Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM

Februar 2022

Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Ausgabe 2)

Erläuternder Bericht

1 Einleitung

Im vorliegenden Dokument werden die Änderungen erläutert, die in der zweiten Ausgabe (2022) der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV) eingeführt worden sind.

2 Änderungen

Kapitel 1.2

Das Europäische Komitee für Normung (CEN) und das Europäische Institut für Telekommunikationsnormen (ETSI) haben neue Normen bzw. neue Fassungen von Normen, auf die in der vorherigen Ausgabe der TAV verwiesen wurde, veröffentlicht. Diesen Änderungen wurde in der Ausgabe 2 der TAV Rechnung getragen.

Die unten stehende Tabelle enthält eine Gegenüberstellung der alten und neuen Verweise:

Verweis in der 1. Ausgabe der TAV (2017)	**Neuer Verweis in der 2. Ausgabe der TAV (2022)**
ETSI EN 319 411-2 V2.1.1 (2016-02) *Policy requirements for trust service providers issuing EU qualified certificates*	ETSI EN 319 411-2 V2.4.1 (2021-11) *Policy requirements for trust service providers issuing EU qualified certificates*
EN 419211-3:2013 *Protection profiles for secure signature creation device. Part 3: Device with key import*	EN 419211-3:2014 *Protection profiles for secure signature creation device. Part 3: Device with key import*
CEN/TS 419241:2014 *Security Requirements for Trustworthy Systems Supporting Server Signing*	EN 419241-1:2018 *Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements* EN 419 241-2:2019 *Protection Profile for QSCD for Server Signing* TS 119 431-1 V1.2.1 (2021-05) *Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD* EN 419221-5:2018 *Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services*
ETSI EN 319 412-1 V1.1.1 (2016-02) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*	ETSI EN 319 412-1 V1.4.4 (2021-05) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*
ETSI EN 319 412-2 V2.1.1 (2016-02) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*	ETSI EN 319 412-2 V2.2.1 (2020-07) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*

ETSI EN 319 412-3 V1.1.1 (2016-02) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons*	ETSI EN 319 412-3 V1.2.1 (2020-07) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons*
ETSI EN 319 412-4 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates	ETSI EN 319 412-4 V1.2.1 (2021-11) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
ETSI EN 319 412-5 V2.1.1 (2016-02) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*	ETSI EN 319 412-5 V2.3.1 (2020-04) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

Die vorgenommenen Änderungen werden grundsätzlich im Anhang der neuen Versionen der Normen beschrieben. Die wichtigsten Änderungen werden in den nachfolgenden Kapiteln erläutert.

Kapitel 2.1.1

Die Überschrift von Kapitel 7 der Norm ETSI EN 319 411-2 wird vervollständigt, damit sie jener in der Norm entspricht.

Kapitel 2.2.2 Bst. a)

Der Verweis auf Kapitel 6.5.2 der Norm ETSI EN 319 411-2 wird gestrichen, da dieses Kapitel der Norm keine Anforderung an die in Kapitel 2.2.2 der TAV geregelte Generierung der Schlüssel der Antragstellerin oder des Antragstellers eines Zertifikats durch die CSP enthält.

Kapitel 2.2.2 Bst. b)

Der Verweis auf FIPS 140-3 wird hinzugefügt, da die FIPS-Zertifizierung von kryptografischen Modulen nun nach dieser Norm erfolgt. Der Verweis auf FIPS 140-2 wird beibehalten, damit die zuvor durchgeführten Zertifizierungen weiterhin gültig bleiben.

Der Verweis auf das Dokument CWA 14169 wird gestrichen, da dieses durch die Normenreihe EN 419211 ersetzt wurde (siehe Einleitung in EN 419211-1 sowie den Anhang zum Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäss Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt1).

[1] ABl. L 109, 26.4.2016, S. 40–42.

Kapitel 2.2.3 Bst. a) und b)

Auch in diesem Kapitel wird der Verweis auf das Dokument CWA 14169 gestrichen, da dieses durch die Normenreihe EN 419211 ersetzt wurde (siehe oben).

Durch die Streichung dieses Verweises entfällt auch der Verweis auf die Version 2005 der Norm ISO/IEC 15408, die in diesem Kapitel nur zur Bestimmung der Prüfstufe der Produkte-Zertifizierungen nach den Anforderungen von CWA 14169 enthalten war.

Die Anforderung, die sich auf die festgelegte Anzahl aufeinanderfolgender und inkorrekter Aktivierungsversuche bezieht, wird gestrichen, da die im selben Kapitel verlangte Produktzertifizierung bereits bestätigt, dass die Signaturerstellungseinheit die für die vorgesehene Verwendung benötigten Anforderungen erfüllt.

Die Anforderung, die die CSP im Falle einer Sperrung der Nutzung des privaten kryptografischen Schlüssels erfüllen muss, wird neu unter Buchstabe e) aufgeführt, da sie sich nicht direkt auf die unter Buchstabe a) erwähnte Signaturerstellungseinheit bezieht. Es handelt sich vielmehr um eine Anforderung an einen operativen Prozess, den die CSP umsetzen muss, wenn sie eine solche Freigabe anbietet.

Kapitel 2.2.3 Bst. c)

Die TAV verweisen auf Kapitel 6.5.1 der Norm ETSI EN 319 411-2. In der neuen Version dieser Norm wurden neue Anforderungen an die Massnahmen hinzugefügt, die zu ergreifen sind, wenn eine Signaturerstellungseinheit ihre Zertifizierung verliert.

Der Verweis auf Kapitel 6.5.2 der Norm ETSI EN 319 411-2 wird gestrichen, da dieses Kapitel der Norm keine Anforderung an die in Kapitel 2.2.3 der TAV geregelte Generierung der Schlüssel der Antragstellerin oder des Antragstellers eines Zertifikats durch die CSP enthält.

Kapitel 2.2.3 Bst. d)

In Buchstabe d) werden die Anforderungen an die Signaturdienste beschrieben, die für die Generierung von elektronischen Signaturen und Siegeln genutzt werden können. Bei diesen Diensten wird der Signierschlüssel der Zertifikatinhaberin oder des Zertifikatinhabers in der Infrastruktur einer Dienstanbieterin unter der alleinigen Kontrolle der Inhaberin oder des Inhabers des Signierschlüssels und des Zertifikats gespeichert und verwendet. Solche Dienste werden manchmal auch als «Signing Services» (Signaturdienste), «Signature in the Cloud» oder «Signing Server» (Signierserver) bezeichnet. In den TAV geht es um Einheiten, die sich nicht im Besitz der Zertifikatinhaberin oder des Zertifikatinhabers befinden. Es handelt sich im Allgemeinen um ein System, das ein kryptografisches Modul, mit dem die Signatur generiert wird, und ein Signaturaktivierungsmodul enthält, das sicherstellt, dass der Signaturschlüssel unter der alleinigen Kontrolle seiner Inhaberin oder seines Inhabers verwendet wird.

Nach dem Inkrafttreten der Ausgabe 1 der TAV setzten die Fachleute des CEN und des ETSI ihre Standardisierungsarbeiten in Bezug auf diese Systeme fort. Die neuen Normen ETSI TS 119 431-1, EN 419241-1, EN 419241-2 und EN 419221-5 wurden veröffentlicht und sind nun für die Prüfung von Signaturdiensten anerkannt. Daher müssen die TAV angepasst werden, um diesen Entwicklungen Rechnung zu tragen. Die neue Spezifikation ETSI TS 119 431-2 gilt nicht für Elemente, die Teil der im Rahmen eines Signaturdienstes verwendeten Umgebung der Signaturerstellungseinheit sind (vgl. EN 419241 Kap. 1.2, 3.10, 5.13.2 und ETSI TS 119 431-2 Kap. 4.3). Aus diesem Grund wird sie in Kapitel 2.2.3 Buchstabe d) nicht erwähnt.

Die Bezeichnung der Versicherungsstufe, die für den Zugang zu einem solchen Dienst erforderlich ist, wird an die neue Bezeichnung SCAL-2 der Norm EN 419241-1 angepasst.

Auf dem Markt gibt es Signaturdienste, die Systeme nutzen, deren Komponenten zuvor anhand anderer Kriterien in Bezug auf die Generierung von elektronischen Signaturen und Siegeln geprüft wurden. Diese Systeme werden als sichere Signatur- und Siegelerstellungseinheiten im Sinne von Artikel 6 Absatz 2 ZertES akzeptiert, sofern sie ähnliche Sicherheitsziele wie jenen der Normen EN 419241-2 und EN 419221-5 erfüllen. Wie in den europäischen Ländern, die Signaturdienste dulden, wird so ein Übergang gewährleistet, bis sich die Normen EN 419 241-2 und EN 419221-5 für die Evaluierung solcher Systeme durchgesetzt haben. Sobald dies der Fall ist, will die Europäische Kommission ihren Durchführungsbeschluss (EU) 2016/650[2] anpassen und diese neuen Normen darin aufnehmen. Letztere werden dann im Rahmen der Zertifizierung dieser Signaturerstellungseinheiten anwendbar sein. In der Folge werden die TAV ein weiteres Mal revidiert werden müssen, um die Anforderungen in der Schweiz an jene der europäischen Länder anzugleichen.

Falls die CSP solche Signaturdienste anbieten, müssen sie die Anforderungen nach Kapitel 2.2.3 Buchstabe d) innerhalb von sechs Monaten nach dem Inkrafttreten erfüllen. Bis zum Ablauf dieser Frist gilt die entsprechende Anforderung nach Kapitel 2.2.3 Buchstabe d) der ersten Ausgabe der technischen und administrativen Vorschriften vom 23. November 2016 (vgl. Kap. 3).

Kapitel 2.3.1 Bst. a)

Das ETSI hat kürzlich die Spezifikation ETSI TS 119 461 veröffentlicht, mit der die Anforderungen an die Identitätsprüfung präzisiert werden, die die Dienstanbieterin in Anwesenheit der zu identifizierenden Person oder auf Distanz durchführt.

Mit diesem Dokument wird dem Wunsch der europäischen Länder (vgl. Kap. 2, *Position Paper On the review of the eIDAS Regulation – FESA's answer to the European Commission's consultation:* http://www.fesa.eu/public-documents/FESA_Position_Paper_eIDAS_2020_Review.pdf) sowie der Empfehlung der Europäischen Agentur für Netz- und Informationssicherheit ENISA (vgl. Kap. 5, *ENISA Report – REMOTE ID PROOFING Analysis of Methods to carry out identity proofing remotely:* https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing) entsprochen, die Anforderungen für die Personenidentifikation auf Distanz festzulegen.

Der Verweis auf diese neue Spezifikation wird vor allem deshalb in die TAV aufgenommen, um Artikel 7 Absatz 1 VZertES zu konkretisieren und die Evaluierung von Verfahren zur Personenidentifikation auf Distanz, insbesondere mittels audiovisueller Kommunikation in Echtzeit (Videokommunikation), zu erleichtern. Damit wird auf das wachsende Bedürfnis der Anbieterinnen von Zertifizierungsdiensten und deren Kundschaft reagiert, das Identifikationsverfahren zu vereinfachen. Mit der neuen ETSI-Spezifikation werden zudem die Artikel 5 und 6 VZertES im Hinblick auf die Überprüfung der Identität von Antragstellerinnen und Antragstellern eines Zertifikats in Anwesenheit der Person präzisiert.

Je nach Sachlage gelten unterschiedliche Anforderungen der technischen Spezifikation. Die Ausgabe 2 der TAV basiert auf den in Kapitel 9 der ETSI-Spezifikation beschriebenen Anwendungsfällen *(Use Cases)*. Die Anwendungsfälle in Kapitel 9.2 *(Use Cases for Identity Proofing of Natural Person)* gelten für die Überprüfung der Identität einer natürlichen Person, die die Ausstellung eines geregelten Zertifikats für sich selbst beantragt, mit oder ohne Hinweis auf spezifische Attribute im Sinne von Artikel 7

[2] ABl. L 109, 26.4.2016, S. 40–42.

Absatz 3 Buchstabe a ZertES. Der Anwendungsfall 9.4 *(Use Case for Identity Proofing of Natural Person Representing Legal Person)* wiederum bezieht sich auf die Überprüfung der Identität sowohl einer natürlichen Person, die die Ausstellung eines geregelten Zertifikats zur Vertretung einer UID-Einheit beantragt, als auch einer natürlichen Person, die die Ausstellung eines geregelten Zertifikats für eine UID-Einheit beantragt, die keine natürliche Person ist. Der Anwendungsfall 9.3 *(Use Case for Identity Proofing of Legal Person)* ist nach schweizerischem Recht nicht anwendbar, da im ZertES nicht vorgesehen ist, dass eine UID-Einheit direkt die Ausstellung eines geregelten Zertifikats beantragen kann, ohne sich durch eine dazu berechtigte natürliche Person vertreten zu lassen (vgl. Art. 9 Abs. 1 Bst. b ZertES).

Die Anforderungen von Kapitel 8 der ETSI-Spezifikation ergänzen die Anwendungsfälle der Kapitel 9.2 und 9.4 unter Berücksichtigung des bestehenden rechtlichen Kontextes und des angewandten Verfahrens zur Personenidentifikation (in Anwesenheit der Person oder auf Distanz). Insbesondere gelten die Anforderungen betreffend öffentliche Register *(Trusted Registers as Supplementary Evidence)* für das Handelsregister oder das UID-Register, soweit sie die Bestimmungen der Artikel 5 und 6 VZertES vervollständigen. Gleiches gilt für die Anforderungen an die Dokumente und Nachweise (*Documents and Attestations as Supplementary Evidence)* in Bezug auf die Bestätigung der zuständigen Stelle oder die Zustimmung der UID-Einheit (Art. 9 Abs. 2 und 3 ZertES), wenn die spezifischen Attribute oder Vertretungsbefugnisse nicht im Handelsregisterauszug erwähnt sind, oder bezüglich der schriftlichen Vollmacht nach Artikel 6 Absatz 1 VZertES.

Die Anforderungen der Kapitel 5, 6, 7 und 9.1 sind in allen Fällen anwendbar. Es ist zu beachten, dass die auf Distanz erfolgende Überprüfung der Identität einer natürlichen Person durch elektronische Identifizierungsmittel (E-ID; *Use Case* 9.2.4) nicht wie in der bei den betroffenen Kreisen in Konsultation geschickten Vorlage vorgesehen zugelassen werden darf. Denn obwohl es sich dabei um ein Verfahren zur Personenidentifikation auf Distanz gemäss Artikel 7 Absatz 1 VZertES handelt, gehört die E-ID nicht zu den Dokumenten im Sinne von Artikel 5 Absatz 1 VZertES, mit denen Personen, die ein geregeltes Zertifikat beantragen, ihre Identität nachweisen können (vgl. Art. 9 Abs. 4 ZertES). Die Verwendung einer elektronischen Signatur *(Use Case* 9.2.5) ist nur in den Fällen und unter den Bedingungen nach Artikel 7 Absatz 3 VZertES möglich.

Eine Konformitätsbewertung eines Verfahrens zur Personenidentifikation nach dem Standard ETSI TS 119 461 durch eine ausländische Konformitätsbewertungsstelle ist möglich. Die Anerkennung von solchen ausländischen Bewertungen in der Schweiz ist im Hinblick auf die Vereinbarungen im Bereich der Akkreditierung (Multilateral Agreement - MLA) möglich. Die ausländische Konformitätsbewertungsstelle müsste durch die Akkreditierungsstelle ihres Landes akkreditiert sein, um Bewertungen nach dem Standard ETSI TS 119 461 durchführen zu können.

Die Anerkennungsstelle nach ZertES (KPMG) wird sich im Rahmen des Anerkennungsverfahrens auf den ausländischen Konformitätsbewertungsbericht stützen. Zudem wird sie noch prüfen, ob die im Kapitel 2.3.1, a) festgelegten spezifischen Bedingungen und Beschränkungen eingehalten werden.

Die Anerkennungsstelle wird sich auch im Rahmen der Aufsicht auf den Bewertungsbericht beziehen, wenn die Gültigkeit des Berichts noch nicht abgelaufen ist.

Kapitel 2.3.1 Bst. b)

Die ausländischen Identitätskarten, die als Identitätsnachweis für Antragstellerinnen und Antragsteller eines Zertifikats akzeptiert werden, sowie die Mittel zur Überprüfung der Gültigkeit der den CSP vorgelegten Ausweisdokumente werfen regelmässig Fragen auf. Deshalb werden in Kapitel 2.3.1 Erläuterungen zu den offiziellen Quellen hinzugefügt, die bei der Überprüfung solcher Dokumente heranzuziehen sind.

Kapitel 2.3.1 Bst. c)

Gemäss Kapitel 6.3.10 der neuen Version der referenzierten Norm ETSI EN 319 411-2 und der sie spezifizierenden Norm ETSI EN 319 411-1 steht es der CSP frei, den OCSP-Dienst anzubieten oder Listen der für ungültig erklärten Zertifikate (CRL) zu veröffentlichen. Für TLS/SSL-Zertifikate ist jedoch die Erbringung des OCSP-Dienstes erforderlich. Der Verweis auf Kapitel 6.3.10 der Norm ETSI EN 319 411-2 stellt keine Änderung der TAV dar. Diese Entwicklung wird in den vorliegenden Erläuterungen jedoch erwähnt, da sie den Dienstanbieterinnen mehr Flexibilität bieten kann.

Kapitel 2.3.2 Bst. d)

Die neue Fassung der Norm EN 319 412-5 sieht nun auch Erklärungen (*Statements*) für Zertifikate vor, die nach den Vorschriften von Drittländern ausgestellt wurden. Die CSP müssen diese Erklärungen *(Statements)* in die geregelten Zertifikate innerhalb von drei Monaten nach Inkrafttreten einfügen, um darauf hinzuweisen, dass die Zertifikate den Schweizer Vorschriften entsprechen. Bis zum Ablauf dieser Frist bleibt die entsprechende Anforderung nach Kapitel 2.3.2 Buchstabe d) der ersten Ausgabe der technischen und administrativen Vorschriften vom 23. November 2016 (vgl. Kap. 3) anwendbar.

Kapitel 2.3.2 Bst. e) und f)

Es wird präzisiert, wie Vor- und Nachnamen in geregelten Zertifikaten anzugeben sind, da dies in den referenzierten Normen nicht ausführlich genug erläutert wird.

Kapitel 2.3.2 Bst. g)

Da in Kapitel 5.1.4 der Norm ETSI EN 319 412-1 zwei Möglichkeiten für die Aufnahme von Identifikationsnummern für juristische Personen erwähnt werden, wird erläutert, wie die eindeutige Unternehmens-Identifikationsnummer anzugeben ist, die in den geregelten Zertifikaten für UID-Einheiten aufgeführt werden muss. Falls erforderlich, müssen die CSP ihre Praxis innerhalb von drei Monaten nach Inkrafttreten anpassen. Bis zum Ablauf dieser Frist bleibt die im selben Kapitel der referenzierten Norm erwähnte Alternative anwendbar (vgl. Kap. 3).

Kapitel 2.3.2 Bst. h)

Da die Normen X.509 und IETF RFC 5280 unterschiedliche Bezeichnungen für das Bit 1 der Erweiterung keyUsage verwenden, werden neu beide Bezeichnungen aufgeführt.

Kapitel 2.3.2 Bst. j)

Die Verweise wurden angegeben.

Kapitel 2.3.2 Bst. l)

Der Verweis auf das entsprechende Kapitel des Dokuments RFC 5280 wurde korrigiert.

Kapitel 2.3.3 Bst. b)

Da die Normen X.509 und IETF RFC 5280 unterschiedliche Bezeichnungen für das Bit 1 der Erweiterung keyUsage verwenden, werden neu beide Bezeichnungen aufgeführt.

Kapitel 2.3.3 Bst. c)

Die Norm ETSI EN 319 412-5 wurde angepasst, damit die Erklärung, dass es sich um ein qualifiziertes Zertifikat handelt, auch für qualifizierte Zertifikate gilt, die in Nicht-EU-Ländern ausgestellt wurden. Diese Entwicklung wird daher berücksichtigt. Die CSP müssen diese Erklärungen *(Statements)* in die qualifizierten Zertifikate einfügen, die sie innerhalb von drei Monaten nach Inkrafttreten ausstellen. Bis zum Ablauf dieser Frist bleibt die entsprechende Anforderung nach Kapitel 2.3.3 Buchstabe c) der ersten Ausgabe der technischen und administrativen Vorschriften vom 23. November 2016 (vgl. Kap. 3) anwendbar.

Kapitel 2.3.4

Das Kapitel 2.3.4 der ersten Ausgabe der TAV wird zum Kapitel 2.3.5.

Auf Verlangen des Bereichs Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei (vormals Informatiksteuerungsorgan des Bundes, ISB) werden in Kapitel 2.3.4 der TAV neue Anforderungen für die Bereitstellung von geregelten Zertifikaten an Behörden auf Gemeinde-, Kantons- oder Bundesebene eingeführt.

Diese neuen Anforderungen stammen aus dem *Konzept geregeltes Behördenzertifikat / Zusammenarbeit mit dem eGov Signaturvalidator* . Die aktuelle Version dieses Konzepts wird auf der Webseite des BAKOM[3] verfügbar sein. In Kap. 5.2 dieses Konzepts werden u. a. die Quellen genannt, auf die sich die CSP beziehen können, um die Informationen zu überprüfen, die in einem geregelten, einer Behörde ausgestellten Zertifikat enthalten sein müssen.

Die CSP müssen die geregelten Zertifikate von Behörden auf kommunaler, kantonaler oder Bundesebene innerhalb von drei Monaten nach Inkrafttreten dieser neuen Regeln nach ebendiesen ausstellen (vgl. Kap. 3).

[3] https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html

Kapitel 2.3.5 Bst. c)

Dieses Kapitel entspricht dem Kapitel 2.3.4 der ersten Ausgabe der TAV.

Wie in Kapitel 2.3.2 Buchstabe g) wird präzisiert, wie die eindeutige Unternehmens-Identifikationsnummer anzugeben ist. Falls erforderlich, müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten ihre Praxis innerhalb von drei Monaten nach Inkrafttreten anpassen. Bis zum Ablauf dieser Frist bleibt die im selben Kapitel der referenzierten Norm erwähnte Alternative anwendbar (vgl. Kap. 3).

Kapitel 2.3.5 Bst. d)

Der Verweis auf Kapitel 6.5.1 der Norm ETSI EN 319 411-2 wird hinzugefügt, da dieses Anforderungen für die Verwaltung von geregelten Zertifikaten durch die CSP enthält.

Kapitel 3

Wie in den entsprechenden Kapiteln dieses Dokuments dargelegt, sind Umsetzungsfristen vorgesehen, damit die CSP genügend Zeit haben, um ihre operativen Prozesse anzupassen.