, die denen nach dem SOG-IS-Abkommen zur gegenseitigen Anerkennung mindestens gleichwertig sind.

Anmerkung: der Link zwischen dem kryptografischen Modul und der C-ITS-Station ist zu schützen.

6.1.6. Backup von privaten Schlüsseln

(326) Die Generierung, Speicherung und Nutzung von Backups privater Schlüssel muss mindestens den Sicherheitsanforderungen genügen, die für die Originalschlüssel erforderlich sind.

(327) Backups privater Schlüssel werden von Root-CA, EA und AA erstellt.

(328) Für EC und AT werden keine Backups privater Schlüssel erstellt.

6.1.7. Vernichtung privater Schlüssel

(329) Root-CA, EA, AA sowie mobile und ortsfeste C-ITS-Stationen vernichten ihren privaten Schlüssel und alle entsprechenden Backups, wenn ein neues Schlüsselpaar und ein entsprechendes Zertifikat generiert und erfolgreich installiert worden ist, und die Überlappungszeit (wenn überhaupt, dann nur bei nur CA) verstrichen ist. Private Schüssel werden mit Hilfe des Mechanismus vernichtet, den das für die Schlüsselspeicherung verwendete kryptografische Modul bietet, oder die Vernichtung erfolgt gemäß Beschreibung in dem entsprechenden, in Abschnitt 6.1.5.2 beschriebenen Schutzprofil (PP).

6.2. Aktivierungsdaten

(330) Aktivierungsdaten beziehen sich auf Authentifizierungsfaktoren, die für den Betrieb von kryptografischen Modulen erforderlich sind, um unbefugten Zugang zu verhindern. Die Nutzung der Aktivierungsdaten eines kryptografischen Geräts einer Wurzelzertifizierungsstelle (CA) erfordert das Tätigwerden von zwei befugten Personen.

6.3. Computer-Sicherheitskontrollen

(331) Die Computersicherheitskontrollen der CA werden dem hohen Sicherheitsniveau entsprechend unter Einhaltung der Anforderungen der ISO/IEC 27002 konzipiert.

6.4. Lebenslange technische Kontrollen

(332) Die technischen Kontrollen der CA erstrecken sich über den gesamten Lebenszyklus der CA, wobei dies insbesondere die Anforderungen in Abschnitt 6.1.4.3 („Krypto-Agilität“) einschließt.

6.5. Kontrollen der Netzsicherheit

(333) Die Netze der CA (Root-CA, EA und AA) werden im Einklang mit den Anforderungen und Durchführungsleitlinien der ISO/IEC 27001 und ISO/IEC 27002 gegen Angriffe widerstandsfähig gemacht.

(334) Die Verfügbarkeit der CA-Netze werden unter Berücksichtigung des geschätzten Verkehrsaufkommens konzipiert.

7. ZERTIFIKATPROFILE, CRL UND CTL

7.1. Zertifikatprofil

(335) Die in [5] definierten Zertifikatprofile werden für TLM, Wurzelzertifikate, EA-Zertifikate, AA-Zertifikate, AT und EC verwendet. Die staatlichen EA in den einzelnen Ländern können für Enrollment-Berechtigungsnachweise (EC) andere Zertifikatprofile nutzen.

(336) In den Zertifikaten von Root-CA, EA und AA werden die Genehmigungen angegeben, für die diese CA (Root-CA, EA und AA) Zertifikate ausstellen dürfen.

(337) Auf der Grundlage von [5]:

- nutzt jede Root-CA ihren eigenen privaten Signaturschlüssel zur Ausstellung von CRL;
- der TLM verwendet seinen eigenen privaten Signatur-Schlüssel zur Ausstellung der ECTL.

7.2. Gültigkeit von Zertifikaten

(338) Alle C-ITS-Zertifikatprofile enthalten ein Ausstellungs- und ein Ablaufdatum, die die Gültigkeitsdauer des Zertifikats darstellen. Auf den einzelnen PKI-Ebenen werden die Zertifikate rechtzeitig vor ihrem Ablauf generiert.

(339) Die Gültigkeitsdauer der CA- und EC-Zertifikate schließt eine Überlappungszeit ein. TLM- und Root-CA-Zertifikate werden frühestens drei Monate und spätestens einen Monat vor Beginn ihrer Gültigkeit ausgestellt (basierend auf dem Laufzeitbeginn laut Zertifikat) und auf die ECTL (Liste vertrauenswürdiger europäischer Zertifikate) gesetzt. Diese Phase des Ladens der Anfangsgrößen wird für die sichere Verteilung der Zertifikate an alle entsprechenden Vertrauenden Dritten gemäß Abschnitt 2.2 benötigt. Dadurch wird sichergestellt, dass alle Vertrauenden Dritten ab dem Beginn der Überlappungszeit bereits in der Lage sind, mit einem neuen Zertifikat herausgegebene Meldungen zu verifizieren.

(340) Zu Beginn der Überlappungszeit werden die aufeinanderfolgenden CA-, EC- und AT-Zertifikate ausgestellt (sofern zutreffend), an die entsprechenden Vertrauenden Dritten verteilt und von diesen installiert. Während der Überlappungszeit werden die aktuellen Zertifikate nur zu Verifizierungszwecken genutzt.

(341) Da die in Tabelle 8 aufgeführten Gültigkeitsdauern die Gültigkeitsdauern der jeweils übergeordneten Zertifikate nicht überschreiten dürfen, gelten folgende Einschränkungen:

- maximumvalidity [maximale Gültigkeit] (Root-CA) = privatekeyusage [Privatschlüsselnutzung] (Root-CA) + maximumvalidity [maximale Gültigkeit] (EA, AA);
- maximumvalidity [maximale Gültigkeit] (EA) = privatekeyusage [Privatschlüsselnutzung] (EA) + maximumvalidity [maximale Gültigkeit] (EC);
- maximumvalidity [maximale Gültigkeit] (AA) = privatekeyusage [Privatschlüsselnutzung] (AA) + [Zeitraum zum Laden der Anfangsgrößen] (AT).

(342) Die Gültigkeit der Link-Zertifikate (Root und TLM) beginnt mit der Nutzung des entsprechenden Privatschlüssels und endet mit der maximalen Gültigkeitsdauer der Root-CA oder des TLM.

(343) Tabelle 8 sind die maximalen Gültigkeitsdauern für C-ITS-CA-Zertifikate zu entnehmen (die Gültigkeitsdauern von AT sind Abschnitt 7.2.1 zu entnehmen).

Stelle	Max. Nutzungszeitsaum für private Schlüssel	Maximale Gültigkeitsdauer
Root-CA	3 Jahre	8 Jahre
EA	2 Jahre	5 Jahre
AA	4 Jahre	5 Jahre
EC	3 Jahre	3 Jahre
TLM	3 Jahre	4 Jahre

Tabelle 8: Gültigkeitsdauer der Zertifikate im Rahmen des C-ITS Trust Models

7.2.1. Pseudonym-Zertifikate

(344) In diesem Zusammenhang werden Pseudonyme durch Berechtigungstickets (AT) umgesetzt. Folglich bezieht sich dieser Abschnitt auf AT und nicht auf Pseudonyme.

(345) Die Anforderungen dieses Abschnitts gelten nur für AT mobiler C-ITS-Stationen, die CAM- und DENM-Benachrichtigungen senden und bei denen datenschutzrechtliche Risiken im Zusammenhang mit dem Standort zutreffen. Für die AT für ortsfeste C-ITS-Stationen und mobile C-ITS-Stationen, die für besondere Aufgaben eingesetzt werden und bei denen keine datenschutzrechtlichen Risiken im Zusammenhang mit dem Standort zutreffen, (z-. B. gekennzeichnete Einsatzfahrzeuge und Fahrzeuge der Strafverfolgungsbehörden) gelten keine besonderen Anforderungen an AT-Zertifikate.

(346) Es gelten folgende Begriffsbestimmungen:

- „Gültigkeitsdauer für AT“ – der Zeitraum, für den ein AT (Berechtigungsticket) gültig ist, d. h. der Zeitraum zwischen dem Anfangs- und dem Ablaufdatum des AT;
- „Zeitraum des Ladens der Anfangsgrößen für AT“ – unter dem Laden der Anfangsgrößen wird die Möglichkeit für C-ITS-Stationen verstanden, AT bereits vor dem Beginn der Gültigkeitsdauer zu erhalten. Der Zeitraum des Ladens der Anfangsgrößen ist der höchstzulässige Zeitraum zwischen der Beantragung von AT bis zum Ende des letzten Gültigkeitsdatums beantragter AT;
- „Nutzungszeitraum für AT“ – der Zeitraum, in dem ein AT effektiv zur Signierung von CAM/DENM-Benachrichtigungen genutzt wird;
- „maximale Anzahl paralleler AT“ – die Anzahl der AT, aus denen eine C-ITS-Station zu einem beliebigen Zeitpunkt zur Signierung einer CAM-/DENM-Benachrichtigung auswählen kann, d. h. die Anzahl verschiedener AT, die an eine C-ITS-Station ausgegeben werden und gleichzeitig gültig sind.

(347) Es gelten die folgenden Anforderungen:

- der Zeitraum des Ladens der Anfangsgrößen für AT darf drei Monate nicht überschreiten;
- die Gültigkeitsdauer für AT darf eine Woche nicht überschreiten;
- die Höchstzahl paralleler AT darf pro C-ITS-Station 100 nicht überschreiten;
- die Nutzungsdauer eines AT hängt davon ab, welche Strategie bei AT-Wechseln verfolgt wird und wie lange ein Fahrzeug in Betrieb ist; sie wird aber durch die maximale Anzahl paralleler AT und die Gültigkeitsdauer begrenzt. Konkret entspricht die durchschnittliche Nutzungsdauer für eine C-ITS-Station mindestens der Betriebszeit des Fahrzeugs während einer Gültigkeitsdauer, geteilt durch die Höchstzahl paralleler AT.

7.2.2. Berechtigungstickets für ortsfeste C-ITS-Stationen

(348) Es gelten die Begriffsbestimmungen in Abschnitt 7.2.1 und die folgenden Anforderungen:

- der Zeitraum des Ladens der Anfangsgrößen für AT darf drei Monate nicht überschreiten;
- die Höchstzahl paralleler AT darf pro C-ITS-Station zwei nicht überschreiten.

7.3. Sperrung von Zertifikaten

7.3.1. Sperrung von CA-, EA- und AA-Zertifikaten

Root-CA-, EA- und AA-Zertifikate können gesperrt werden. Gesperrte Zertifikate von Root-CA, EA und AA werden so bald wie möglich unter Vermeidung unangemessener Verzögerungen auf einer Zertifikatssperrliste (CRL) veröffentlicht. Diese CRL wird von der entsprechenden Root-CA signiert und verwendet das in Abschnitt 7.4 beschriebene Profil. Zur Sperrung von Zertifikaten einer Root-CA gibt

die entsprechende Root-CA eine CRL heraus, auf der sie selbst steht. Darüber hinaus gilt für Fälle einer Sicherheitskompromittierung Abschnitt 5.7.3. Darüber hinaus streicht der TLM gesperrte CA aus der Trust List und gibt eine neue Trust List heraus. Abgelaufene Zertifikate sind aus dem entsprechenden CRL und der Liste vertrauenswürdiger Zertifikate zu streichen.

(349) Zertifikate werden gesperrt, wenn:

- die Root-CA Grund zu der Annahme oder dem starken Verdacht haben, dass der entsprechende private Schlüssel kompromittiert wurde;
- der Root-CA mitgeteilt wurde, dass der Vertrag mit dem Abonnenten beendet worden ist;
- Angaben (beispielsweise Name und Verbindungen zwischen CA und Subjekt) im Zertifikat falsch sind oder sich geändert haben;
- ein Sicherheitsvorfall eintritt, der sich auf den Zertifikatsinhaber auswirkt;
- ein Audit (siehe Abschnitt 8) zu einem negativen Ergebnis führt.

(350) Der Abonnent unterrichtet die CA unverzüglich über eine bekannte oder vermutete Kompromittierung seines privaten Schlüssels. Es muss sichergestellt sein, dass nur authentifizierte Anträge zu gesperrten Zertifikaten führen.

7.3.2. Sperrung von Enrollment-Berechtigungsnachweisen

(351) Die Sperrung von Enrollment-Berechtigungsnachweisen (EC) kann vom Abonnenten der C-ITS-Station ausgelöst werden (Ablauf 34) und wird mittels einer internen schwarzen Liste in einer Datenbank für Sperrungen mit einem Zeitstempel umgesetzt, die von den einzelnen EA generiert und gepflegt wird. Die schwarze Liste wird nie veröffentlicht und ist vertraulich zu behandeln; sie wird nur von der entsprechenden EA verwendet, um im Zusammenhang mit Anträgen auf AT und neue EC die Gültigkeit der entsprechenden EC zu verifizieren.

7.3.3. Sperrung von Berechtigungstickets

(352) Da AT nicht von entsprechenden CA gesperrt werden, habe sie eine kurze Laufzeit und dürfen nicht zu lange bevor sie gültig werden ausgestellt werden. Die zulässigen Werte für den Lebenszyklusparameter des Zertifikats werden in Abschnitt 7.2 dargelegt.

7.4. Zertifikatssperrliste

(353) Format und Inhalt der von der Root-CA herausgegebenen Zertifikatsperrliste (CRL) entsprechen den in [1] festgelegten Werten.

7.5. European Certificate Trust List (Liste vertrauenswürdiger europäischer Zertifikate)

(354) Format und Inhalt der vom TLM herausgegebenen Zertifikatsperrliste (CRL) entsprechen den in [1] festgelegten Werten.

8. COMPLIANCE-AUDITS UND ANDERE BEWERTUNGEN

8.1. Audit-Themen und Audit-Grundlage

(355) Der Zweck von Compliance-Audits besteht darin, zu verifizieren, ob TLM, Root-CA, EA und AA nach der vorliegenden Certificate Policy (CP) arbeiten. Die TLM, Root-CA, EA und AA wählen für den Audit ihrer Erklärung zum Zertifizierungsbetrieb (CPS) einen unabhängig handelnden, akkreditierten PKI-Prüfer. Der Audit wird mit einer Bewertung nach ISO/IEC 27001 und ISO/IEC 27002 kombiniert.

(356) Für eine Root-CA werden Compliance-Audits von der Root-CA selbst (Ablauf 13) und für eine Sub-CA von deren untergeordneten EA/AA angeordnet.

(357) Ein Compliance-Audit für den TLM wird von der CPA angeordnet (Ablauf 38).

(358) Auf entsprechendes Ersuchen führt ein akkreditierter PKI-Prüfer einen Compliance-Audit auf einer der folgenden Ebenen durch:

(1) Konformität der CPS von TLM, Root-CA, EA oder AA mit dieser Certificate Policy (CP);

(2) Konformität der vorgesehenen Praktiken von TLM, Root-CA, EA oder AA mit deren CPS, vor der Aufnahme des Betriebs;

(3) Konformität der Praktiken und betrieblichen Tätigkeiten von TLM, Root-CA, EA oder AA mit deren CPS, während des Betriebs.

(359) Der Audit erstreckt sich auf alle in der vorliegenden Certificate Policy (CP) aufgeführten, von den zum Audit vorgesehenen TLM, Root-CA, EA oder AA zu erfüllenden Anforderungen. Sie umfasst darüber hinaus den Betrieb der CA in der PKI der C-ITS einschließlich aller in deren CPS erwähnten Prozesse, der Räumlichkeiten und der verantwortlichen Personen.

(360) Der akkreditierte PKI-Prüfer legt der Root-CA (Ablauf 36), EA, AA oder CPA (Ablauf 16 und 40), wie jeweils zutreffend, einen ausführlichen Bericht über den Audit vor.

8.2. Häufigkeit der Audits

(361) Root-CA, TLM, EA oder AA beauftragen in den folgenden Fällen einen akkreditierten PKI-Prüfung mit einer Compliance-Prüfung an sich selbst:

- bei ihrer ursprünglichen Einrichtung (Compliance der Stufen 1 und 2);
- bei jeder Änderung der CP. Die CPA legt den Inhalt der CP-Änderung und den Zeitplan für deren Einsatz fest und bestimmt den Audit-Bedarf dementsprechend (einschließlich der erforderlichen Compliance-Stufe);
- bei jeder Änderung ihrer CPS (Compliance-Stufen 1, 2 und 3). Da die Verwaltungsstellen von Root-CA TLM und EA/AA entscheiden, welche Änderungen bei der Umsetzung sich aus der Aktualisierung ihrer Erklärung zum Zertifizierungsbetrieb (CPS) ergeben, geben sie einen Compliance-Audit in Auftrag, bevor sie die betreffenden Änderungen umsetzen. Bei nur geringfügigen Änderungen der CPS (z. B. redaktioneller Art) kann die Verwaltungsstelle bei der CPA in einem

ordnungsgemäß begründeten Antrag um die Genehmigung bitten, Compliance-Audits der Stufe 1, 2 oder 3 überspringen zu dürfen;

- regelmäßig, mindestens jedoch alle drei Jahre während des Betriebs (Compliance der Stufe 3).

8.3. Identität/Qualifikation des Prüfers

(362) Die zu prüfende CA wählt ein(n) unabhängig handelnde(s), akkreditierte(s) Unternehmen/Organisation („Audit-Stelle“) oder akkreditierte PKI-Prüfer für ihren Audit nach vorliegender Certificate Policy (CP) aus. Die Audit-Stelle wird von einem Mitglied der European Accreditation[1] akkreditiert und zertifiziert.

8.4. Beziehung des Prüfers zur geprüften Stelle

(363) Der akkreditierte PKI-Prüfer muss von der geprüften Stelle unabhängig sein.

8.5. Aufgrund von Mängeln getroffene Maßnahmen

(364) Wird in einem Auditbericht mangelnde Compliance eines TLM festgestellt, erteilt die CPA dem TLM eine Anordnung, umgehend Vorbeugungs- bzw. Korrekturmaßnahmen zu treffen.

(365) Stellt eine Root-CA, in deren Auditbericht mangelnde Compliance festgestellt wurde, einen neuen Antrag, lehnt die CPA den Antrag ab und übermittelt der Root-CA eine entsprechenden Ablehnungsbescheid (Ablauf 4). In derartigen Fällen wird die Root-CA suspendiert. Sie muss Korrekturmaßnahmen treffen, den Audit erneut in Auftrag geben und einen erneuten Antrag auf Genehmigung durch die CPA stellen. Die Root-CA darf nicht zulassen, dass während der Suspendierung Zertifikate ausgestellt werden.

(366) Bei einem regulären Audit einer Root-CA oder bei einer Änderungen an der CPS einer Root-CA kann die CPA je nach Art der im Auditbericht beschriebenen Nichtkonformität entscheiden, die Root-CA zu sperren und diese Entscheidung dem TLM mitzuteilen (Ablauf 2) und so die Streichung des Zertifikats der Root-CA aus der ECTL und die Aufnahme der Root-CA in die Zertifikatssperrliste (CRL) veranlassen. Die CPA übermittelt der Root-CA einen entsprechenden Ablehnungsbescheid (Ablauf 4). Die Root-CA muss Korrekturmaßnahmen treffen, erneut einen umfassenden Audit (Stufen 1 bis 3) in Auftrag geben und einen neuen Antrag auf die Genehmigung durch die CPA stellen. Alternativ kann die CPA beschließen, die Root-CA nicht zu sperren, sondern ihr eine Nachfrist zu gewähren, in der die Root-CA Korrekturmaßnahmen trifft, erneut einen Audit in Auftrag gibt und den Auditbericht erneut bei der CPA einreicht. In diesem Fall muss der Betrieb der Root-CA ausgesetzt werden und ihr ist es nicht gestattet, Zertifikate und CRL auszustellen.

(367) Im Falle Audits von EA/AA entscheidet die Root-CA, ob sie den Bericht annimmt oder nicht. Je nach Ergebnis des Audits entscheidet die Root-CA, ob sie das EA-/AA-Zertifikat gemäß den Vorschriften in der Erklärung zum Zertifizierungsbetrieb (CPS) der Root-CA sperrt. Die Root-CA stellt jederzeit sicher, dass EA/AA die vorliegende Certificate Policy (CP) einhalten.

---

[1] Die Mitglieder der Europäischen Akkreditierungsstelle werden unter folgender Adresse aufgeführt: http://www.european-accreditation.org/ea-members

8.6. Mitteilung der Ergebnisse

(368) Root-CA und der TLM übermitteln den Auditbericht an die CPA (Ablauf 16). Die Root-CA und der TLM speichern alle Berichte über von ihnen in Auftrag gegebene Audits. Die CPA übermittelt der Root-CA und dem TLM eine entsprechende Genehmigung oder Ablehnung (Ablauf 4).

(369) Die Root-CA sendet der entsprechenden EA/AA ein Konformitätszertifikat.

9. SONSTIGE BESTIMMUNGEN

9.1. Gebühren

(370) Ein Grundsatz des implementierten C-ITS Trust Models der EU besteht darin, dass die Root-CA gemeinsam für die vollständige Finanzierung der regelmäßigen laufenden Betriebskosten der CPA und der zentralen Elemente (TLM und CPOC), die im Zusammenhang mit den in der vorliegenden Certificate Policy (CP) dargelegten Tätigkeiten anfallen, sorgen.

(371) Die Root-CA (einschließlich der Root-CA der EU) sind berechtigt, bei ihren Sub-CA Gebühren zu erheben.

(372) Jeder Teilnehmer des C-ITS Trust Models erhält während des gesamten Betriebszeitraums diskriminierungsfrei Zugang zu mindestens einer Root-CA, EA und AA.

(373) Jede Root-CA ist berechtigt, die von ihr für die CPA und die zentralen Elemente (TLM und CPOC) gezahlten Gebühren auf die registrierten Teilnehmer des C-ITS Trust Models einschließlich der angemeldeten und autorisierten C-ITS-Stationen umzulegen.

9.2. Finanzielle Verantwortlichkeiten

(374) Die erstmalige Einrichtung einer Root-CA erstreckt sich über einen Zeitraum von mindestens drei Jahren, damit sie Mitglied des C-ITS Trust Models der EU werden kann. Die CPS eines Root-CA-Betreibers enthält auch ausführliche Bestimmungen über die Sperrung oder Schließung von Root-CA.

(375) Jede Root-CA muss die finanzielle Tragfähigkeit der juristischen Person nachweisen, von der sie mindestens drei Jahre lang implementiert wird. Dieser Plan für die finanzielle Tragfähigkeit ist Bestandteil des anfänglichen Satzes von für das Enrollment erforderlichen Unterlagen und muss alle drei Jahre aktualisiert und der CPA gemeldet werden.

(376) Jede Root-CA muss zum Nachweis ihrer finanziellen Nachhaltigkeit der Betriebsleitung und der CPA jedes Jahr die Gebührenstruktur melden, die für die EA/AA und die angemeldeten und autorisierten C-ITS-Stationen gelten.

(377) Alle finanziell und rechtlich verantwortlichen Stellen der Root-CA, EA, AA und der zentralen Elemente (CPOC und TLM) des C-ITS Trust Models müssen ihre betrieblichen Pflichten durch Versicherungen in angemessener Höhe abdecken, um eine Entschädigung für betriebliche Fehler und einen finanziellen Ausgleich für ihre Pflichten erzielen zu können, falls eines der technischen Elemente ausfallen sollte.

9.3. Vertraulichkeit von Geschäftsinformationen

(378) Folgende Angaben sind vertraulich zu behandeln und zu schützen:

- Antragsaufzeichnungen, ob gebilligt oder abgelehnt, von Root-CA, EA, AAA;
- Auditberichte von Root-CA, EA, AA und TLM;
- Pläne der Datenwiederherstellung im Falle eines Systemabsturzes von Root-CA, EA, AA, CPOC und TLM;
- private Schlüssel der Elemente des C-ITS Trust Models (C-ITS-Stationen, TLM, EA, AA, Root-CA);
- sonstige von der CPA sowie den Root-CA, A, AA, TLM und CPOC. als vertraulich eingestufte Informationen.

9.4. Datenschutzplan

(379) In den CPS der Root-CA und der EA/AA werden der Datenschutzplan und die Anforderungen an die Behandlung personenbezogener Angaben und den Datenschutz auf der Grundlage der DSGVO und anderer anwendbarer gesetzlicher Rahmen (z. B. nationale Rechtvorschriften) dargelegt.

10. REFERENZDOKUMENTE

In diesem Anhang werden folgende Referenzdokumente herangezogen:

[1] ETSI TS 102 941 V1.2.1, Intelligent transport systems (ITS) – security, trust and privacy management.

[2] ETSI TS 102 940 V1.3.1, Intelligent transport systems (ITS) – security, ITS communications security architecture and security management.

[3] Certificate policy and certification practices framework (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1 Policy requirements for certification authorities issuing public key certificates.

[5] ETSI TS 103 097 V1.3.1, Intelligent transport systems (ITS) – security, security header and certificate formats.

[6] Calder, A. (2006). Information security based on ISO 27001/ISO 1779: a management guide. Van Haren Publishing.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011): Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement. ISO.