Deutsche Telekom Security GmbH
Trust Center Certificate Policy

Öffentlich

Version: 01.00

Gültig ab: 01.03.2021

Status: Freigabe

Letztes Review: 25.02.2021

IMPRESSUM

Tabelle 1 – Impressum

Angaben	Ausprägung
Herausgeber	Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Deutschland
Dateiname	Telekom Security CP DE v00.17 ENTWURF.docx
Gültig ab	01.03.2021
Titel	Trust Center Certificate Policy
Version	01.00
Letztes Review	25.02.2021
Status	Freigabe
Autor	Telekom Security
Inhaltlich geprüft von	Telekom Security
Freigegeben von	--
Beteiligte Organisationseinheit	Telekom Security Trust Center & ID-Solutions
Ansprechpartner	Telekom Security Leiter Trust Center Betrieb
Kurzbeschreibung	Übergreifende Zertifizierungsrichtlinie

ÄNDERUNGSHISTORIE

Tabelle 2 – Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
00.10	29.06.2020	T-Systems	Initialversion basierend auf der Root-CP, Kapitel 1, 2, 5 und 7 überarbeitet
00.11	01.07.2020	Telekom Security	Anpassung Herausgeber
00.12	06.07.2020	Telekom Security	Kapitel 3 und 4 überarbeitet
00.13	06.10.2020	Telekom Security	Einarbeitung BR 1.7.2, EV 1.7.3, Microsoft Incident Reporting, G-Suite, Kapitel 6 überarbeitet
00.14	01.12.2020	Telekom Security	Überarbeitung Kap. 8, Einarbeitung Findings zu Kap 1-7, Einarbeitung BR 1.7.3
00.15	06.12.2020	Telekom Security	Überarbeitung Kap. 9
00.16	07.01.2021	Telekom Security	Einarbeitung Findings Stage 1 Prüfung
00.17	25.01.2021	Telekom Security	QS, Version zur Freigabe
00.90	26.02.2021	Telekom Security	Formelle QS
01.00	01.03.2021	Telekom Security	Freigabe

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS

1 EINLEITUNG

1.1 Überblick

Die Deutsche Telekom Security GmbH (nachfolgend kurz Telekom Security genannt) betreibt in ihrem Trust Center als Trust Service Provider (TSP) verschiedene Stammzertifizierungsstellen (Root Certification Authorities, Root-CAs) sowie untergeordnete Zertifizierungsstellen (Subordinate Certification Authorities, Sub-CAs) für die Ausgabe von Zertifikaten, sowohl für Kunden als auch Mitarbeiter des Konzerns Deutsche Telekom AG.

Bei dem vorliegenden Dokument handelt es sich um die Zertifizierungsrichtlinie (Certificate Policy, CP) des Trust Centers der Telekom Security. Diese CP gilt für alle Zertifikate, die

- von der Telekom Security unterhalb ihrer öffentlichen und qualifizierten Root-CAs,
- von der Telekom Security unterhalb ihrer internen Root-CAs, die sich zu dieser CP bekennen,
- von den Sub-CAs des Deutschen Forschungsnetzes (DFN) unterhalb der öffentlichen Root-CAs der Telekom Security sowie
- von der Telekom Security unterhalb der Root-CAs des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) gemäß den Vorgaben der technischen Richtlinie TR-03145 des BSI [TR3145]

ausgestellt werden.

Das Dokument beschreibt in der Struktur des RFC 3647 die Anforderungen, die von den TSP der Root- und Sub-CAs im Scope dieser CP umgesetzt werden müssen.

Es gilt dabei folgende Semantik:

- Anforderungen, die nicht besonders markiert sind, gelten grundsätzlich übergreifend für alle Zertifikatstypen,
- eingerahmte Anforderungen, die mit der Angabe eines oder mehrerer Zertifikatstypen in eckigen Klammern beginnen (wie z.B. der letzte Absatz dieses Kapitels), gelten nur für die betroffenen Zertifikatstypen. Es werden in diesem Dokument folgende Zertifikatstypen unterschieden:
  - [SSL] kennzeichnet alle TLS-Authentisierungs-Zertifikate, die unterhalb der in den Trusted Root Programmen der Browser-Hersteller integrierten öffentlichen Roots der Telekom Security, gemäß der jeweils aktuellen Version der „CA/Browser-Forum Baseline Requirements“ [BR], veröffentlicht unter http://www.cabforum.org, herausgegeben werden. Diese Kennzeichnung gilt grundsätzlich auch für TLS-Zertifikate die gemäß [EVCP], [OVCP], [DVCP], [IVCP] oder [QCP-w] ausgestellt werden
  - [SMIME] kennzeichnet alle S/MIME-Zertifikate zur E-Mail-Absicherung, die unterhalb der in den Trusted Root Programmen von Microsoft [MSRP], Mozilla [MOZRP], Google [GGLRP] und Apple [APLRP] integrierten öffentlichen Roots der Telekom Security herausgegeben werden.
  - [3145] kennzeichnet alle Zertifikate, die von der Telekom Security gemäß den [TR3145] unterhalb der Root-CAs des BSI ausgestellt werden.
  - [VS-NfD] kennzeichnet alle Zertifikate, die gemäß den [TR3145] ausgestellt werden und darüber hinaus den Anforderungen für VS-NfD (Verschlusssache, nur für den Dienstgebrauch) gemäß der Erweiterung der [TR3145] für VS-NfD [TR3145NfD] genügen.

- [Non-QCP] kennzeichnet übergreifend alle nicht-qualifizierten Zertifikate, die gemäß der ETSI EN 319 411-1 [ETS4111] ausgestellt werden. Im Einzelnen sind das:
  - [LCP] Zertifikate, die gemäß der Lightweight Certificate Policy ausgestellt werden.
  - [NCP] bzw. [NCP+] Zertifikate, die gemäß der Normalized Certificate Policy bzw. der Extended Normalized Certificate Policy ausgestellt werden.
  - [EVCP] Zertifikate, die gemäß der Extended Validation Certificate Policy ausgestellt werden.
  - [OVCP] Zertifikate, die gemäß der Organizational Validation Certificate Policy ausgestellt werden.
  - [DVCP] Zertifikate, die gemäß der Domain Validation Certificate Policy ausgestellt werden.
  - [IVCP] Zertifikate, die gemäß der Individual Validation Certificate Policy ausgestellt werden.
- [QCP] kennzeichnet übergreifend alle qualifizierten Zertifikate, die gemäß der ETSI EN 319 411-2 [ETS4112] ausgestellt werden. Im Einzelnen sind das:
  - [QCP-n] qualifizierte Zertifikate für natürliche Personen
  - [QCP-l] qualifizierte Zertifikate für juristische Personen
  - [QCP-n-qscd] qualifizierte Zertifikate für natürliche Personen mit Nutzung des privaten Schlüssels in einer QSCD
  - [QCP-l-qscd] qualifizierte Zertifikate für juristische Personen mit Nutzung des privaten Schlüssels in einer QSCD
  - [QCP-w] für Webseiten-Authentisierung (TLS-Server)

Die Optionen oder Pflichten zur Umsetzung der Anforderungen werden durch die Schlüsselwörter gemäß RFC 2119 beschrieben:

- MUSS/MÜSSEN kennzeichnen eine unbedingte Verpflichtung.
- DARF/DÜRFEN NICHT kennzeichnen ein unbedingtes Verbot.
- SOLLTE/SOLLTEN kennzeichnen eine grundsätzliche Verpflichtung zur Umsetzung, auf die nur beim Vorliegen guter Gründe verzichtet werden kann.
- SOLLTE/SOLLTEN NICHT kennzeichnen ein grundsätzliches Verbot, es sei denn, dass gute Gründe zur Umsetzung vorliegen.
- DARF/DÜRFEN kennzeichnen eine Option.

Die TSP MÜSSEN die Umsetzung und Einhaltung der Anforderungen dieser CP sowie der referenzierten Dokumente in der jeweils aktuellen Version in ihren Certification Practise Statements (CPS) beschreiben. Im Falle eines Widerspruchs zwischen dieser CP, den CPS der TSP und den referenzierten Dokumenten haben die Regelungen aus den referenzierten Dokumenten Vorrang.

[EVCP] Die TSP MÜSSEN in ihren CPS explizit auf die Einhaltung der jeweils aktuellen Version der [BR] und der [EVCG] inkl. der Angabe des Links zu den Dokumenten (http://www.cabforum.org) sowie der EVCP-Policy gemäß ETSI EN 319 411-1 verweisen.

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument trägt den Namen „Certificate Policy des Trust Centers der Telekom Security“ und wird durch die OID 1.3.6.1.4.1.7879.13.42 gekennzeichnet. Die OID ist wie folgt zusammengesetzt:

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Certificate Policy des Trust Centers der Telekom Security (42)}

Die verbindlichen Angaben zu Version, Gültigkeitsdatum und Status sind auf dem Deckblatt aufgeführt.

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

1.3.1.1 Stammzertifizierungsstellen (Root-CA)

Die Stammzertifizierungsstellen bilden die obersten Hierarchiestufen der PKIn. Sie stellen ausschließlich ihre eigenen Root-CA-Zertifikate sowie die CA-Zertifikate der ihr direkt untergeordneten Zertifizierungsstellen aus. Darüber hinaus stellen Sie ggf. noch CRL- oder OCSP-Signer-Zertifikate für die von ihnen betriebenen Statusdienste aus.

Die Telekom Security betreibt mehrere eigene öffentliche und interne Root-CAs und stellt auch eigene Cross-Zertifikate aus, sie stellt jedoch keine Cross-Zertifikate zu Root- oder Sub-CAs anderer TSP aus.

In diesem Dokument werden folgende Begriffe verwendet:

- In Anlehnung an [ETS4111] wird die Telekom Security mit dem Begriff „Root Trust Service Provider“ (Root-TSP) als Betreiber der Root-CAs bezeichnet.
- Mit dem Begriff „Root-CA“ wird die im Betrieb eingesetzte Technik bezeichnet.

Mit dem Begriff „Root-CA Zertifikat“ wird ein konkretes CA-Zertifikat einer Stammzertifizierungsstelle bezeichnet.

1.3.1.2 (Untergeordnete) Zertifizierungsstellen (Subordinate CA, Sub-CA)

Die Zertifizierungsstellen stellen entweder Endteilnehmerzertifikate oder CA-Zertifikate weiterer untergeordneter Zertifizierungsstellen aus und bilden somit die zweite bis vorletzte Hierarchiestufe der PKIn. Darüber hinaus stellen Sie ggf. noch CRL- oder OCSP-Signer-Zertifikate für die von ihnen betriebenen Statusdienste aus.

Die Telekom Security betreibt mehrere öffentliche und interne Sub-CAs, die allesamt ausschließlich Endteilnehmerzertifikate sowie CRL- oder OCSP-Signer-Zertifikate und keine Zertifikate für weitere untergeordnete Zertifizierungsstellen ausstellen.

Im Scope dieses Dokuments liegen darüber hinaus die Zertifizierungsstellen des DFN-Vereins (Verein zur Förderung eines Deutschen Forschungsnetzes e. V., nachfolgend kurz DFN genannt). Die Telekom Security stellt für den DFN Sub-CA-Zertifikate unterhalb ihrer öffentlichen Root-CA-Zertifikate aus. Diese von der Telekom Security ausgestellten Sub-CA-Zertifikate werden vom DFN zur Ausstellung weiterer untergeordneter Sub-CA-Zertifikate

verwendet, welche dann wiederum die Endteilnehmerzertifikate ausstellen. Die Sub-CAs der beiden Hierarchiestufen stellen darüber hinaus noch bei Bedarf CRL- oder OCSP-Signer-Zertifikate aus.

In diesem Dokument werden folgende Begriffe verwendet:

- Mit dem Begriff „Trust Service Provider“ (TSP) wird die Telekom Security oder der DFN als Betreiber der Sub-CAs bezeichnet.
- Mit dem Begriff „Sub-CA“ wird die im Betrieb eingesetzte Technik bezeichnet.
- Mit dem Begriff „Sub-CA-Zertifikat“ wird ein konkretes CA-Zertifikat eines TSP bezeichnet.

Bei den TSP handelt es sich ausschließlich um juristische Personen, d.h. es fungiert keine natürliche Person als Aussteller von Zertifikaten.

Wo bei der Beschreibung der Anforderungen in diesem Dokument eine Unterscheidung zwischen den TSP Telekom Security und DFN erforderlich ist, werden die Anforderungen in Analogie zur Unterscheidung der Zertifikatstypen (s.o.) durch eine Kennzeichnung in eckigen Klammern gekennzeichnet:

- [TSEC-CA] bezieht sich auf die von der Telekom Security herausgegebenen Zertifikate,
- [DFN-CA] bezieht sich auf die vom DFN herausgegebenen Zertifikate.

1.3.2 Registrierungsstellen (Registration Authorities, RA)

Die Registrierungsstellen übernehmen die Identifizierung und Authentifizierung von Endteilnehmern im Rahmen der Beantragung einer Neuausstellung, Verlängerung oder Sperrung von Zertifikaten. Sie können entweder Bestandteil der TSP sein, oder als externe Registrierungsstelle in dessen Auftrag handeln.

Die in diesem Dokument aufgeführten Anforderungen an die TSP gelten, sofern anwendbar, auch für die externen Registrierungsstellen. Beim Einsatz externer Registrierungsstellen MÜSSEN die TSP in ihrem CPS die Strukturen, die relevanten Prozesse sowie die Rechte und Pflichten der externen Registrierungsstellen beschreiben und mit diesen entsprechende Vereinbarungen abschließen.

[EVCP] Anmerkung: Es werden derzeit keine externen RAs eingesetzt.

1.3.3 Endteilnehmer

Endteilnehmer sind natürliche oder juristische Personen, welche die Endteilnehmerzertifikate beantragen und besitzen und somit auch die Verantwortung für die Schlüssel tragen.

Gegenstand eines Endteilnehmerzertifikats kann der Endteilnehmer als natürliche oder juristische Person selbst oder ein/e vom Endteilnehmer verantwortete Gruppe, Funktion, IT-Prozess oder technisches Gerät sein.

Die TSP MÜSSEN in ihren CPS die im Scope des CPS zu betrachtenden Endteilnehmer sowie die möglichen Gegenstände der Endteilnehmerzertifikate beschreiben

1.3.4 Vertrauende Dritte

Vertrauende Dritte sind Personen oder IT-Prozesse, welche den Zertifikaten vertrauen und

- zur Prüfung digitaler Signaturen,
- zur Prüfung von Authentifizierungen oder
- zur Verschlüsselung

nutzen.

1.3.5 Andere Teilnehmer

Keine Vorgabe.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Die Nutzung der Root-CA-Zertifikate MUSS auf folgende Anwendungsfälle beschränkt werden:

- Signatur von Sub-CA-Zertifikaten,
- Signatur von OCSP- oder CRL-Signer-Zertifikaten,
- Signatur von Sperrlisten.

Die Nutzung der Sub-CA-Zertifikate MUSS auf folgende Anwendungsfälle beschränkt werden:

- Signatur von Sub-CA-Zertifikaten,
- Signatur von Endteilnehmerzertifikaten,
- Signatur von OCSP- oder CRL-Signer-Zertifikaten,
- Signatur von Sperrlisten,
- Signatur von OCSP-Auskünften.

Die Nutzung der Endteilnehmer-Zertifikate MUSS auf die Anwendungsfälle beschränkt werden, die sich aus dem Attribut keyUsage und, sofern gesetzt, der Erweiterung extendedKeyUsage ergeben. Die TSP MÜSSEN in den CPS die zugelassene Verwendung der Sub-CA- und Endteilnehmerzertifikate beschreiben.

1.4.2 Unzulässige Verwendung von Zertifikaten

Zertifikate DÜRFEN NICHT für andere als den in Kap. 1.4.1 aufgeführten Anwendungsfällen verwendet werden.

Insbesondere DÜRFEN Root-CA-Zertifikate NICHT für die Ausstellung von Endteilnehmerzertifikaten verwendet werden.

1.5 Verwaltung des Dokuments

1.5.1 Organisation, die das Dokument verwaltet

Das Dokument wird verwaltet von:

Deutsche Telekom Security GmbH

Trust Center – Root Programm

Untere Industriestraße 20

57250 Netphen, Deutschland

1.5.2 Ansprechpartner

Ansprechpartner für diese CP ist das Root Programm des Trust Centers, welches wie folgt zu erreichen ist:

Telefon: +49 (0) 1805 268 204

Hinweis zu den anfallenden Kosten:

Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute

WWW: www.telesec.de

E-Mail: FMB_Trust_Center_Rootprogram@t-systems.com

1.5.3 Person für die Feststellung der Konformität eines CPS zu dieser CP

Zuständig für die Feststellung der Konformität eines CPS zu dieser CP ist das Root-Programm des Trust Centers, Kontakte siehe Kap. 1.5.2.

1.5.4 Genehmigungsverfahren dieser CP und eines CPS

Diese CP wurde von der Leitung des Trust Centers freigegeben und behält ihre Gültigkeit, solange sie nicht widerrufen oder durch eine neue Version ersetzt wird.

Diese CP MUSS bei Bedarf, z.B. aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, mindestens aber einmal pro Jahr einem Review durch das Root Programm unterzogen werden. Das Root-Programm MUSS daher regelmäßig in angemessenen Abständen die zugrunde liegenden Anforderungen (z.B. die des CABF, ETSI oder des BSI) auf neue Versionen überprüfen. Änderungen an dieser CP sowie das jährliche Review MÜSSEN in der Änderungshistorie dieses Dokuments aufgeführt werden. Dies gilt auch für den Fall, dass beim jährlichen Review keine inhaltlichen Änderungen vorgenommen werden. Jede neue Version MUSS von der Leitung des Trust Centers freigegeben werden, eine neue aufsteigende Versionsnummer erhalten und gemäß den Vorgaben aus Kap. 2.2 veröffentlicht werden. Spätestens mit der Veröffentlichung einer neuen Version MÜSSEN alle betroffenen TSP informiert werden.

Die CPS, welche auf dieser CP basieren, MÜSSEN analog überprüft werden. Die Revisions- und Freigabeprozesse sowie die freigebende Instanz MÜSSEN im jeweiligen CPS beschrieben werden. Darüber hinaus MUSS das Root Programm zur Feststellung der Konformität des überarbeiteten CPS zu dieser CP in den Freigabeprozess involviert werden. Nach Freigabe einer neuen Version eines CPS MÜSSEN alle betroffenen Mitarbeiter der TSP sowie, falls vorhanden, der externen Registrierungsstellen informiert werden.

Die TSP MÜSSEN mit dem Root-TSP Vereinbarungen zur Einhaltung der jeweils aktuellen Version dieser CP treffen.

1.6 Definitionen und Abkürzungen

1.6.1 Glossar

Tabelle 3 - Glossar

Begriff	Erläuterung
Antrag auf ein Zertifikat mit erhöhtem Risiko	Ein Antrag, für den die CA eine Zusatzprüfung im Hinblick auf interne Kriterien und Datenbanken vorsieht, die von der CA geführt werden. Dies kann Namen betreffen, die in Bezug auf Phishing oder eine andere betrügerische Nutzung einem höheren Risiko ausgesetzt sind, Namen, die in zuvor abgelehnten Zertifikatsanträgen oder widerrufenen (gesperrten) Zertifikaten enthalten sind, Namen, die auf der MillerSmiles-Phishing-Liste oder auf der Safe-Browsing-Liste von Google stehen bzw. Namen, die die CA anhand ihrer eigenen Risikominderungskriterien identifiziert.
Antragsteller	Die natürliche oder juristische Person, die ein Zertifikat (oder dessen Erneuerung) beantragt. Ist das Zertifikat einmal ausgestellt, wird der Antragsteller als Zertifikatnehmer bezeichnet. Bei für Geräte ausgestellten Zertifikaten ist der Antragsteller die Organisation, die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt, auch wenn das Gerät den eigentlichen Antrag auf das Zertifikat sendet.
Anwendungssoftwareanbieter	Ein Anbieter von Internetbrowser-Software oder anderer Anwendungssoftware der vertrauenden Seite, die Zertifikate anzeigt oder verwendet und Stammzertifikate (Root) beinhaltet.
Ausstellende Zertifizierungsstelle (CA)	Die Zertifizierungsstelle (CA), die ein bestimmtes Zertifikat ausgestellt hat. Dabei kann es sich um eine Stammzertifizierungsstelle (Root-CA) oder eine untergeordnete Zertifizierungsstelle (Sub-CA) handeln.
Authentifizierung	Prüfung einer Identität an Hand behaupteter Merkmale.
Authority Revocation List (ARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (außer Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
Beauftragte Drittpartei	Eine natürliche oder juristische Person, die nicht identisch mit der Zertifizierungsstelle (CA) ist, jedoch von dieser bevollmächtigt ist, den Zertifikatsverwaltungsprozess zu unterstützen, indem sie Aufgaben zur Erfüllung einer oder mehrerer Anforderungen erfüllt. Dies kann z.B. eine externe Registrierungsstelle oder auch eine interne enterprise Registrierungsstelle sein.
Berechtigungsdokument	Die Dokumentation, die die Berechtigung eines Antragstellers belegt, ein oder mehrere Zertifikat(e) für eine bestimmte natürliche Person, Personen- und Funktionsgruppen, juristische Personen oder Gerät zu beantragen. Es kann sich auch um ein Dokument der Zertifizierungsstelle über eine Kommunikation mit der betreffenden Person oder Organisation handeln.

Begriff	Erläuterung
Bezugsvertrag (Subscriber Agreement)	Eine Vereinbarung zwischen der Zertifizierungsstelle (CA) und dem Antragsteller/Zertifikatnehmer, in der die Rechte und Verpflichtungen der Parteien festlegt werden.
Bulk	Funktion einer CA mit der der Sub-Registrator Soft-PSE per Massengenerierung erzeugen kann.
Certificate Management Protocol (CMP)	Das Zertifikat-Verwaltungsprotokoll, ist ein von der IETF entwickeltes Protokoll, zur Verwaltung von X.509-Zertifikaten innerhalb einer Public-Key-Infrastruktur (PKI).
Certificate Policy (CP)	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Signing Request (CSR) [TC]	Von einem Gerät (z.B. Server) elektronisch erstellt und mit dem privaten Schlüssel signierter Zertifikatsantrag, der in kodierter Form den öffentlichen Schlüssel und die Zertifikatsdaten enthält. Die Syntax wird durch den Standard PKCS#11 beschrieben.
Certificate Revocation List (CRL)	Siehe Sperrliste
Certification Authority (CA)	Siehe Zertifizierungsstelle.
Certification Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
Chipkarte	Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.
Dezentrales Registrierungsmodell	Der Benutzer stellt über die Benutzer-Webseite oder per Mail-Request oder das Gerät stellt über seine SCEP-Schnittstelle den Zertifikatsantrag, den der Sub-Registrator bearbeitet (Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage)).
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Domain-Berechtigungs-dokument	Die Dokumentation, die von der Domain-Namen-Registrierungsstelle (Domain Name Registrar), einem registrierten Domain-Inhaber (Domain Name Registrant) oder der Person bzw. Organisation bereitgestellt wird, die in WHOIS als registrierter Domain-Inhaber aufgeführt ist (einschließlich aller privaten, anonymen oder Proxy-Registrierungsservices), und die Berechtigung eines Antragstellers belegt, ein Zertifikat für einen bestimmten Domain-Namensraum zu beantragen. Es kann sich auch um ein Dokument der Zertifizierungsstelle über eine Kommunikation mit der betreffenden Person oder Organisation handeln.
Domain-Name	Die Bezeichnung, die einem Knoten im Domain Name System (DNS) zugeordnet ist.
Dual-Key-Zertifikat	Variante, bei der für Verschlüsselung und Signatur getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt zwei korrespondierende Zertifikate.
Endteilnehmer	Siehe auch Zertifikatnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Endteilnehmer-Zertifikat	Ein Zertifikat, welches nicht die Basiseinschränkung (basic constraints) „Zertifizierungsstelle“ verwendet, daher selber keine Zertifikate signieren kann.
Erklärung zum Zertifizierungsbetrieb (CPS)	Eines von mehreren Dokumenten, die allgemeine und spezifische Rahmenbedingungen vorgibt. Das beninhaltet insbesondere eine Beschreibung der Verfahrensweise, wie die Zertifizierungsstelle (CA) Zertifikate ausstellt, verwaltet, sperrt und erneuert.

Begriff	Erläuterung
Erlaubte Internet-Domänen	Ein Domänenname, der aus der Top-Level-Domain und weiteren Sub-Domains besteht, und nach erfolgreicher Prüfung durch die interne Registrierungsstelle als „erlaubte Internet-Domäne“ in die PKI-Konfiguration des Mandanten (Master-Domäne) aufgenommen wird.
ETSI-Zertifizierung	Überprüfung und Bestätigung für Zertifizierungsstellen durch einen unabhängigen Gutachter, das die PKI nach den ETSI-Kriterien „ETSI TS 102 042“ betrieben werden. Ziel der ETSI-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken.
Externe Registrierungsstelle	Ein Mitarbeiter (Beschäftigter) oder Vertreter eines der Zertifizierungsstelle (CA) nicht verbundenen Unternehmens (non Affiliate), der die Ausstellung von Zertifikaten für Dritte genehmigt. Diese Rollen (Trusted Roles) werden z.B. vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen.
Gerät	Komponente wie beispielsweise Router, Server, Gateway, Applikation, die zertifikatsbasierende Funktionen unterstützen, selbst aber nicht oder nur begrenzt selbst Zertifikate beantragen können. Häufig werden Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.
Geräte-Zertifikat	X.509 V3 Zertifikat, welches im commonName-Feld (CN) des distinguishedName des Zertifikatnehmers (Subject) und/oder in mindestens einer subjectAltName-Erweiterung entweder einen Hostname, IP-Adresse oder Mail-Adresse enthält.
Gültiges Zertifikat	Ein Zertifikat, das dem in RFC 5280 dargelegten Validierungsverfahren besteht.
Gültigkeitsdauer	Der Zeitraum vom Ausstellungsdatum (not before) des Zertifikats bis zum Ablaufdatum (not after).
Hardware Security Modul (HSM)	Hardware zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hashwert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
Identifizierung	Der Prozess der Mitteilung der Identität eines Subjekts oder Objekts (z.B. Benutzer, Gerät) an ein System. Die Identifizierung ist ein Bestandteil der Validierung.
Interface	Schnittstelle als Teil eines Systems, dass zur Kommunikation (Ein- und Ausgabe) dient.
Interne Registrierungsstelle	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer der CA, der die vom PKI-Mandanten benannten „Domain“ prüft und diesem zur Zertifikatsbeantragung zur Verfügung stellt. Diese Rolle (Trusted Role) wird z.B. vom Trust-Center-Operator der T-Systems wahrgenommen.
Interner Server-Name	Ein Server-Name (der einen nicht registrierten Domain-Namen enthalten kann oder nicht), der nicht mit dem öffentlichen Domain Name System (DNS) aufgelöst werden kann.
Issuer-Distinguished-Name (Issuer-DN)	Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Issuer-DN bezeichnet eindeutig die Zertifizierungsstelle.
Juristische Person	Eine Gesellschaft, ein Konzern, eine Partnerschaft, Einzelfirma, Treuhandgesellschaft, Regierungsbehörde oder eine andere klagebefugte Rechtspersönlichkeit innerhalb des Rechtssystems eines Landes.
Key-Back-Up	Mechanismus zur Schlüsselsicherung. Um beispielsweise verschlüsselte E-Mails bei Schlüsselverlust wieder herstellen zu können empfiehlt sich das Key-Back-Up des Schlüsselmaterials des Verschlüsselungsschlüssels. Key-Back-Up wird auch als Synonym für Key-Archiving benutzt.

Begriff	Erläuterung
Key-Recovery	Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert.
Kompromittierung	Ein privater Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
Land	Entweder ein Mitglied der Vereinten Nationen oder eine geographische Region, die von mindestens zwei Mitgliedsländern der UNO als souveräner Staat anerkannt wird.
Latenzzeit	Zeitraum zwischen einer Aktion und dem Eintreten einer verzögerten Reaktion (Verzögerungszeitraum). Bei der Latenzzeit erfolgt die Aktion im Verborgenen und wird erst durch die Reaktion festgestellt.
LDAP-Server	Server, der Informationen speichert, die über LDAP abrufbar sind.
Lightweight Directory Access Protocol (LDAP)	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Mail-Security	Security-Funktionen wie Digitale Signatur und Verschlüsselung, die Standard-Mail-Anwendungen unterstützen.
Managementsystem für Informationssicherheit (ISMS)	Das „Managementsystem für Informationssicherheit“ (ISMS) ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Der Begriff wird im Standard ISO/IEC 27002 verwendet, ISO/IEC 27001 definiert ein ISMS.
Mandant	Der Mandant stellt eine eigene logische abgeschlossene Einheit mit eigener Rechte-, Organisations- und Datenverwaltung innerhalb des Systems dar. Der Mandant strukturiert somit die Nutzung des Systems. Als Mandant wird z.B. die Master-Domäne bezeichnet. Innerhalb der Master-Domäne bestehen weitere Untergliederungen in Form von Zuständigkeitsbereichen (auch als Sub-Domänen bezeichnet).
Mandantenfähigkeit	Als Mandantenfähigkeit bezeichnet man in der Informationstechnik (IT) die Eigenschaft einer Software bzw. Server, auf einer Installation mehrere logisch voneinander vollständig getrennte Mandanten abzubilden. Die jeweiligen Mandanten, etwa unterschiedliche rechtliche Einheiten oder Firmen, haben dabei keinerlei gegenseitigen Einblick in die Daten, Benutzerverwaltung oder Ähnliches der anderen Parteien/Mandanten.
Master-Domäne	Eigenständiger, mit einem eindeutigen Namen festgelegter Verwaltungsbereich, der ausschließlich für eine beauftragte Drittpartei (Delegated Third Party) eingerichtet wird. Innerhalb des Mandanten kann die beauftragte Drittpartei Zertifikate genehmigen und verwalten. Der Mandant wird mit dem Master-Registrator-Zertifikat verwaltet. Weitere Informationen finden Sie auch unter: Mandant.
Master-Registrator	Natürliche Person (Trusted Role) der die Master-Domäne verwaltet.
Nicht registrierter Domain-Name	Ein Domain-Name, der kein registrierter Domain-Name ist.
Nutzungsbedingungen (Terms of Use)	Bestimmungen bezüglich der Verwahrung und zugelassenen Verwendungszwecke eines ausgestellten Zertifikats in Übereinstimmung mit den gegebenen Anforderungen, wenn der Antragsteller/Zertifikatnehmer beispielsweise ein verbundenes Unternehmen der Zertifizierungsstelle (CA) ist.

Begriff	Erläuterung
Object Identifier (OID)	Ein eindeutiger alphanumerischer oder numerischer Bezeichner, der unter dem jeweiligen Standard für ein bestimmtes Objekt oder eine Objektklasse der Internationalen Organisation für Normung (ISO) registriert ist.
Online Certificate Status Protocol (OCSP) [BR]	Ein Protokoll zur Online-Zertifikatsvalidierung, mit dessen Hilfe die Anwendungssoftware der vertrauenden Seite den Status eines identifizierten Zertifikats bestimmen kann. Siehe auch OCSP-Responder.
OCSP-Responder	Ein Online-Server, der der Zertifizierungsstelle (CA) untersteht und mit deren zentrale Datenablage (Repository) zur Bearbeitung von Zertifikatsstatusanfragen verbunden ist. Siehe auch Online Certificate Status Protocol (OCSP).
Öffentlicher Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Inhaber des entsprechenden privaten Schlüssels offen gelegt werden darf und der von der vertrauenden Seite verwendet wird, um digitale Signaturen zu verifizieren, die mit dem privaten Schlüssel des Inhabers erstellt wurden, und/oder um Mitteilungen zu verschlüsseln, die nur mit dem zugehörigen privaten Schlüssel des Inhabers entschlüsselt werden können.
Öffentliches Geräte-Zertifikat	Ein Geräte-Zertifikat, welches in der CA-Hierarchie von einer Sub-CA unterhalb eines öffentlichen Root-Zertifikates ausgestellt ist.
Personal Identification Number (PIN)	Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.
Personal Security Environment (PSE)	In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Privater Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Schlüsselpaarinhaber geheim gehalten und verwendet wird, um digitale Signaturen zu erstellen und/oder elektronische Daten und Dateien zu entschlüsseln, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
Public Key Service (PKS)	Service des T-Systems Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Policy	Richtlinien bzw. Erklärung, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
Personal Security Environment (PSE)	In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Public Key Infrastruktur	Hardware, Software, Personen, Verfahren, Regeln, Richtlinien und Verpflichtungen, mit denen die vertrauenswürdige Generierung, Ausstellung, Verwaltung und Verwendung von Zertifikaten und Schlüsseln auf der Basis der Public-Key-Kryptographie ermöglicht wird.
Qualifizierter Auditor	Eine natürliche oder juristische Person, welche die an sie gestellten Anforderungen erfüllt.
Registrierter Domain-Name	Ein Domain-Name, der bei einer Domain-Namen-Registrierungsstelle (Registrar) registriert wurde.
Registrierungsstelle (RA)	Eine juristische Person, die für die Identifizierung und Authentifizierung von Zertifikatssubjekten zuständig ist. Sie ist jedoch keine CA und signiert somit keine Zertifikate und stellt diese nicht aus. Eine RA kann bei der Beantragung oder beim Widerruf eines Zertifikats oder in beiden Fällen Unterstützung leisten. Wenn „RA“ als Adjektiv verwendet wird, um eine Rolle oder eine Funktion zu beschreiben, ist nicht zwangsläufig von einer eigenständigen Stelle die Rede. Sie kann jedoch Teil der CA sein.
Registrierungsmodell	Es wird zwischen Zentralem Registrierungsmodell (siehe dort) und Dezentralem Registrierungsmodell (siehe dort) unterschieden.

Begriff	Erläuterung
Registrierungs-stelle eines Unternehmens (Enterprise RA)	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der nicht der Zertifizierungsstelle (CA) angegliedert ist (non Affiliate), der die Ausstellung von Zertifikaten für diese Organisation genehmigt. Diese Rollen (Trusted Roles) können z.B. vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen werden.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, dass nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
Root-CA	Siehe Wurzelzertifizierungsstelle.
Schlüssel-kompromittierung	Ein privater Schlüssel (Private Key) gilt als kompromittiert, wenn sein Wert einer nicht autorisierten Person offen gelegt wurde, eine nicht autorisierten Person Zugriff auf ihn hatte oder es eine praktische Methode gibt, mit der eine nicht autorisierte Person seinen Wert ausfindig machen kann.
Schlüsselpaar	Der private Schlüssel und der dazugehörige öffentliche Schlüssel.
Schlüsselverantwortlicher	Eine durch die beauftragte Drittpartei (Delegated Third Party) autorisiert natürliche Person, die verantwortlich ist für die ordnungsgemäße Verwendung (Verteilung, Nutzung und ggf. Sperrung) des Schlüsselpaars und Zertifikat, dass für eine Personen- und Funktionsgruppe, juristische Person oder Gerät ausgestellt wurde.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Erweiterung des E-Mail-Formats MIME, die Zusätze für kryptografische Dienste beschreibt, welche Authentizität, Integrität und Vertraulichkeit von Nachrichten sicherstellen.
Secure Socket Layer (SSL)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet, inzwischen durch das neuere Verfahren TLS abgelöst. Kann ihn vielen Fällen statt dem komplexeren IPSec verwendet werden.
Service Desk	Das Service Desk ist eine organisatorische Einheit innerhalb eines Unternehmens, das für den Mandanten bzw. beauftragte Drittpartei (Delegated Third Party) als zentrale Anlaufstelle für alle Service- und Supportanfragen dient und diese innerhalb des Unternehmens entsprechend den vereinbarten Geschäftsprozessen vermittelt.
Simple Certificate Enrollment Protocol (SCEP)	Simple Certificate Enrollment Protocol. Protokoll zur Beauftragung und zum Laden von Zertifikaten in IPSec Devices.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP stellt einen einfachen Mechanismus zum Austausch von strukturierter Information zwischen Anwendungen in einer dezentralisierten, verteilten Umgebung zur Verfügung.
Single-Key-Zertifikat	Variante, bei der für Verschlüsselung und Signatur das gleiche Schlüsselpaar verwendet wird. D. h. ein Benutzer besitzt ein Zertifikat.
Software-PSE (Soft-PSE)	Eine verschlüsselte Datei zur Speicherung des Zertifikats und den zugehörigen privaten und öffentlichen Schlüssel.
Smartcard	Spezielle Plastikkarte mit integriertem Computerchip, die auch für kryptografische Anwendungen eingesetzt werden kann.
Sperrberechtigte(r)	Person, die von einem Zertifikatnehmer oder Schlüsselverantwortlichen autorisiert ist, ein Zertifikat für eine Personen- und Funktionsgruppe, juristische Person oder Gerät sperren zu dürfen. Die Autorisierung erfolgt über das Zertifikatssperrpasswort.
Sperrinstanz	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der Zertifikatssperrungen durchführt.
Stammzertifizierungsstelle (Root-CA)	Die oberste Zertifizierungsstelle, deren Stammzertifikat von Anwendungssoftwareanbietern verteilt wird und die untergeordnete CA-Zertifikate (Sub-Zertifikate) ausstellt.
Subject Alternative Name	Zusätzliche Felder in einem Zertifikat. Die Felder können zusätzliche Namen des Zertifikatsnehmers enthalten und ist eine Standarderweiterung des X509 Standards.
Subject-Distinguished-Name (Subject-DN)	Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Subject-DN bezeichnet eindeutig die Person oder Gerät.

Begriff	Erläuterung
Subjekt	Die natürliche Person, das Gerät, System, die Einheit oder juristische Person, die in einem Zertifikat als Subjekt benannt wird. Das Subjekt ist entweder der Zertifikatnehmer oder ein Gerät, das der Kontrolle des Zertifikatnehmers untersteht oder von diesem betrieben wird.
Subjektidentitätsdaten	Daten, die das Zertifikatssubjekt identifizieren. Subjektidentitätsdaten beinhalten keinen Domain-Namen, der in der Erweiterung subjectAltName oder im Feld Subject commonName aufgeführt ist.
Sub-Registrator	Natürliche Person (Trusted Role) der den Zuständigkeitsbereich verwaltet.
Suspension	Im Zusammenhang von PKI ist unter Suspendierung die vorläufige bzw. temporäre Sperrung zu verstehen. Das Zertifikat erscheint zunächst in der Zertifikatssperrliste kann aber durch den Sub-Registrator wieder aktiv geschaltet werden.
Transport-Layer Security (TLS)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet.
Triple-Key-Zertifikat	Variante, bei der für Verschlüsselung, Signatur und Microsoft Smartcard-LogOn getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt drei entsprechende Zertifikate.
T-Systems Advisory Board	Gremium innerhalb der T-Systems das über PKI-Funktionalitäten entscheidet.
Untergeordnete Zertifizierungsstelle (Sub-CA)	Eine Zertifizierungsstelle, deren Zertifikat von der Stammzertifizierungsstelle (Root-CA) oder einer anderen untergeordneten Zertifizierungsstelle (CA) signiert wird.
Validierung	Ein Nachweis der Reproduzierbarkeit eines Ergebnisses aus einer beschriebenen Vorgehensweise unter definierten Bedingungen. Je exakter eine Vorgehensweise beschrieben ist und je weniger unbekannte Einflussfaktoren bestehen, desto sicherer ist es, übereinstimmende Resultate zu erzeugen. Für eine Validierung benötigt man die Beschreibung des Zieles und des Weges. Valide bedeutet in diesem Zusammenhang, dass der Weg wiederholbar zum Ziel führt. Im Kontext einer PKI besteht ein Validierungsprozess an folgenden Stellen: Mitteilung und Prüfung einer Identität (z.B. natürliche Person, Gerät) gegenüber dem Zertifikatsantrag. Algorithmus zur Überprüfung eines Zertifikats auf Gültigkeitsdauer (Gültigkeitszeitraum), ausstellende Zertifizierungsstellen und Zertifikatsstatus (gültig, gesperrt).
Validierungsspezialist	Jemand, der die Datenüberprüfungsaufgaben gemäß den jeweiligen Anforderungen wahrnimmt. Im Kontext des Trust-Centers sind dies die Rolleninhaber: Trust-Center-Operator, Master-Registrator, Sub-Registrator
Verbundenes Unternehmen (Affiliate)	Beispielsweise ein Unternehmen, eine Partnerschaft, ein Joint Venture, Körperschaft, (Kapital) Gesellschaft, Verband, Stiftung oder eine andere Organisation (juristische Person), welche eine andere Organisation (juristische Person), Einrichtung, Abteilung, Gebietskörperschaft oder eine Einheit, die einer Regierungsbehörde direkt unterstellt ist, beaufsichtigt, von dieser beaufsichtigt wird oder mit dieser einer gemeinsamen Kontrolle untersteht.
Vertrauende Dritte (Relying Parties)	Eine natürliche oder juristische Person, die sich auf ein gültiges Zertifikat verlässt. Ein Anbieter von Anwendungssoftware gilt nicht als vertrauender Dritter, wenn die von diesem Anbieter vertriebene Software lediglich Informationen zu einem Zertifikat anzeigt.
Vertrauenswürdiges Zertifikat	Ein Zertifikat, dem aufgrund der Tatsache vertraut wird, dass sein entsprechendes Stammzertifikat als Vertrauensanker in weit verbreiteter Anwendungssoftware verteilt ist

Begriff	Erläuterung
Vertreter des Antragstellers	Falls abweichend vom Antragsteller, eine natürliche Person oder Kostenträger, ein Beschäftigter des Antragstellers oder ein Handlungsbevollmächtigter ist, der die ausdrückliche Befugnis besitzt, den Antragsteller zu vertreten: (i) die im Namen des Antragstellers einen Antrag auf ein Zertifikat unterzeichnet, einreicht oder genehmigt, und/oder (ii) die im Namen des Antragstellers eine Bezugsvertrag (Subscriber Agreement) unterzeichnet und einreicht, und/oder (iii) die im Namen des Antragstellers die Nutzungsbestimmungen des Zertifikats anerkennt und ihnen zustimmt, wenn der Antragsteller eine verbundene Unternehmen (Affiliate) der Zertifizierungsstelle (CA) ist.
Verzeichnisdienst	Datenspeicher zum Abruf von Zertifikaten und Zertifikats-Validierungsinformationen (Sperrlisten).
Vollmacht	Unter einer Vollmacht versteht man die durch ein Rechtsgeschäft begründete Vertretungsmacht. Die Vollmacht entsteht durch einseitige empfangsbedürftige Willenserklärung des Vollmachtgebers gegenüber dem Vollmachtnehmer.
Voll qualifizierter Domain-Name (FQDN)	Korrekter und vollständiger Domain-Name, d.h. Verkettung aller Labels eines Pfades im Domain-Namensraum (weitere Informationen siehe RFC 2181).
WHOIS	Informationen die (a) direkt von dem Domain-Namen Registrator oder dem Registrierungsstellenmitarbeiter mittels RFC 3912 Protokoll abgefragt wurden, (b) die anhand des Registry Data Access Protokolls (RFC 7482) ermittelt wurden oder (3) die über eine HTTPS Webseite ermittelt wurden.
Wildcard-Zertifikat	Ein Zertifikat, das ein Sternchen (*) in der äußersten linken Position eines in dem Zertifikat enthaltenen voll qualifizierten Domain-Namens (Fully-Qualified Domain Names) des Subjekts aufweist.
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zentrale Datenablage (Repository)	Eine Online-Datenbank, die öffentliche PKI-Dokumente (z.B. Zertifizierungsrichtlinie, Erklärung zum Zertifizierungsbetrieb, CA-Zertifikate) sowie Zertifikatsstatusinformationen, entweder in Form einer CRL- oder OCSP-Antwort, enthält.
Zentrales Registrierungsmodell	Nach erfolgreicher Registrierung beantragt der Sub-Registrator über die Sub-RA-Webseite das Zertifikat (per Webformular oder Bulk) und erhält dieses bzw. das Schlüsselmaterial für den Endteilnehmer (außer Registrator-Zertifikat) direkt ausgestellt.
Zertifikat	Ein elektronisches Dokument, das eine digitale Signatur verwendet, um einen öffentlichen Schlüssel an eine Identität (z.B. Person, Gerät) zu binden.
Zertifikat einer Stammzertifizierungs-stelle (Root-Zertifikat)	Das selbstsignierte Zertifikat, das von der Stammzertifizierungsstelle (Root-CA) zur Eigenidentifizierung ausgestellt wurde. Ferner soll dieses Zertifikat auch bei der Prüfung (Validierung) ausgestellten Sub-Zertifikate unterstützen.
Zertifikatnehmer	Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die rechtlich durch einen Bezugsvertrag oder Nutzungsbedingungen gebunden ist.
Zertifikatsantrag	Ein in elektronischer oder schriftlicher Form erstellter Antrag, der Daten zu einem Antragsteller enthält.
Zertifikatsdaten	Zertifikatsanträge und damit verbundene Daten (vom Antragsteller oder anderweitig eingeholt), die sich im Besitz der Zertifizierungsstelle (CA) befinden, die der Kontrolle durch die CA unterliegen oder auf die die CA Zugriff hat.
Zertifikatsproblem-bericht	Beschwerde wegen des Verdachts der Gefährdung des Schlüssels, des Zertifikatsmissbrauchs oder hinsichtlich anderer Arten von Betrug, Gefährdung, Missbrauch oder eines Fehlverhaltens im Zusammenhang mit Zertifikaten.

Begriff	Erläuterung
Zertifikatssperrliste (CRL)	Eine regelmäßig aktualisierte, mit Zeitstempel versehene Liste gesperrter (widerrufener) Zertifikate, die von der ausstellenden Zertifizierungsstelle (CA) generiert und digital signiert wird. Die Authority Revocation List (ARL) ist ein Spezialfall der Zertifikatssperrliste (CRL), da sie nur Sub-CA-Zertifikate enthält.
Zertifikatsverwaltungsprozess	Prozesse, Praktiken und Verfahren im Zusammenhang mit der Verwendung von Schlüsseln, Software und Hardware, mit deren Hilfe die Zertifizierungsstelle (CA) Zertifikatsdaten prüft, Zertifikate ausstellt, eine zentrale Datenablage (Repository) unterhält und Zertifikate widerruft/sperrt.
Zertifizierungsrichtlinie (CP)	Ein Regelwerk, das die Verwendungsmöglichkeit eines genannten Zertifikats auf eine bestimmte Gemeinschaft (PKI-Beteiligte) und/oder eine PKI-Implementierung mit gängigen Sicherheitsanforderungen, vorgibt.
Zertifizierungsstelle (CA)	Eine Organisation, die für die Generierung, Ausstellung, die Sperrung und die Verwaltung von Zertifikaten zuständig ist. Die Bezeichnung bezieht sich sowohl auf Stammzertifizierungsstellen (Root-CA) als auch auf untergeordnete Zertifizierungsstellen (Sub-CA).
Zuständigkeitsbereich	Hierarchisch untergeordneter Teilbereich der Master-Domäne, der von einem Sub-Registrator verwaltet wird.
Zuverlässige öffentliche Datenquelle	Ein Authentifizierungsdokument oder eine Datenquelle (z.B. Identitätsdatenbank, Handelsregister), anhand der Subjektidentitätsdaten überprüft werden und die im Allgemeinen von kommerziellen Unternehmen und Behörde (öffentliche Verwaltung) als zuverlässig anerkannt wird und die von einer dritten Partei für einen anderen Zweck als der Zertifikatsausstellung durch den Antragsteller erstellt wurde.

1.6.2 Abkürzungsverzeichnis

Tabelle 4 - Abkürzungsverzeichnis

Überschrift	Definition
ARL	Authority Revocation List, siehe auch CARL
BR	Baseline Requirements
DK	Dual Key
CA	Certification Authority
CARL	Certification Authority Revocation List, siehe auch ARL
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
EDV	Elektronische Datenverarbeitung
eIDAS	electronic Identification and Signature
ERP	Enterprise-Resource-Planning
ETSI	European Telecommunications Standards Institute (deutsch: Europäisches Institut für Telekommunikationsnormen)
FQDN	Fully Qualified Domain Name
GRP	Kennzeichner für Gruppen, Funktions-, Rollenzertifikat
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
IPSec	Internet Protocol Security

Überschrift	Definition
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)
ISO	International Organization for Standardization
IV	Individual Validation
LB	Leistungsbeschreibung
LDAP	Lightweight Directory Access Protocol
NCP	"Normalized" Certificate Policy
NIC	Network Information Center
n.v.	nicht vorhanden
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
OV	Organizational Validated
OVCP	Organizational Validation" Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudonym
PSE	Personal Security Environment
PTC	Publicly-trusted certificate
RA	Registration Authority
RFC	Requests for Comments
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key
SLA	Service Level Agreement
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SigG	Signaturgesetz
SigV	Signaturverordnung
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TK	Triple Key
TSP	Trust Service Provider
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language

1.6.3 Referenzen

Tabelle 5 - Referenzen

Kürzel	Referenz
[BDSG]	Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66.
[CAB-BR]	Zum jeweiligen Zeitpunkt gültige Version des vom CA/Browser-Forum unter http://www.cabforum.org/documents.html veröffentlichten Dokuments „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“
[EU-RL]	Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 1999/93/EG, EU, 1999
[Moz-2-7]	Mozilla Root Store Policy, Version 2.7, Stand 01.01.2020, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy

[PKCS]	RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“, http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
[RFC6962]	Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013.
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften, Bundesgesetzblatt I 2001, S. 876
[SigV]	Signaturgesetzverordnung, „Verordnung zur elektronischen Signatur“, BGBl. I S. 3074, 21.November 2001
[TSYSROOTSIGN]	Leistungsbeschreibung T-Systems Root Signing
[X.509]	Information technology - Open Systems Interconnection - The Directory:authentication framework, Version 3, ITU, 1997

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

Die TSP MÜSSEN in ihren CPS beschreiben, wer welche Verzeichnisse mit Informationen zu den von ihnen ausgestellten Zertifikaten betreibt.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Die jeweils gültige Version dieses Dokuments sowie die relevanten abgelösten Versionen werden auf den Webseiten des Trust Centers der Telekom Security unter folgender Adresse veröffentlicht: https://www.telesec.de/de/service/downloads/pki-repository/

Die TSP MÜSSEN mindestens

- die Nutzungsbedingungen in einer allgemein verständlichen Sprache,
- die CPS in der Struktur gemäß RFC 3647,
- die Root-, Cross- und Sub-CA-Zertifikate sowie
- die Statusinformationen gemäß Kap. 4.9 und 4.10 zu allen von ihnen ausgestellten und noch nicht abgelaufenen Zertifikaten

über geeignete Online-Services rund um die Uhr veröffentlichen. Die relevanten Nutzungsbedingungen und CPS MÜSSEN dabei den Zertifikaten leicht erkennbar zugordnet werden können.

Die TSP MÜSSEN die vollständigen CA-Hierarchien, d.h. alle Root- und Sub-CA-Zertifikate, die im Scope des CPS liegen, in ihren CPS aufführen.

Darüber hinaus DÜRFEN die TSP mit Zustimmung des Endteilnehmers die Endteilnehmerzertifikate veröffentlichen.

[SSL] Die TSP, welche technisch nicht beschränkte Sub-CAs betreiben, MÜSSEN ihre CPS und die Audit-Bescheinigungen (auch) in englischer Sprache veröffentlichen. Die in die englische Sprache übersetzten CPS MÜSSEN dabei die gleiche Versionsnummer haben, wie die originalen CPS in deutscher Sprache. Die übersetzte Version DARF NICHT wesentlich von der originalen Version abweichen, sie muss aber nicht maßgeblich in allen Streitfällen sein.

Die TSP SOLLEN alle ausgestellten Zertifikate, inkl. mindestens aller Sub-CA-Zertifikate und ggf. der Root-CA (optional) aus dessen Kette, in mindestens einem „Certificate Transparency Log“ (CTLog) veröffentlichen. Darüber hinaus DÜRFEN die TSP auch „Pre-Zertifikate“ (siehe Kap. 4.3.1) in einem oder mehreren CTLog veröffentlichen.

[SSL] [SMIME] Der Root-TSP MUSS die erforderlichen Informationen zu den Root- und Sub-CA-Zertifikaten in der „Common CA Database“ (CCADB) gemäß der CCADB-Policy (siehe https://www.ccadb.org) veröffentlichen und aktuell halten, siehe dazu auch Kap. 4.9.3 bzgl. gesperrter Sub-CA-Zertifikate.

Die TSP MÜSSEN ihre CPS über ihre eigene offizielle Webseite veröffentlichen.

[QCP] Die TSP MÜSSEN ergänzend zur CPS auch ein „PKI Disclosure Statements“ (PDS) in der Struktur gemäß des Anhang A der [ETS4111] veröffentlichen.

[3145] Die TSP MÜSSEN sicherstellen, dass neue Sub-CA-Zertifikate oder Informationen darüber den Endteilnehmern in authentischer Form übergeben werden. Die TSP MÜSSEN die Fingerprints ihrer Sub-CA-Zertifikate (auch) über einen anderen Weg veröffentlichen als das Sub-CA-Zertifikat.

[EVCP] Die TSP MÜSSEN Test-Webseiten bereitstellen, die mit entsprechenden TLS-Serverzertifikaten des TSP gesichert sind, welche bis zu einer öffentlichen Root verkettet sind. Es MÜSSEN Webseiten mit einem gültigen, einem abgelaufenen und einem gesperrten Zertifikat bereitgestellt werden.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Die TSP MÜSSEN in ihren CPS die Zeitpunkte bzw. Häufigkeiten der in Kap. 2.2 aufgeführten Veröffentlichungen beschreiben.

2.4 Zugang zu den Verzeichnissen

Die Verzeichnisse MÜSSEN im Internet ohne Zugriffsbeschränkung verfügbar sein und MÜSSEN auf die ausschließliche Lesemöglichkeit eingeschränkt und vor unbefugter Manipulation sowie Datenverlust geschützt sein.

[3145] [VSNfD] Die Endteilnehmer MÜSSEN selbst entscheiden können, ob ihre Endteilnehmerzertifikate im Internet oder ggf. nur in internen kundenspezifischen Verzeichnissen veröffentlicht werden sollen. Die Sperrlisten sowie Root- und Sub-CA-Zertifikate MÜSSEN in jedem Fall in einem Verzeichnis im Internet bereitgestellt werden.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

Falls ein Zertifikat für eine natürliche Person in Assoziation mit einer juristischen Person ausgestellt wird, dann MÜSSEN die Zertifikatsattribute, welche die Organisation identifizieren, die juristische Person wiederspiegeln und der Subject Identifier im Zertifikat SOLL die natürliche Person sein.

Siehe Kapitel 7.1.2 und 7.1.4.

3.1.1 Namensformen

Siehe Kapitel 7.1.2 und 7.1.4.

3.1.2 Aussagekraft von Namen

Siehe Kapitel 7.1.2 und 7.1.4.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Siehe Kapitel 7.1.2 und 7.1.4.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Siehe Kapitel 7.1.2 und 7.1.4.

3.1.5 Eindeutigkeit von Namen

Über die Laufzeit einer CA SOLL ein bereits verwendeter Subject Distinguished Name NICHT einem anderen Zertifikatsinhaber zugewiesen werden.

[SSL] Ausgenommen hiervon ist der Subject Distinguished Name in Domain-validierten Zertifikaten, wenn ein Antragsteller sein rechtmäßiges Eigentumsrecht nachgewiesen hat.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Keine Vorgabe.

3.2 Initiale Validierung der Identität

Die TSP MÜSSEN die Identität des Antragstellers sowie des Zertifikatinhabers verifizieren und prüfen, ob die Zertifikatsanträge akkurat, autorisiert und vollständig entsprechend der vorliegenden Nachweise sind.

Die TSP MÜSSEN von dem Antragsteller eine physische Adresse oder andere Kontaktangaben einfordern.

Die TSP MÜSSEN entweder direkte Nachweise oder Bescheinigungen von angemessenen und autorisierten Quellen zur Prüfung der Identität und, falls anwendbar, weiterer Attribute der Zertifikatsinhaber verwenden. Nachweise DÜRFEN in Papierform oder elektronisch übermittelt werden. Die TSP MÜSSEN die Authentizität der bereitgestellten Nachweise auf Änderungen und Fälschungen hin prüfen. Alle Informationen, die für die Verifikation der Identität und weiterer Attribute des Zertifikatsinhabers verwendet wurden, MÜSSEN dokumentiert werden.

Die TSP MÜSSEN nur die für die Verifizierung der Identität notwendigen Nachweise verlangen.

Die Verifizierung der Identität MUSS in einem geeigneten Zeitrahmen der Registrierung stattfinden.

[EVCP] Die TSP MÜSSEN ausreichende Informationen, wie z.B. Name, Gerichtsbarkeit und Website, zur eindeutigen Identifizierung der autorisierten Quellen, die zur Validierung der Identitäten herangezogen werden, online auf eine geeignete und leicht zugängliche Art und Weise veröffentlichen und in ihren CPS in Kap. 3.2 beschreiben, wo diese Informationen veröffentlicht werden. Darüber hinaus MÜSSEN die TSP die zugelassenen Werte zu den nachfolgend aufgeführten Feldern veröffentlichen, welche in Endteilnehmerzertifikate aufgenommen werden, die auf Basis der Informationen dieser Quelle ausgestellt werden:

- jurisdictionLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1),
- jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2) sowie
- jursidictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3).

[SMIME] Die TSP MÜSSEN angemessene und sichere Methoden anwenden, um die Kontrolle des Antragstellers über die im Zertifikat referenzierte Email-Adresse bzw. die Autorisierung des Antragstellers, im Namen des tatsächlichen Inhabers der Email-Adresse zu handeln, zu verifizieren. Die Validierung des Domain-Anteils der Email-Adresse DARF NICHT durch die TSP an Dritte delegiert werden. Die TSP DÜRFEN auf Validierungen, die für einen Authorization Domain Name (wie in den Baseline Requirements definiert) durchgeführt wurden, als valide für Subdomains von diesem Authorization Domain Name zurückgreifen. Die angewandten Verifizierungsmethoden MÜSSEN von den TSP in ihren CPS beschrieben werden.

[VS-NfD] Die TSP MÜSSEN zusätzlich die Sicherheitsfreigabe des Antragstellers in Bezug auf die Nutzung der PKI verifizieren.

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Wenn das Schlüsselpaar nicht durch den TSP generiert wird, MUSS der Prozess zur Überprüfung des Zertifikatsantrags den Besitz oder die Kontrolle über den privaten Schlüssel abdecken.

[3145] Falls der Schlüssel vom Antragsteller generiert wird, MÜSSEN mindestens der öffentliche Schlüssel und die Antragsteller-Attribute mit dem privaten Schlüssel signiert sein. Die TSP MÜSSEN die Signatur prüfen.

3.2.2 Authentifizierung von Organisationen

[SSL] Ist ein Zertifikatsantragsteller eine Organisation, MÜSSEN die TSP eine zuverlässige Methode der Kommunikation verwenden, um die Autorisierung des Antragsteller-Vertreters, einen Zertifikatsantrag im Namen der Organisation zu stellen, zu verifizieren.

Die TSP DÜRFEN die Authentizität des Zertifikatsantrags direkt mit dem Vertreter des Antragstellers oder über eine verbindliche Quelle innerhalb der Organisation des Antragstellers überprüfen.

Die TSP MÜSSEN einen Prozess etablieren, welcher dem Antragsteller die Spezifizierung von Individuen erlaubt, welche Zertifikatsanträge stellen dürfen. Werden entsprechende Individuen vom Antragsteller benannt, MÜSSEN die TSP alle Zertifikatsanträge von nicht-spezifizierten Individuen ablehnen. Auf schriftliche Anfrage des Antragstellers, MÜSSEN die TSP dem Antragsteller eine Liste der autorisierten Zertifikatsantragsteller-Individuen bereitstellen.

[NCP] Nachweise zur Identität eines juristischen Zertifikatsinhabers und, falls anwendbar, weiterer Attribute MÜSSEN gegen einen ordnungsgemäß beauftragten Antragsteller entweder direkt, in physischer Anwesenheit eines berechtigten Vertreters der juristischen Person, oder indirekt, unter Verwendung von Mitteln, die eine zur physischen Anwesenheit vergleichbare Zusicherung bieten, überprüft werden.

Ist der Zertifikatsinhaber eine juristische Person oder eine organisatorische Entität, die in Assoziation mit einer juristischen Person identifiziert wird, dann MÜSSEN überprüft werden:

- Vollständiger Name der organisatorischen Entität/juristischen Person basierend auf nationalen oder anderweitig anwendbaren Identifikationspraktiken
- Falls anwendbar, die Assoziierung der juristischen Person zu der organisatorischen Entität, die in Assoziation mit dieser juristischen Person identifiziert wird, welche in dem Organization-Attribut im Zertifikat eingetragen wird.

Ist der Zertifikatsinhaber ein Gerät oder System, welches im Namen einer juristischen Person oder einer organisatorischen Entität, die in Assoziation mit einer juristischen Person identifiziert wird, betrieben wird, dann MÜSSEN zusätzlich überprüft werden:

- Identifikator des Geräts oder Systems

[SSL] Werden die Identität einer Organisation, Adresse einer Organisation, eine Firmierung oder ein Markenname in ein Zertifikat aufgenommen, dann MÜSSEN diese anhand bereitgestellter Dokumente von oder durch Kommunikation mit mindestens einer der folgenden Instanzen verifiziert werden:

- Staatliche Behörde im Amtsbereich der Gründung, Existenz oder Anerkennung der juristischen Person (Identität, Adresse, Firmierung, Markenname)
- Datenbestand eines Dritten, der regelmäßig aktualisiert und als zuverlässige Datenquelle angesehen wird (Identität, Adresse, Firmierung, Markenname)
- Vorort-Besichtigung durch den TSP oder einen autorisierten Vertreter (Identität, Adresse)
- Bescheinigungsschreiben (Identität, Adresse, Firmierung, Markenname)
- Betriebskostenabrechnung, Bankauszug, Kreditkartenauszug, vom Staat ausgegebenen Steuerbelege oder andere Identifikationsformen, welche der TSP als zulässig identifiziert (Adresse, Firmierung, Markenname)
- Kommunikation mit einer staatlichen Behörde für die Verwaltung von Firmierungen oder Markennamen (Firmierung, Markenname)

Falls das Attribut countryName gesetzt werden soll, MUSS das mit dem Zertifikatsinhaber assoziierte Land basierend auf folgenden Informationen verifiziert werden:

- IP-Adressbereich-Zuweisung nach Land für die IP-Adresse der Webseite, wie es durch den DNS-Record für diese Webseite angegeben wird oder die IP-Adresse des Antragstellers
- ccTLD des angefragten Domain-Namen
- Informationen vom Domain-Namensregistrar
- Mithilfe einer der im vorherigen Abschnitt aufgeführten Methoden

Für die Verifizierung der IP-Adresse SOLLTE ein Prozess implementiert werden, um die Verwendung von Proxy Servern zu ermitteln.

Vor Verwendung einer Datenquelle als zuverlässige Datenquelle MUSS die Quelle im Hinblick auf ihre Zuverlässigkeit, Genauigkeit und Änderungs- oder Fälschungssicherheit evaluiert werden. Es MUSS Folgendes berücksichtigt werden:

- Alter der vorgelegten Informationen
- Häufigkeit der Aktualisierungen der Informationsquelle
- Datenanbieter und der Zweck der Datenerfassung
- Verfügbarkeit der Daten
- Integrität der Daten

Datenbanken, die von der CA, ihrem Eigentümer oder ihren Beteiligungsgesellschaften gepflegt werden, gelten nicht als zuverlässige Datenquelle, wenn der Hauptzweck der Datenbank darin liegt, Informationen zur Erfüllung der Validierungsanforderungen zu sammeln.

[QCP-w] Es MUSS zusätzlich die Verbindung des Antragstellers mit dem angegebenen Domain Name verifiziert werden.

3.2.2.1 [SSL] Authentifizierung von Domain-Identitäten

Jeder vollqualifizierte Domain-Name (FQDN), der in einem Zertifikat aufgeführt werden soll, MUSS durch den TSP wie folgt validiert werden:

- Falls der FQDN nicht „onion“ als rechtesten Eintrag enthält, MÜSSEN die TSP den FQDN mithilfe einer der in den Baseline Requirements [CAB/BR] Kap. 3.2.2.4 bzw. EV Guidelines [EVCG] Kap. 11.7 beschriebenen Methoden validieren.
- Falls der FQDN „onion“ als rechtesten Eintrag enthält, MÜSSEN die TSP den FQDN entsprechend Appendix C der Baseline Requirements [CAB/BR] bzw. Appendix F der EV Guidelines [EVCG] validieren.

Die Validierung der Kontrolle über eine IP-Adresse muss entsprechend Kapitel 3.2.2.5 der Baseline Requirements [CAB/BR] durchgeführt werden.

Durchgeführte Validierungen DÜRFEN im Laufe der Zeit für die Ausstellung mehrerer Zertifikate gültig sein. Eine Validierung MUSS in innerhalb von 825 Tagen vor der Zertifikatsausstellung initiiert worden sein.

Es MÜSSEN weiterhin die Anforderungen aus Kapitel 3.2.2.6 und 3.2.2.8 der Baseline Requirements [CAB/BR] bzw. die weiteren Anforderungen aus Kapitel 11 der EV-Guidelines [EVCG] berücksichtigt werden. Die TSP MÜSSEN in ihren CPS die verwendeten Methoden aufführen.

3.2.3 Authentifizierung von natürlichen Personen

[NCP] Nachweise zur Identität eines natürlichen Zertifikatsinhabers und, falls anwendbar, weiterer Attribute MÜSSEN gegen die natürliche Person entweder direkt, in physischer Anwesenheit der Person oder eines ordnungsgemäß beauftragten Antragstellers, oder indirekt, unter Verwendung von Mitteln, die eine zur physischen Anwesenheit vergleichbare Zusicherung bieten, überprüft werden.

Ist der Zertifikatsinhaber eine natürliche Person, dann MÜSSEN überprüft werden:

- Vollständiger Name der Person (Nachname, Vornamen)
- Geburtsdatum und -ort, Referenzen auf national anerkannte Identifikationsdokumente oder andere Attribute, welche für eine eindeutige Identifikation herangezogen werden können

Ist der Zertifikatsinhaber eine natürliche Person, die in Assoziation mit einer juristischen Person identifiziert wird, dann MÜSSEN zusätzlich überprüft werden:

- Vollständiger Name und juristischer Stand der assoziierten juristischen Person
- Relevante Registrierungsinformationen der assoziierten juristischen Person
- Zugehörigkeit der natürlichen Person zur juristischen Person
- Bestätigung der juristischen und natürlichen Person, dass die Attribute des Zertifikatsinhabers auch die Organisation identifizieren

Ist der Zertifikatsinhaber ein Gerät oder System, welches von einer natürlichen Person betrieben wird, dann MÜSSEN überprüft werden:

- Identifikator des Geräts
- National anerkannte Identitätsnummer oder andere Attribute, welche für eine eindeutige Identifikation der natürlichen Person herangezogen werden können

[SSL] Die TSP MÜSSEN den Namen, Anschrift und Authentizität des Zertifikatsantrags verifizieren.

Für die Verifizierung des Namen MUSS mindestens eine leserliche Kopie eines gültigen, staatlichen Lichtbildausweises, der das Gesicht des Antragstellers erkennbar zeigt, herangezogen werden. Die Kopie MUSS auf Anzeichen von Änderungen und Fälschungen untersucht werden.

Für die Verifizierung der Anschrift MUSS eine Form der Identifizierung herangezogen werden, welche die TSP als vertrauenswürdig erachten. Es dürfen die staatlichen Lichtbildausweise verwendet werden, die für die Verifizierung des Namens verwendet werden.

Für die Verifizierung der Authentizität des Zertifikatsantrags MUSS eine zuverlässige Methode der Kommunikation verwendet werden (vgl. Baseline Requirements Reliable Method of Communication).

[QCP-w] Es MUSS zusätzlich die Verbindung des Antragstellers mit dem angegebenen Domain Name verifiziert werden.

3.2.4 Nicht überprüfte Informationen

Keine Vorgabe.

3.2.5 Validierung der Bevollmächtigung

Falls der Antragsteller nicht der Zertifikatsinhaber ist, dann MÜSSEN der vollständige Name und die Berechtigung des Antragstellers, im Namen des Zertifikatsinhabers zu agieren, überprüft werden.

Zur Vermeidung von Interessenskonflikten MÜSSEN die TSP und der Antragsteller unterschiedliche Entitäten sein. Einzige Ausnahme bildet die Organisation, welche RA-Aufgaben durchführt und sich selbst oder Personen, die in Verbindung mit dieser Organisation identifiziert werden, ein Zertifikat ausstellt. Die Ausnahme MUSS in den Richtlinien der TSPs beschrieben sein.

3.2.6 Cross-Zertifikate

Keine Vorgabe.

[SSL] Die TSP MÜSSEN alle Cross-Zertifikate veröffentlichen, welche als Zertifikatsinhaber die CAs der TSP angegeben haben, vorausgesetzt, dass die TSP diese Cross-Zertifizierungen veranlasst bzw. akzeptiert hat.

3.3 Identifizierung und Authentifizierung für Zertifikatserneuerungen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Zertifikatserneuerungen

Die TSP MÜSSEN das Vorhandensein und die Gültigkeit des zu erneuernden Zertifikats sowie die Gültigkeit der Informationen zur Verifikation der Identität und Attribute des Zertifikatsinhabers gemäß Kapitel 3.2 prüfen.

Bereits vorhandene Nachweise DÜRFEN für die Validierung der Identität unter Berücksichtigung der anwendbaren Rechtslage und der verbliebenen Gültigkeit der Nachweise wiederverwendet werden.

[SSL] Die Verifikation von Informationen, die für eine Zertifikatserneuerung verwendet werden, DARF NICHT älter als 825 sein. Sollte die Verifikation älter als 825 Tage sein, MÜSSEN die Informationen auf Aktualität und Richtigkeit geprüft werden.

[EVCP] Die TSP MÜSSEN alle Aufgaben zur Authentifizierung und Verifizierung entsprechend der EV Guidelines [EVCG] durchführen, um sicherzustellen, dass der Zertifikatsantrag autorisiert ist und die Informationen noch immer akkurat und gültig sind.

Falls ein Antragsteller bereits ein zum Zeitpunkt der Antragstellung gültiges EV-Zertifikat des TSP besitzt, DARF der TSP auf die vorherige Authentifizierung und Verifikation entsprechend Kapitel 11.14.1 der EV-Guidelines [EVCG] zurückgreifen.

Für die Neu-Ausstellung von EV-Zertifikaten DARF die Verifikation der in Kapitel 11.14.3 der EV-Guidelines [EVCG] angegebenen Informationen NICHT älter als 13 Monate sein. Die Frist der 13 Monate beginnt mit dem Erhalt der Informationen.

Für die Ausstellung von Ersatz-Zertifikaten DÜRFEN die TSP auf bereits verifizierte Zertifikatsanträge zurückgreifen, soweit das zu ersetzende Zertifikat nicht aufgrund von Betrug oder anderer rechtswidriger Handlungen gesperrt wurde und das Ablaufdatum des Ersatz-Zertifikats sowie die Subject Information identisch bleiben.

3.3.2 Identifizierung und Authentifizierung für Zertifikatserneuerungen nach einer Sperrung

Keine Vorgabe.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die TSP MÜSSEN in ihren CPS die Methoden für die Identifizierung und Authentifizierung von Sperranträgen festlegen.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Die Root-CA und die TSP MÜSSEN in ihren CPS festlegen, wer welche Zertifikate beantragen darf und dabei die möglichen Rollen (z.B. Antragsteller, Subjekt des Zertifikats, natürliche Personen, juristische Personen) beschreiben.

[SSL] Die TSP MÜSSEN eine interne Datenbank betreiben, die alle Zertifikatsanträge und Zertifikate enthält, die aufgrund des Verdachts einer betrügerischen Verwendung zurückgewiesen oder gesperrt wurden. Weitere Anträge von den in dieser Datenbank aufgeführten Endteilnehmern MÜSSEN bzgl. des Verdachts einer betrügerischen Verwendung geprüft und ggf. abgelehnt werden.

[EVCP] Die Ausstellung von Zertifikaten MUSS auf folgende Organisationsformen (Definitionen dazu siehe Kap. 1.6.1) eingeschränkt werden:

- Unternehmen,
- Behörden,
- Private Organisationen und
- Nichtkommerzielle Unternehmen.

[3145] Suspendierte Endteilnehmer DÜRFEN NICHT Zertifikatsanträge stellen.

Die TSP MÜSSEN ihre Datenbank prüfen, ob der Endteilnehmer bereits zuvor registriert wurde. Wenn das der Fall ist, so MÜSSEN alle weiteren Zertifikate dieser Registrierung zugeordnet werden, damit im Fall einer Suspendierung des Endteilnehmers alle Zertifikate dieses Endteilnehmers gemäß den Nutzungsbedingungen gleichzeitig suspendiert oder gesperrt werden können.

4.1.2 Antragsprozess und -verantwortlichkeiten

4.1.2.1 Beantragung eines Root-CA-Zertifikats

Der Root-TSP MUSS in seinem CPS die Antragsprozesse und -verantwortlichkeiten beschreiben.

4.1.2.2 Beantragung eines Sub-CA-Zertifikats

Vor der Ausstellung eines Sub-CA-Zertifikats MUSS der Root-TSP

- ein von der Root-CA bereitgestelltes und vom beantragenden TSP ausgefülltes und unterschriebenes Zertifikatsantragsformular,

- eine elektronische Zertifikatsanforderung („Certificate Signing Requeust“, CSR) in dem von der Root-CA vorgegebenen Format sowie
- ggf. weitere vom Root-TSP geforderte Dokumente (z.B. kommerzielle Vereinbarungen)

erhalten haben.

Darüber hinaus MUSS sich der Root-TSP versichern, dass der beantragende TSP den privaten Schlüssel, der dem zur Zertifizierung vorgelegten öffentlichen Schlüssel zugeordnet ist, besitzt oder die Kontrolle darüber hat.

Der beantragende TSP MUSS die Akzeptanz der Nutzungsvereinbarungen (siehe Kap.9.6.3) und die Korrektheit der gemachten Angaben im Zertifikatsantragsformular bestätigen.

Das Zertifikatsantragsformular DARF in elektronischer Form übergeben werden. In diesem Fall muss es aber mit einer mindestens fortgeschrittenen elektronischen Signatur oder einem fortgeschrittenen elektronischen Siegel versehen sein.

4.1.2.3 Beantragung eines Endteilnehmer-Zertifikats

Die TSP MÜSSEN den Antragsprozess inkl. der zu nutzenden Schnittstellen für die Endteilnehmer klar beschreiben.

Wenn der Antragsteller nicht das Subjekt des Zertifikats ist und das Subjekt des Zertifikats eine natürliche oder juristische Person ist, MUSS der Zertifikatsantrag aus zwei Teilen bestehen:

- Der erste Teil MUSS vom Antragsteller unterschrieben sein und mindestens Folgendes beinhalten:
  - die Bestätigung zur Kenntnisnahme und Akzeptanz der Nutzungsbedingungen,
  - die Zustimmung zu den Pflichten des Antragstellers,
  - die Zustimmung zur Nutzung eines entsprechenden kryptografischen Moduls (HSM oder QSCD), sofern dieses vom TSP gefordert wird,
  - die Zustimmung zur Aufzeichnung der im Rahmen der Antragstellung- und -Bearbeitung sowie in der Ausstellung und Auslieferung und ggf. späteren Sperrung eines Zertifikats aufgenommen Daten durch den TSP,
  - die Information, ob der Antragsteller die Veröffentlichung des Zertifikats wünscht und dieses vom Subjekt des Zertifikats akzeptiert wird,
  - die Bestätigung, dass die Angaben zu den ins Zertifikat aufzunehmenden Daten korrekt sind,
  - die Pflichten des Subjekts des Zertifikats.
- Der zweite Teil MUSS vom Subjekt des Zertifikats unterschrieben sein und mindestens Folgendes beinhalten:
  - die Bestätigung zur Kenntnisnahme und Akzeptanz der Nutzungsbedingungen,
  - die Zustimmung zu den Pflichten des Subjekts,
  - die Zustimmung zur Nutzung eines entsprechenden kryptografischen Moduls (HSM oder QSCD), sofern dieses vom TSP gefordert wird,
  - die Zustimmung zur Aufzeichnung der im Rahmen der Antragstellung- und -Bearbeitung sowie in der Ausstellung und Auslieferung und ggf. späteren Sperrung eines Zertifikats aufgenommen Daten durch den TSP.

  Hinweis zu Zertifikaten für juristische Personen: Wenn der Antragsteller der offizielle Vertreter des Subjekts des Zertifikats ist, oder das Subjekt der offizielle Vertreter des

Antragstellers, DÜRFEN die beiden Teile des Antrags zusammen unterschrieben werden.

Wenn der Antragsteller zugleich das Subjekt des Zertifikats ist oder das Subjekt des Zertifikats ein Gerät ist, DARF der Zertifikatsantrag entweder aus einem oder zwei Teilen mit den o.g. Inhalten bestehen.

Zertifikatsanträge DÜRFEN, sofern vom TSP nicht anders vorgegeben, in elektronischer Form gestellt werden.

[QCP] Elektronisch eingereichte Zertifikatsanträge SOLLTEN mindestens mit einer fortgeschrittenen elektronischen Signatur oder einem fortgeschrittenen elektronischen Siegel versehen sein.

[SSL] Die Endteilnehmer MÜSSEN zur Beantragung eines Zertifikats sowohl einen formalen Zertifikatsantrag mit den o.g. Angaben als auch eine elektronische Zertifikatsanforderung (z.B. im PKCS#10-Format) beim TSP einreichen.

Die TSP DÜRFEN, unter Berücksichtigung der Gültigkeitsfristen von Identifizierungen, einen Zertifikatsantrag akzeptieren, in dem mehrere Zertifikate eines Antragstellers beantragt werden, sofern für jedes Zertifikat ein separater gültiger elektronischer Zertifikatsrequest eingereicht wird.

[EVCP] Der erste Teil des Antrags (s.o.) MUSS eine Bestätigung der Berechtigung des Antragstellers zur Beantragung eines Zertifikats im Namen der Organisation beinhalten.

Bei den Antragstellern MÜSSEN folgende Rollen (Definitionen dazu siehe Kap. 1.6.1) implementiert werden:

- Zertifikatsanforderer,
- Zertifikatsgenehmiger,
- Vertragsunterzeichner sowie
- ggf. Vertreter des Antragstellers (für den Fall, dass der Antragsteller mit dem TSP verbunden ist).

Der Antragsteller DARF eine Person mit mehreren der aufgeführten Rollen betrauen und die Rollen mit mehreren Personen besetzen.

[VS-NfD] Der Antragsprozess MUSS durch den Sicherheitsbeauftragten freigegeben werden.

4.2 Bearbeitung der Zertifikatsanträge

Die nachfolgend aufgeführten Bearbeitungsschritte MÜSSEN von vertrauenswürdigem Personal (siehe dazu auch Kap. 5.2.1) durchgeführt werden.

Die TSP DÜRFEN die Bearbeitung der Zertifikatsanträge oder Teilen davon an Externe RAs auslagern. In diesem Fall MÜSSEN die TSP sicherstellen, dass der Prozess als Ganzes den Anforderungen dieser CP genügt. Dementsprechend MÜSSEN die TSP die externen RAs identifizieren und authentisieren und MÜSSEN sicherstellen, dass die zwischen externer RA und TSP ausgetauschten Informationen sicher ausgetauscht werden.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die TSP MÜSSEN die Identifizierung und Authentifizierung gemäß Kap. 3.2 durchführen und die Prozesse und Vorgaben für die Durchführung der Identifizierung und Authentifizierung inkl. der Überprüfung aller vom Antragsteller zur Aufnahme in das Zertifikat angeforderten Daten in ihren CPS beschreiben.

[SSL] Wenn Zertifikatsanträge durch externe Kunden-RAs geprüft werden, MUSS der TSP

- vor Aufnahme eines FQDN in ein Zertifikat sicherstellen, dass dieser aus dem erlaubten Namensbereich des Kunden stammt,
- vor Aufnahme eines anderen Namens (kein FQDN) in ein Zertifikat sicherstellen, dass der Name entweder dem Kunden selbst oder einem Vertragspartner des Kunden entspricht oder dass der Kunde des TSP diesen vertritt.

Die TSP MÜSSEN diese Vorgaben als vertragliche Anforderung den Kunden-RAs auferlegen und deren Einhaltung überprüfen.

[SSL] Die TSP MÜSSEN, sofern anwendbar, zusätzlich erforderliche Prüfungen für „High-Risk-Zertifikate“ umsetzen und in den CPS beschreiben.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Die Genehmigung oder Ablehnung von Zertifikatsanträgen MUSS durch RAs der TSP oder von den TSP zugelassenen externen RAs erfolgen.

Wenn ein Endteilnehmer ein Zertifikat für einen Schlüssel beantragt, der nicht durch den TSP generiert wurde, so MUSS der TSP prüfen, dass der Endteilnehmer den privaten Schlüssel besitzt oder die Kontrolle darüber hat.

[SSL] Wenn in einem Antrag ein Schlüssel vorgelegt wird, der nicht den Anforderungen aus Kap. 6.1.5 und 6.1.6 genügt oder es sich um einen „Debian weak key“ handelt oder der Schlüssel zuvor von einer Sub-CA generiert wurde, MUSS der TSP den Antrag ablehnen.

Wenn in einem Zertifikatsantrag nicht alle erforderlichen Informationen enthalten sind, MUSS der TSP die fehlenden Informationen vom Antragsteller einfordern oder, nachdem der TSP diese über einer anderen zuverlässigen Weg erhalten hat, diese vom Antragsteller bestätigen lassen.

Die TSP MÜSSEN in Kap. 4.2 ihrer CPS die zu den [BR] konforme Behandlung von CAA-Records für FQDNs beschreiben und die vom TSP akzeptierten Aussteller-Domain-Namen aufführen.

[3145] Wenn in einem Antrag ein Schlüssel vorgelegt wird, der nicht den Anforderungen aus Kap. 6.1.5 und 6.1.6 genügt, MUSS der TSP den Antrag ablehnen.

Wenn die Nutzung kryptografischer Token gefordert ist, MÜSSEN die TSP über technische Maßnahmen sicherstellen, dass der gelieferte öffentliche Schlüssel korrekt dem Token und den Registrierungsdaten zugeordnet wird.

[QCP-l-qscd] [QCP-n-qscd] Die TSP MÜSSEN sicherstellen, dass der vorgelegte öffentliche Schlüssel von einem Schlüsselpaar stammt, welches in einer QSCD generiert wurde.

[EVCP] Wenn in einem Zertifikatsantrag nicht alle erforderlichen Informationen enthalten sind, MUSS der TSP die fehlenden Informationen vom Zertifikatsgenehmiger oder Vertragsunterzeichner und nicht vom Zertifikatsanforderer (Rollen siehe Kap. 4.1.2.3) bestätigen lassen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgabe.

4.3 Ausstellung von Zertifikaten

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

Die TSP MÜSSEN bei der Ausstellung der Zertifikate die Integrität und Authentizität gewährleisten und dementsprechende (technische, organisatorische oder personelle) Maßnahmen zum Schutz vor Fälschung der Daten vor der Ausstellung der Zertifikate treffen. Der Prozess der Ausstellung der Zertifikate MUSS sicher mit der zugehörigen Registrierung und, sofern anwendbar, mit dem vom Antragsteller übergebenen öffentlichen Schlüssel verknüpft werden.

Wenn die Endteilnehmer die in die Zertifikate aufzunehmenden öffentlichen Schlüssel liefern, MÜSSEN sich die TSP davon überzeugen, dass diese im Besitz der Schlüssel sind oder die Kontrolle darüber haben. Dieses kann z.B. durch die Übergabe eines Schlüssels mittels signiertem PKCS#10-Request erfolgen, dessen Signatur der TSP vor Ausstellung des Zertifikats prüft.

Wenn die TSP die Schlüssel der Endteilnehmer generieren, MÜSSEN sie die Vertraulichkeit der Schlüssel im Generierungsprozess sicherstellen.

[SSL] Die Endteilnehmerzertifikate MÜSSEN vor Ausstellung in einer hinreichend großen Anzahl von CT-Log-Servern (Certificate Transparency gemäß RFC 6962) als „Pre-Zertifikate“ veröffentlicht werden. Die dabei zurückgelieferten Bestätigungen mit Zeitstempel MÜSSEN in die Zertifikate als Extension mit der OID 1.3.6.1.4.1.11129.2.4.2 aufgenommen werden.

[3145] Die TSP SOLLTEN vor der Ausstellung von Zertifikaten prüfen, dass keine Zertifikate mit den gleichen Attributen jedoch anderen Schlüsseln existieren. In diesem Fall SOLLTE kein weiteres Zertifikat mit diesen Attributen erzeugt werden.

Wenn die Nutzung kryptografischer Token gefordert ist, MÜSSEN die TSP

- sicherstellen, dass der korrekte öffentliche Schlüssel des ausgewählten Tokens ins Zertifikat übernommen wird und dass das Zertifikat auf dem Token abgelegt wird,
- sicherstellen, dass der personalisierte Token an den richtigen Empfänger gesendet wird,
- den Versand/die Übergabe der Token so gestalten, dass ein von einem Angreifer abgefangener Token nicht verwendet werden kann, z.B. durch eine zur Nutzung des Tokens erforderliche Aktivierung, die nur durch den berechtigten Empfänger mittels

Aktivierungsdaten, die ihm über einen separaten Kanal übergeben wurden, durchgeführt werden kann.

DIE TSP MÜSSEN die Verfahren zur Ausgabe der Token in den Nutzungsbedingungen und den CPS beschreiben.

Wenn die TSP die Schlüssel für die Endteilnehmerzertifikate generieren, MÜSSEN die TSP

- sicherstellen, dass die Schlüssel dem korrekten Empfänger übermittelt werden,
- sicherstellen, dass die Vertraulichkeit der Schlüssel während der Übermittlung gewährleistet ist,
- sicherstellen, dass die Schlüssel beim TSP nach der Übermittlung an den korrekten Empfänger gelöscht werden, es sei denn, der TSP bietet ein Schlüsselbackup für die Endteilnehmer an.

DIE TSP MÜSSEN die Verfahren zur Übergabe der Schlüssel in den Nutzungsbedingungen und den CPS beschreiben.

[VS-NfD] Ergänzend zu den o.g. Anforderungen zu [3145] MÜSSEN die Vorgaben aus [VSA] zum Schutz der Schlüssel gemäß ihrer Klassifikation beachtet werden.

4.3.2 Benachrichtigung des Endteilnehmers über die Ausstellung eines Zertifikats

Die TSP MÜSSEN, sofern anwendbar, die ausgestellten Endteilnehmerzertifikate den Endteilnehmern, d.h. dem Antragsteller und/oder dem Subjekt des Zertifikats, übergeben oder diese über die Ausstellung benachrichtigen.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Keine Vorgabe.

4.4.2 Veröffentlichung des Zertifikats durch die TSP

Die TSP MÜSSEN Endteilnehmerzertifikate für jeden zugänglich veröffentlichen, sofern die Endteilnehmer (Antragsteller oder sofern anwendbar das Subjekt des Zertifikats) der Veröffentlichung zugestimmt haben, ansonsten DÜRFEN sie die Endteilnehmerzertifikate NICHT veröffentlichen.

Die TSP MÜSSEN die Prozesse der Veröffentlichung in ihren CPS beschreiben, siehe dazu auch Kap. 2.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP

Keine Vorgabe.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des Schlüsselpaars und des Zertifikats durch den Endteilnehmer

Die TSP MÜSSEN in ihren CPS die erlaubten und nicht erlaubten Verwendungszwecke der Endteilnehmerzertifikate beschreiben.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte

Keine Vorgabe.

4.6 Zertifikatserneuerung unter Beibehaltung der Schlüssel (Renewal)

4.6.1 Umstände für ein Renewal

Die TSP MÜSSEN die Umstände festlegen, unter denen ein Renewal erlaubt ist. Dabei sind u.a. die Aspekte der Schwächung der Schlüssel sowie die Anforderung nach bis zum Gültigkeitsende des neuen Zertifikats ausreichenden Schlüssellängen und zulässige Algorithmen zu betrachten.

[3145] Die TSP MÜSSEN in ihren CPS sowie in den Nutzungsbedingungen beschreiben, in welchem Zeitraum und unter welchen Umständen ein Renewal erlaubt ist.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese aufgrund eines Sicherheitsvorfalls gesperrt wurden.

4.6.2 Antragsberechtigte für ein Renewal

Siehe Kap. 4.1.1.

4.6.3 Verarbeitung von Anträgen auf Renewal

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, MÜSSEN die TSP die Akzeptanz dieser neuen Nutzungsbedingungen vom Endteilnehmer vor der Ausstellung eines neuen Zertifikats einholen.

Die TSP MÜSSEN vor der Erneuerung die Gültigkeit des ablaufenden Zertifikats sowie der ursprünglichen vorgelegten Identifizierungsdaten und Attribute des Subjekts prüfen. Die Anträge MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

Bei der Erneuerung von Zertifikaten MÜSSEN, sofern nicht in den CPS der TSP anders festgelegt, die gleichen Gültigkeitsdauern wie bei einer Erstausstellung angesetzt werden (siehe Kap. 6.3.2.3).

[SSL] Die TSP DÜRFEN zur Validierung auf bestehende Dokumente und Daten zurückgreifen, sofern diese nicht älter als 825 Tage sind.

[EVCP] Die TSP MÜSSEN in einem erneuerten Endteilnehmerzertifikat das gleiche Ablaufdatum und den gleichen Subject-DN wie im ursprünglichen Zertifikat setzen.

[3145] Die TSP MÜSSEN in ihren CPS die erforderlichen Prozesse beschreiben, für den Fall dass die Integrität der ursprünglichen Daten nicht mehr gegeben ist.

4.6.4 Benachrichtigung des Endteilnehmers über die Ausstellung neuer Zertifikate

Siehe Kap. 4.3.2.

4.6.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.6.6 Veröffentlichung erneuerter Zertifikate durch die TSP

Siehe Kap. 4.4.2.

4.6.7 Information Dritter über die Ausstellung neuer Zertifikate durch die TSP

Siehe Kap. 4.4.3.

4.7 Zertifikatserneuerung mit neuen Schlüsseln (Re-Keying)

4.7.1 Umstände für ein Re-Keying

Die TSP MÜSSEN die Umstände festlegen, unter denen ein Re-Keying erlaubt ist.

[3145] Die TSP MÜSSEN in ihren CPS sowie in den Nutzungsbedingungen beschreiben, in welchem Zeitraum und unter welchen Umständen ein Re-Keying erlaubt ist.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese aufgrund eines Sicherheitsvorfalls gesperrt wurden.

4.7.2 Antragsberechtigte für ein Re-Keying

Siehe Kap. 4.1.1.

4.7.3 Verarbeitung von Anträgen auf Re-Keying

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, MÜSSEN die TSP die Akzeptanz dieser neuen Nutzungsbedingungen vom Endteilnehmer vor der Ausstellung eines neuen Zertifikats einholen.

Die TSP MÜSSEN vor der Erneuerung die Gültigkeit des ablaufenden Zertifikats sowie der ursprünglichen vorgelegten Identifizierungsdaten und Attribute des Subjekts prüfen. Die Anträge MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

Bei der Erneuerung von Zertifikaten MÜSSEN, sofern nicht in den CPS der TSP anders festgelegt, die gleichen Gültigkeitsdauern wie bei einer Erstausstellung angesetzt werden (siehe Kap. 6.3.2.3).

[SSL] Die TSP DÜRFEN zur Validierung auf bestehende Dokumente und Daten zurückgreifen, sofern diese nicht älter als 825 Tage sind.

[3145] Die TSP MÜSSEN in ihren CPS die erforderlichen Prozesse beschreiben, für den Fall, dass die Integrität der ursprünglichen Daten nicht mehr gegeben ist.

Die TSP MÜSSEN die Generierung neuer Schlüssel erzwingen und prüfen, dass diese den Anforderungen gemäß Kap. 6.1.5 und 6.1.6 genügen.

4.7.4 Benachrichtigung des Endteilnehmers über die Ausstellung eines erneuerten Zertifikats

Siehe Kap. 4.3.2.

4.7.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.7.6 Veröffentlichung erneuerter Zertifikate durch die TSP

Siehe Kap. 4.4.2.

4.7.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

Siehe Kap. 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Änderung von Zertifikatsdaten

Die TSP MÜSSEN die Endteilnehmer verpflichten, die Änderung von registrierten Daten im Gültigkeitszeitraum der auf Basis der registrierten Daten erstellten Zertifikate dem TSP zu melden und MUSS die Endteilnehmer über die Prozesse bei Änderung der Zertifikatsdaten informieren.

4.8.2 Antragsberechtigte für eine Änderung von Zertifikatsdaten

Siehe Kap. 4.1.1.

4.8.3 Verarbeitung von Anträgen auf eine Änderung von Zertifikatsdaten

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, MÜSSEN die TSP die Akzeptanz dieser neuen Nutzungsbedingungen vom Endteilnehmer vor der Ausstellung eines neuen Zertifikats einholen.

Die TSP MÜSSEN vor der Änderung von Zertifikatsdaten die Gültigkeit des ablaufenden Zertifikats sowie der nicht geänderten ursprünglich vorgelegten Identifizierungsdaten und Attribute des Subjekts prüfen. Die Daten MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

[3145] Die TSP MÜSSEN in ihren CPS die erforderlichen Prozesse beschreiben, für den Fall, dass die Integrität der ursprünglichen Daten nicht mehr gegeben ist.

Die TSP MÜSSEN die Generierung neuer Schlüssel erzwingen und prüfen, dass diese den Anforderungen gemäß Kap. 6.1.5 und 6.1.6 genügen.

4.8.4 Benachrichtigung des Endteilnehmers über die Ausstellung eines erneuerten Zertifikats

Siehe Kap. 4.3.2.

4.8.5 Verhalten, das die Annahme eines geänderten Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.8.6 Veröffentlichung geänderter Zertifikate durch die TSP

Siehe Kap. 4.4.2.

4.8.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

Siehe Kap. 4.4.3.

4.9 Zertifikatssperrung und Suspendierung

Aufgrund der Kritikalität der Sperrung oder Suspendierung von Zertifikaten müssen alle beteiligten TSP und Endteilnehmer die zu beachtenden Sperrgründe und -fristen sowie die Abläufe kennen. Diese MÜSSEN daher in den CPS der TSP beschrieben werden.

Darüber hinaus MÜSSEN insbesondere die Endteilnehmer bei der Antragstellung über die Sperrgründe sowie die verfügbaren Schnittstellen zur Beantragung einer Sperrung informiert werden, z.B. in den AGB, Nutzungsbedingungen, PDS etc.

4.9.1 Sperrgründe

4.9.1.1 Gründe für die Sperrung eines Sub-CA Zertifikats

Ein Sub-CA-Zertifikat MUSS gesperrt werden, wenn

- ein schriftlicher Sperrantrag, auch ohne Angabe von Gründen, vom TSP gestellt wurde,
- festgestellt wird, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- festgestellt wird, dass der private Schlüssel der Sub-CA kompromittiert oder einer nicht autorisierten Person oder einer Organisation, die nicht mit der Sub-CA verbunden ist, bekannt gegeben wurde, oder nicht mehr den Anforderungen (siehe Kap. 6.1.5 und 6.1.6) entspricht,
- festgestellt wird, dass das Zertifikat missbräuchlich eingesetzt wurde,
- festgestellt wird, dass das Sub-CA-Zertifikat nicht konform zu dieser CP herausgegeben wurde oder der TSP nicht konform zu dieser CP arbeitet,
- festgestellt wird, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist,
- der Betrieb der Root-CA oder der Sub-CA eingestellt wird und keine Regelungen zur Weiterführung des Sperrservice getroffen wurden,
- das Recht der Root-CA oder Sub-CA, Zertifikate gemäß den Anforderungen dieser CP auszustellen erlischt oder widerrufen oder beendet wird und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden.

Darüber hinaus DÜRFEN der Root-TSP oder die TSP in ihren CPS weitere Sperrgründe festlegen.

4.9.1.2 Gründe für die Sperrung eines Endteilnehmer-Zertifikats

Endteilnehmerzertifikate müssen aus verschiedenen Gründen gesperrt werden. Da abhängig von den Sperrgründen unterschiedliche Sperrfristen festgelegt sind, werden die Sperrgründe nachfolgend nach Sperrfristen sortiert aufgeführt.

Ergänzend dazu DARF ein TSP in seinem CPS weitere Sperrgründe festlegen.

4.9.1.2.1 Kurzfristige Sperrung innerhalb von 24 Stunden

Ein Endteilnehmer-Zertifikat MUSS innerhalb von 24 Stunden gesperrt werden, wenn

- ein schriftlicher Sperrantrag, auch ohne Angabe von Gründen, vom Endteilnehmer gestellt wurde,
- festgestellt wird, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- festgestellt wird, dass der private Schlüssel des Endteilnehmer-Zertifikats kompromittiert wurde oder einer unautorisierten Person oder einer nicht mit dem Endteilnehmer verbundenen Organisation übergeben wurde.

[SSL] Ein Endteilnehmerzertifikat MUSS darüber hinaus gesperrt werden, wenn festgestellt wird, dass der Validierung der Domainautorisierung oder der Kontrolle über einen FQDN oder eine IP-Adresse im Zertifikat nicht vertraut werden kann.

[S/MIME] Ein Endteilnehmerzertifikat MUSS darüber hinaus gesperrt werden, wenn festgestellt wird, dass die in dem Zertifikat benannte E-Mail-Adresse rechtlich nicht länger genutzt werden darf.

[QCP] Ein Endteilnehmerzertifikat MUSS darüber hinaus gesperrt werden, wenn festgestellt wird, dass der private Schlüssel des Endteilnehmer-Zertifikats verloren gegangen ist.

4.9.1.2.2 Mittelfristige Sperrung innerhalb von fünf Tagen

Ein Endteilnehmer-Zertifikat SOLLTE innerhalb von 24 Stunden und MUSS spätestens innerhalb von fünf Tagen gesperrt werden, wenn

- festgestellt wird, dass das Zertifikat nicht in Übereinstimmung mit der CPS der Sub-CA ausgestellt wurde,
- der private Schlüssel nicht mehr den Anforderungen aus Kap. 6.1.5 und 6.1.6 genügt, oder Methoden bekannt geworden sind, die den privaten Schlüssel des Zertifikatinhabers gefährden oder die Berechnung des privaten Schlüssels aus dem öffentlichen Schlüssel ermöglichen oder dass es eindeutige Beweise dafür gibt, dass die für die Generierung des privaten Schlüssels verwendete Methode mangelhaft war.
- festgestellt wird, dass das Zertifikat missbräuchlich eingesetzt wurde,
- festgestellt wird, dass der Endteilnehmer gegen eine oder mehrere wesentliche Vereinbarungen oder Nutzungsbedingungen verstoßen hat,
- festgestellt wird, dass die Informationen im Zertifikat nicht korrekt sind oder es wesentliche Änderungen daran gegeben hat.

[SSL] Ein Endteilnehmerzertifikat MUSS darüber hinaus gesperrt werden, wenn

- das Recht des TSP zur Ausstellung von Zertifikaten gemäß den Baseline Requirements des CA/Browser-Forums erloschen ist oder widerrufen oder gekündigt wurde und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden,
- festgestellt wird, dass die Verwendung eines FQDN oder einer IP-Adresse im Zertifikat nicht mehr gesetzlich zulässig ist,
- festgestellt wird, dass ein Wildcard-Zertifikat zur Authentifizierung eines betrügerisch irreführenden sub-FQDN verwendet wurde.

4.9.1.2.3 Sperrung in einem angemessenen, nicht festgelegten Zeitraum

Ein Endteilnehmerzertifikat MUSS gesperrt werden, wenn

- der TSP den Betrieb einstellt und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden,
- Sicherheitsvorfälle, Integritätsprobleme oder Störungen dies erfordern.

[3145] Ein Endteilnehmerzertifikat MUSS darüber hinaus gesperrt werden, wenn

- von Dritten eine zulässige Begründung dafür angeführt wird,
- der Endteilnehmer suspendiert wird.

Die zuvor genannten Sperrgründe erfordern i.d.R. weitere Prüfungen oder Abstimmungen, so dass hierfür vorab keine Zeiträume festgelegt werden können. In diesen Fällen MÜSSEN Sperrungen in einem möglichst kurzen angemessenen Zeitraum erfolgen.

4.9.2 Berechtigte Sperrantragsteller

Die Sperrung einer Sub-CA MUSS grundsätzlich durch einen berechtigten Vertreter des TSP beantragt werden. Sollte einer der in Kap. 4.9.1.1 aufgeführten Sperrgründe vom Root-TSP festgestellt werden, so DARF eine Sperrung auch durch den Root-TSP veranlasst werden. Die weiteren organisatorischen und prozessualen Vorgaben MÜSSEN im CPS des Root-TSP beschrieben werden.

[3145] Die Sperrung einer Sub-CA im Anwendungsbereich der TR-03145 liegt nicht im Scope dieser CP, da die Sub-CA-Zertifikate nicht von einer Root-CA der Telekom ausgestellt werden. Die Sperrung der Sub-CAs MUSS gemäß den Vorgaben des zuständigen Root-TSP erfolgen und MUSS im CPS des TSP beschrieben werden.

Die Sperrung eines Endteilnehmerzertifikats MUSS grundsätzlich durch den Endteilnehmer selbst oder die zuständige RA beantragt werden. Sollte einer der in Kap. 4.9.1.2 aufgeführten Sperrgründe vom TSP festgestellt oder durch einen Dritten gemeldet und vom TSP nachvollzogen werden können, so MUSS eine Sperrung durch den TSP veranlasst werden. Die weiteren organisatorischen und prozessualen Vorgaben MÜSSEN im CPS des TSP beschrieben werden.

[SSL] [SMIME] Die Sperrung eines Endteilnehmerzertifikats MUSS darüber hinaus durch den TSP veranlasst werden, wenn ein Vertreter der relevanten Trusted Root Programme einen der in Kap. 4.9.1.2 aufgeführten Sperrgründe meldet.

[3145] Die Sperrung eines Endteilnehmerzertifikats MUSS darüber hinaus vom TSP veranlasst werden, wenn der Endteilnehmer suspendiert wird.

[VS-NfD] Die Sperrung eines Endteilnehmerzertifikats MUSS darüber hinaus vom TSP auf ein begründetes Verlangen des Sicherheitsbeauftragten veranlasst werden.

4.9.3 Ablauf einer Sperrung

Zur Sperrung von Zertifikaten aller Hierarchieebenen MÜSSEN ständig verfügbare Schnittstellen (7x24h) zur Übergabe von Sperranträgen oder Problemmeldungen, die zur Sperrung von Zertifikaten führen können, bereitgestellt werden.

Sperranträge DÜRFEN NICHT bearbeitet werden, wenn diese nicht von berechtigten Sperrantragstellern gestellt werden oder auf Problemmeldungen beruhen, die vom verantwortlichen TSP geprüft und nicht als berechtigter Auslöser einer Sperrung eingestuft werden.

Die berechtigten Sperrantragsteller MÜSSEN über die bereitgestellten Schnittstellen und deren Nutzung informiert werden.

[SSL] [SMIME] Die Schnittstellen zur Meldung von Problemen, wie z.B. Verdacht einer Schlüsselkompromittierung, Zertifikatsmissbrauch oder andere Arten von Betrug oder unangemessenem Verhalten im Zusammenhang mit Zertifikaten, MÜSSEN auf den Web-Seiten der TSP sowie in den relevanten CPS (in den Kontaktinformationen in Kap. 1.5.2 gemäß RFC3647) aufgeführt sein.

Über eine durchgeführte Sperrung MÜSSEN, sofern möglich, sowohl der Sperrantragsteller als auch der Inhaber des gesperrten Zertifikats informiert werden.

Endgültig gesperrte Zertifikate DÜRFEN NICHT wieder entsperrt werden.

[SSL] [SMIME] Nach der Sperrung eines Sub-CA-Zertifikats MUSS der TSP die CCADB updaten. Wenn die Sperrung des Sub-CA-Zertifikats aufgrund eines Sicherheitsvorfalls erforderlich ist, MUSS die CCADB innerhalb von 24 Stunden upgedatet werden, ansonsten innerhalb von 7 Tagen.

Die Abläufe zur Sperrung von Root- und Sub-CA-Zertifikaten MÜSSEN im CPS der Telekom-Root-CA beschrieben werden.

Die Abläufe zur Sperrung von Endteilnehmerzertifikaten MÜSSEN in den CPS der TSP beschrieben werden.

[SSL] Die TSP MÜSSEN rund um die Uhr in der Lage sein, auf hochpriorisierte Problemmeldungen zu reagieren und bei Bedarf eine Meldung an Strafverfolgungsbehörden weiterzuleiten und / oder die von dem Problem betroffenen Zertifikate zu sperren.

[3145] Die Abläufe zur Suspendierung von Endteilnehmern MÜSSEN im CPS des TSP beschrieben werden.

[VS-Nfd] Die Abläufe zur Sperrung von Endteilnehmerzertifikaten inkl. der festgelegten Fristen MÜSSEN vom Sicherheitsbeauftragten freigegeben werden.

4.9.4 Fristen zur Beantragung einer Sperrung

Sobald ein Sperrgrund gemäß Kap. 4.9.1 festgestellt wird, MUSS unverzüglich ein Sperrantrag gestellt werden.

4.9.5 Fristen zur Verarbeitung von Sperranträgen durch die TSP

Sub-CA-Zertifikate MÜSSEN innerhalb von sieben Tagen nach Erhalt eines autorisierten Sperrantrags gesperrt werden, diese Frist beinhaltet die Zeit zur Umsetzung des Sperrstatus in den Zertifikatsstatusdiensten.

Endteilnehmerzertifikate MÜSSEN grundsätzlich so schnell wie möglich, jedoch spätestens innerhalb von 24 Stunden nach Eingang eines autorisierten Sperrantrags gesperrt werden, diese Frist beinhaltet die Zeit zur Umsetzung des Sperrstatus in den Zertifikatsstatusdiensten.

Davon ausgenommen sind Sperrungen, die für einen späteren Zeitpunkt beantragt werden, z.B. aufgrund einer geplanten Beendigung der Teilnahme eines Endteilnehmers. In diesem Fall DARF der TSP, sofern dieses Vorgehen im CPS beschrieben ist, das im Sperrantrag aufgeführte Wunschdatum zur Sperrung des Zertifikats als Eingangsdatum des autorisierten Sperrantrags setzen.

Für Sperrungen, die nicht auf autorisierten Sperranträgen basieren, sondern aus Problemmeldungen resultieren, gelten die in Kap. 4.9.1 aufgeführten Fristen.

[SSL] Innerhalb von 24 Stunden nach Eingang einer Problemmeldung MÜSSEN die Fakten und Umstände vom betroffenen TSP untersucht werden und es MUSS dem Endteilnehmer sowie der meldenden Person eine erste Rückmeldung zu den bis dahin vorliegenden Erkenntnissen gegeben werden. Anschließend MÜSSEN mit dem Endteilnehmer und der meldenden Person die Analyseergebnisse besprochen werden und es MUSS entschieden werden, ob eine Sperrung erforderlich ist. Falls eine Sperrung erforderlich ist, MUSS unter Beachtung der zeitlichen Vorgaben aus Kap. 4.9.1 und Berücksichtigung der folgenden Aspekte der Zeitpunkt der Sperrung festgelegt werden:

- die Art des mutmaßlichen Problems (Umfang, Kontext, Schweregrad, Ausmaß, Schadensrisiko),
- die Auswirkungen einer Sperrung (direkte und kollaterale Auswirkungen auf Endteilnehmer vertrauende Dritte),
- die Anzahl der Problemmeldungen zu einem Zertifikat oder Endteilnehmer,
- die Entität welche die Meldung eingestellt hat sowie
- die einschlägigen Rechtsvorschriften.

Ergänzend zu den aufgeführten Fristen DARF ein TSP in seinem CPS kürzere Fristen für bestimmte Sperrgründe festlegen.

4.9.6 Anforderungen an Dritte zur Prüfung von Sperrinformationen

Vertrauende Dritte MÜSSEN zur Prüfung des Status von Zertifikaten die von den TSP angebotenen Zertifikatsstatusdienste gemäß Kap. 4.10 abfragen.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Sperrlisten, die Auskunft über gesperrte Sub-CAs geben, MÜSSEN innerhalb von 24 Stunden nach Sperrung eines Sub-CA-Zertifikats sowie regelmäßig mindestens alle 12 Monate aktualisiert werden. Diese Vorgabe gilt sowohl für die von den Root-CAs als auch von den Sub-CAs, welche weitere Sub-CA-Zertifikate ausstellen (Hierarchien mit mehreren Sub-CA-Ebenen) ausgestellten CA Revocation Lists (CARL).

Sperrlisten, die Auskunft über gesperrte Endteilnehmerzertifikate geben (Certificate Revocation Lists (CRL)), MÜSSEN regelmäßig mindestens alle 24 Stunden aktualisiert werden.

[SSL] [3145] Sperrlisten, die Auskunft über gesperrte Endteilnehmerzertifikate geben, MÜSSEN ergänzend zur regelmäßigen Ausstellung auch im Anschluss an die Sperrung eines Endteilnehmer-Zertifikats erstellt und veröffentlicht werden.

4.9.8 Maximale Latenzzeit von Sperrlisten

Neu erstellte Sperrlisten MÜSSEN innerhalb einer Stunde nach ihrer Erzeugung veröffentlicht werden.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Der Root-TSP DARF Online-Statusinformationen für die Root- und Sub-CA-Zertifikate per OCSP anbieten.

Die Sub-CAs MÜSSEN Online-Statusinformationen für die Endteilnehmerzertifikate per OCSP anbieten.

4.9.10 Anforderungen an Online Überprüfungsverfahren

Wenn Dritte den Status von Zertifikaten per OCSP prüfen, MÜSSEN diese RFC6960-konforme OCSP-Clientkomponenten verwenden, d.h. diese MÜSSEN OCSP-Antworten des Typs „id-pkix-ocsp-basic response" sowie den Signaturalgorithmus „sha256WithRSAEncryption" verarbeiten können und prüfen, dass

- das in der Antwort referenzierte Zertifikat dem Zertifikat in der Anfrage entspricht,
- die Signatur der Antwort gültig ist,
- die Identität des OCSP-Signers mit dem beabsichtigten Empfänger der Anfrage übereinstimmt,
- der OCSP-Signer zum Zeitpunkt der Signatur berechtigt ist, eine Statusauskunft zum angefragten Zertifikat zu geben,
- der Zeitpunkt der Erstellung der Statusauskunft („thisUpdate") hinreichend aktuell ist und,

- sofern angegeben, der Zeitpunkt für die geplante Aktualisierung der Statusinformationen („nextUpdate“), in der Zukunft liegt.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine Vorgabe.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Es gelten die in Kap. 4.9.1 getroffenen Vorgaben.

4.9.13 Umstände für eine Suspendierung

Root- und Sub-CA-Zertifikate DÜRFEN NICHT suspendiert werden.

Endteilnehmerzertifikate DÜRFEN suspendiert werden, es gibt diesbezüglich keine konkreten Vorgaben. Falls eine Suspendierung von einer Sub-CA angeboten wird, MUSS der TSP in dem relevanten CPS die Umstände für eine Suspendierung festlegen.

[SSL] Endteilnehmerzertifikate DÜRFEN NICHT suspendiert werden.

[3145] Ergänzend zur Sperrung oder Suspendierung von Endteilnehmerzertifikaten MÜSSEN unterbestimmten Umständen auch Endteilnehmer suspendiert werden. Die Vorgaben und Abläufe MÜSSEN im CPS des TSP beschrieben werden.

4.9.14 Berechtigte Antragsteller für eine Suspendierung

Falls eine Suspendierung von einer Sub-CA angeboten wird, MÜSSEN die berechtigten Antragsteller für eine Suspendierung im CPS des TSP festgelegt werden.

[SSL] Nicht anwendbar.

[3145] Die berechtigten Antragsteller für eine Suspendierung von Endteilnehmern MÜSSEN im CPS des TSP beschrieben werden.

4.9.15 Ablauf einer Suspendierung

Falls eine Suspendierung von einer Sub-CA angeboten wird, MÜSSEN die Abläufe für eine Suspendierung im CPS des TSP festgelegt werden.

[SSL] Nicht anwendbar.

[3145] Die Abläufe zur Suspendierung von Endteilnehmern MÜSSEN im CPS des TSP beschrieben werden.

4.9.16 Begrenzung der Suspendierungsperiode

Falls eine Suspendierung von einer Sub-CA angeboten wird, MÜSSEN die Zeiträume und Fristen für eine Suspendierung im CPS des TSP festgelegt werden.

[SSL] Nicht anwendbar.

[3145] Die Zeiträume und Fristen für eine Suspendierung von Endteilnehmern MÜSSEN im CPS des TSP beschrieben werden.

4.10 Zertifikatsstatusdienste

Es MÜSSEN mindestens über die Gültigkeitsdauer aller ausgestellten Zertifikate authentische und integre Zertifikatsstatusdienste bereitgestellt werden.

Zu den Root- und Sub-CA-Zertifikaten MÜSSEN Sperrlisten oder OCSP-Auskünfte oder beides bereitgestellt werden.

Zu den Teilnehmerzertifikaten MÜSSEN Sperrlisten und OCSP-Auskünfte bereitgestellt werden.

[QCP] Ergänzend bzw. abweichend gelten für die Zertifikatsstatusdienste zu qualifizierten Zertifikaten folgende Vorgaben:

- Die Zertifikatsstatusdienste MÜSSEN über die Zertifikatsgültigkeit hinaus bereitgestellt werden.
- Sperrlisten DÜRFEN bereitgestellt werden. Wenn Sperrlisten bereitgestellt werden, MÜSSEN diese mindestens solange bereitgestellt werden, bis alle Zertifikate im Anwendungsbereich der Sperrliste abgelaufen oder gesperrt sind. Wenn Sperrlisten über die Gültigkeitsdauer der Zertifikate hinaus angeboten werden, MUSS die Bereitstellungszeit im CPS des TSP beschrieben werden und die Integrität der Sperrliste für die Dauer der Bereitstellung sichergestellt werden.

4.10.1 Betriebliche Vorgaben

Die Zertifikatsstatusdienste (Sperrlisten und OCSP) MÜSSEN mindestens alle 24 Stunden zeitsynchronisiert (UTC) werden.

Wenn Sperrlisten und OCSP-Auskünfte bereitgestellt werden, MÜSSEN diese unter Berücksichtigung der unterschiedlichen Aktualisierungsfristen beider Methoden spätestens nach 24 Stunden konsistent sein.

4.10.1.1 Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

Die OCSP-Responder MÜSSEN konform zum RFC6960 arbeiten. Konkretisierend zum RFC6960 gilt, dass Anfragen zu Zertifikaten mit NICHT bekannten Zertifikatseriennummern nicht mit dem Status „good“ beantwortet werden DÜRFEN, sondern entweder mit der

Fehlermeldung „unauthorized“ oder dem Status „unknown“ oder „revoked“ beantwortet werden MÜSSEN.

Die zu wählende Antwort hängt von der Arbeitsweise des OCSP-Responders ab:

- Bei vorproduzierten OCSP-Antworten MÜSSEN solche Anfragen mit der Fehlermeldung „unauthorized“ beantwortet werden, da dem OCSP-Responder keine vorproduzierte Antwort auf die Anfragen vorliegt und auch nicht adhoc produziert werden kann.
- Bei adhoc erzeugten OCSP-Antworten SOLLTEN solche Anfragen mit dem Status „unknown“ beantwortet werden, da dem OCSP-Responder kein Status zu der angefragten Seriennummer vorliegt, jedoch adhoc eine gültige OCSP-Antwort produziert werden kann. Es DÜRFEN bei adhoc erzeugten OCSP-Antworten solche Anfragen auch mit dem Status „revoked“ beantwortet werden, dann MUSS jedoch die Erweiterung „Extended Revoked Definition“ gemäß RFC6960 #4.4.8 gesetzt werden.

Die OCSP-Antworten zu Sub-CA-Zertifikaten DÜRFEN eine Gültigkeit von maximal 12 Monaten NICHT überschreiten. Nach einer Sperrung eines Sub-CA-Zertifikats MUSS innerhalb von 24 Stunden eine aktualisierte Auskunft im OCSP-Responder abrufbar sein.

Die OCSP-Antworten zu Endteilnehmer-Zertifikaten MÜSSEN eine Gültigkeit von mindestens 8 Stunden jedoch maximal 10 Tagen haben. Nach einer Sperrung eines Endteilnehmerzertifikats MUSS innerhalb von 60 Minuten eine aktualisierte Auskunft im OCSP-Responder abrufbar sein.

[QCP] Es DARF ein Gültigkeitsende (nextUpdate) gesetzt werden, die Angabe ist nicht verpflichtend.

Die einmal auf OCSP-Anfragen erstellten OCSP-Antworten DÜRFEN im OCSP-Responder vorgehalten und innerhalb ihrer Gültigkeit für weitere Anfragen wiederverwendet werden, solange sich der Status des angefragten Zertifikats nicht geändert hat.

[SSL] Für die Wiederverwendung vorhandener noch gültiger OCSP-Antworten gelten folgende Bedingungen:

- Falls die OCSP-Antworten eine Gültigkeit von weniger als 16 Stunden haben, DÜRFEN diese nach Ablauf der Hälfte ihrer Gültigkeit NICHT mehr wiederverwendet werden.
- Falls die OCSP-Antworten eine Gültigkeit von 16 Stunden oder mehr haben, DÜRFEN diese NICHT länger als 4 Tage nach ihrer Ausstellung und länger als 8 Stunden vor Ablauf Ihrer Gültigkeit wiederverwendet werden.

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

Alle Sperrlisten MÜSSEN über den Zeitpunkt der nächsten regelmäßigen Aktualisierung hinaus gültigen sein.

Sperrlisten, die Auskunft über gesperrte Sub-CAs geben, DÜRFEN eine Gültigkeit von 12 Monaten NICHT überschreiten.

Sperrlisten, die Auskunft über gesperrte Endteilnehmerzertifikate geben, DÜRFEN eine Gültigkeit von 10 Tagen NICHT überschreiten.

Die Gültigkeitsdauer einer letzten Sperrliste zu den Zertifikaten ihres Anwendungsbereichs SOLLTE auf den Wert „99991231235959Z“ gesetzt werden.

Gesperrte Zertifikate DÜRFEN grundsätzlich nach ihrem Gültigkeitsende aus der Sperrliste entfernt werden, sie MÜSSEN jedoch noch Kap. 4.10.1.2in der nächsten regulären Sperrliste nach ihrem Gültigkeitsende enthalten sein.

[QCP] Wenn Sperrlisten bereitgestellt werden, Kap. 4.10.2abgelaufene Zertifikate nicht aus der Sperrliste entfernt werden.

4.10.2 Verfügbarkeit

Der Zertifikatsstatusdienste MÜSSEN 7x24h zur Verfügung zu stehen. Im Falle von Störungen MÜSSEN größtmögliche Bemühungen unternommen werden, die Störungen innerhalb der vereinbarten Entstörungsfristen zu beheben.

Es MÜSSEN ausreichende Kapazitäten zur Verfügung gestellt werden, so dass die Antwortzeit unter normalen Betriebsbedingungen 10 Sekunden nicht überschreitet.

[EVCP] Es MÜSSEN ausreichende Kapazitäten zur Verfügung gestellt werden, so dass die Antwortzeit unter normalen Betriebsbedingungen 3 Sekunden nicht überschreitet.

[3145] [NCP] Die TSP MÜSSEN in ihren CPS die maximale Ausfallzeit der Systeme aufführen.

4.10.3 Optionale Merkmale

Keine Vorgabe.

4.11 Kündigung durch den Endteilnehmer

Keine Vorgabe.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und-Praktiken

Wenn ein TSP eine Schlüsselhinterlegung anbietet, so

- DÜRFEN Verschlüsselungsschlüssel hinterlegt werden,
- DÜRFEN Authentisierungsschlüssel und Signaturschlüssel NICHT in einer Form hinterlegt werden, die ein Entschlüsseln dieser Schlüssel ohne Kontrolle des Zertifikatsinhabers ermöglichen,
- MUSS der TSP sicherstellen, dass alle Kopien der privaten Schlüssel unter dem gleichen Sicherheitslevel aufbewahrt werden wie das Original und nur an autorisierte Empfänger herausgegeben werden,
- DÜRFEN NICHT mehr Kopien der privaten Schlüssel erzeugt werden, wie für die Sicherstellung der Kontinuität erforderlich sind,
- DARF ein privater Schlüssel, den der TSP oder eine festgelegte Rolle zur Entschlüsselung der hinterlegten Schlüssel nutzt, nicht zu anderen Zwecken genutzt werden.

4.12.2 Richtlinien und Praktiken für die Kapselung und Wiederherstellung von Sitzungsschlüsseln

Keine Vorgabe.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE REGELUNGEN

Die TSP MÜSSEN in einer vom Management freigegebenen Informationssicherheitsrichtlinie den Ansatz zum Management der Informationssicherheit festlegen und MÜSSEN über ein geeignetes Informationssicherheits-Management-System (ISMS, z.B. in Anlehnung an ISO 27001) verfügen, welches unter anderem

- die Entwicklung, Einführung und Aufrechterhaltung der Sicherheitskonzepte inkl. regelmäßiger Risikoanalysen zu den Diensten der TSP managt,
- die Informationen inventarisiert und gemäß dem Risikomanagement klassifiziert,
- in das Changemanagement zu sicherheitskritischen Änderungen involviert ist und
- eine regelmäßige Auditierung der Dienste der TSP vorsieht.

[VS-NfD] Bevor IT-Systeme für VS-NfD eingesetzt werden, MÜSSEN diese bzgl. der Einhaltung der erforderlichen Geheimschutzmaßnahmen gemäß [VSA] überprüft werden.

Die Sicherheitskonzepte MÜSSEN die folgenden Anforderungen erfüllen:

- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Zertifikatsdaten und des Zertifikatsmanagements-Prozesses.
- Schutz gegen mögliche Bedrohungen und Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses.
- Schutz gegen unautorisierten oder ungerechtfertigten Zugriff, Nutzung, Veröffentlichung, Auswechselung oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses.
- Schutz gegen Verlust oder mutwillige Zerstörung von Zertifikatsdaten oder Manipulationen im Zertifikatsmanagement-Prozess.
- Einhaltung von gesetzlich geforderten Sicherheitsanforderungen.

Die Sicherheitskonzepte MÜSSEN insbesondere folgende Aspekte berücksichtigen:

- Physikalische Sicherheit (Gebäude und Umfeld),
- Netzwerksicherheit und Firewallmanagement,
- Integritätssicherung der Systeme (inkl. Konfigurationsmanagement) sowie der verwendeten vertrauenswürdigem Codes,
- Malware-Erkennung und Verhinderung,
- Benutzer- und Rollenmanagement inkl. der Prozesse zur Vergabe vertrauenswürdiger Rollen
- Schulung, Sensibilisierung und Fortbildung der Mitarbeiter,
- Logische Zugriffskontrolle,
- Protokollierung und
- automatische Sperrung der Arbeitsplätze bei Inaktivität.

Es MÜSSEN jährlich Risikoanalysen durchgeführt werden, welche die vorhersehbaren internen und externen Bedrohungen die zu einem unautorisierten Zugriff, Veröffentlichung, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können, identifiziert, analysiert und bewertet.

Die Risikoanalysen MÜSSEN die Wahrscheinlichkeiten und die potenziellen Schäden dieser Bedrohungen unter Berücksichtigung der Sensibilität der Zertifikatsdaten und des

Zertifikatsmanagement-Prozesses betrachten und die Angemessenheit der Richtlinien, Verfahren, Informationssysteme, Technologien und weiterer Vorkehrungen bewerten, die getroffen wurden, um den Bedrohungen entgegenzuwirken.

Auf Basis der Bewertung der Risiken MÜSSEN geeignete, angemessene Risikobehandlungsmaßnahmen (z.B. bauliche, organisatorische, personelle sowie dem Stand der Technik entsprechende technische Sicherheitsmaßnahmen) entwickelt und deren Umsetzung im ISMS gemanagt und kontrolliert werden.

Die Risikobewertung sowie ggf. identifizierte Restrisiken müssen vom Management der TSP genehmigt werden.

5.1 Physikalische Maßnahmen

Die TSP MÜSSEN physikalische Maßnahmen treffen um Verlust, Diebstahl, Schaden oder Kompromittierung von Anlagen, Medien und Informationen zu vermeiden.

5.1.1 Standort und Bauweise

Die TSP MÜSSEN ihre Systeme an geeigneten Standorten in sicheren Räumlichkeiten mit hinreichendem physikalischem Schutz betrieben und bei der Wahl der Standorte mögliche Naturkatastrophen (z.B. Hochwasser) sowie die Wiederherstellung nach Katastrophen berücksichtigen.

Wenn Räumlichkeiten mit anderen Organisationen geteilt werden, die nicht zum TSP gehören, MÜSSEN die nicht zum TSP gehörenden Systeme außerhalb des Bereichs betrieben werden, in dem die CA- und Statusdienst-Systeme des TSP betrieben werden. Die verschiedenen Bereiche MÜSSEN durch geeignete physikalische Barrieren voneinander getrennt sein.

Die Systeme der TSP DÜRFEN gemäß der sich aus der Risikobewertung ergebenden Kritikalität oder den an sie gestellten Sicherheitsanforderungen in unterschiedlichen Sicherheitszonen betrieben werden, wobei insbesondere die Systeme der Root-CA in einer hochsicheren Zone betrieben werden MÜSSEN.

[VS-NfD] Die Hinweise für den Schutz von VSIT-Räumen nach § 29 VSA [VSIT] MÜSSEN als Anleitung berücksichtigt werden.

5.1.2 Physikalischer Zutritt

Der Zugang zu den Räumlichkeiten, in denen die Systeme der TSP betrieben werden, MUSS über geeignete Zugangskontrollen auf die zutrittsberechtigten Personen in vertrauenswürdigen Rollen beschränkt werden. Sofern nicht-autorisierte Personen Zutritt zu diesen Räumlichkeiten benötigen, MÜSSEN diese immer durch eine autorisierte Person begleitet werden.

Die Räumlichkeiten, in denen die Systeme der TSP betrieben werden, MÜSSEN über eine Alarmierung zur Erkennung von unautorisierten Zutritten verfügen.

Die erteilten Zutrittsberechtigungen MÜSSEN regelmäßig überprüft werden.

5.1.3 Stromversorgung und Klimatisierung

Es MUSS eine unterbrechungsfreie Stromversorgung sowie Klimatisierung der Systeme entsprechend der sich aus der Risikobewertung ergebenden Kritikalität sowie der vereinbarten Service-Level gewährleistet sein.

5.1.4 Wassereinwirkung

Die Räume in denen Komponenten des TSP betreiben werden, MÜSSEN entsprechend der sich aus der Risikobewertung ergebenden Kritikalität vor Wassereinwirkung geschützt werden.

5.1.5 Brandvorsorge und Brandschutz

Die Räume in denen Komponenten des TSP betreiben werden, MÜSSEN entsprechend der sich aus der Risikobewertung ergebenden Kritikalität vor Zerstörung durch Feuer geschützt werden.

5.1.6 Aufbewahrung von Medien

Es MÜSSEN Maßnahmen zum Schutz vor unbeabsichtigter Verwendung außerhalb der gesicherten Umgebung, Beschädigung, Diebstahl, unbefugtem Zugriff und Veralterung der relevanten Medien der TSP getroffen werden. Bei diesen Maßnahmen MUSS die Aufbewahrungsfrist der Medien berücksichtigt werden. Alle Medien MÜSSEN entsprechend der Klassifizierung der darauf gespeicherten Informationen sicher behandelt werden.

5.1.7 Abfallentsorgung

Die TSP MÜSSEN zur Verhinderung der unbefugten Nutzung oder des unbefugten Zugriffs auf Informationen sichere Entsorgungsprozesse etablieren. Insbesondere Medien, die sensible Daten enthalten, MÜSSEN sicher entsorgt werden, wenn sie nicht mehr benötigt werden.

5.1.8 Offsite Sicherung

Keine Vorgabe.

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Zur Gewährleistung eines sicheren Betriebs MÜSSEN die TSP über eine geeignete Organisation verfügen, in der mindestens die folgenden vertrauenswürdigen Rollen abgebildet sind:

- Leiter TSP: trägt die gesamte Verantwortung für die Dienste des TSP
- Sicherheitsbeauftragter: plant und überwacht die Implementierung von Sicherheitsmaßnahmen
- Registrierungsmitarbeiter: prüft und bearbeitet Anträge zur Zertifikatsausstellung, -Suspendierung, -Sperrung oder Verlängerung
- Administrator: konfiguriert und wartet die IT-Struktur einschließlich der Netzwerke, Datenbanken und Server
- CA Operator: generiert Root- und CA-Schlüssel und -Zertifikate und richtet technisch die Zugriffsrechte für die Mitarbeiter der RA (bei mehrstufigen RA-Konzepten die oberste Instanz der RA) ein.
- interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten z.B. Protokolldaten, Datenbanken und papierbasierte Dokumentationen des TSP

[SSL] Ergänzend zu den o.g. Rollen MÜSSEN die TSP die Rolle des Validierungsspezialisten etablieren.

Die TSP MÜSSEN die relevanten Rollen des TSP incl. einer Übersicht der zugewiesenen Tätigkeiten im CPS beschreiben.

Wenn vertrauenswürdige Rollen oder Teile davon an Dritte übertragen werden (z.B. externe RAs, siehe Kap. 1.3.2), MÜSSEN vom TSP die Verantwortlichkeiten und Regelungen klar definiert und entsprechende Vereinbarungen mit den Dritten getroffen werden, um sicherzustellen, dass alle vom TSP vorgegebenen Regelungen auch von den Dritten eingehalten werden.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Für alle in Kap. 5.2.1 aufgeführten Rollen MUSS mindestens ein Vertreter benannt werden.

Sicherheitsrelevante oder -kritische Tätigkeiten, wie z.B. Generierung, Sicherung und Wiederherstellung von Root-CA oder CA-Schlüsseln, MÜSSEN im Vier-Augen-Prinzip durch Personen in vertrauenswürdigen Rollen durchgeführt werden. Die Anzahl der Mitarbeiter, die solche sicherheitsrelevanten oder -kritischen Tätigkeiten ausüben, MUSS auf ein Minimum beschränkt sein.

[EVCP] Zertifikatsanträge für Endteilnehmerzertifikate MÜSSEN im Vier-Augen-Prinzip validiert und freigegeben werden. Die TSP MÜSSEN auditierbare Sicherheitsmaßnahmen zur Sicherstellung des Vier-Augen-Prinzips umsetzen.

Die TSP MÜSSEN die sicherheitsrelevanten und -kritischen Tätigkeiten, für die ein Vier-Augen-Prinzip (oder mehr) benötigt wird, im CPS beschreiben.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Die Identifizierung geeigneter Personen zur Besetzung von Rollen, die Übertragung der Rollen (Authentifizierung) sowie deren Entzug MÜSSEN nach einem dokumentierten Prozess erfolgen.

Vor der Übertragung einer vertrauenswürdigen Rolle MÜSSEN vom Management des TSP und von der Person, der diese Rolle übertragen werden soll, die Akzeptanz zur Übertragung der Rolle und der damit verbundenen Verantwortung sowie den daraus resultierenden Pflichten zur Gewährleistung der Sicherheit eingeholt werden.

Die Rolleninhaber MÜSSEN vom Management des TSP offiziell in die vertrauenswürdige Rolle berufen werden.

Darüber hinaus MUSS sichergestellt werden, dass durch die Übertragung einer Rolle keine Interessenskonflikte entstehen und die Unabhängigkeit gewahrt ist, d.h. dass

- die Bereiche des TSP, die mit der Generierung und Sperrung von Zertifikaten betraut sind, bei ihren Entscheidungen über die Einrichtung, Bereitstellung, Aufrechterhaltung und Aussetzung von Diensten in Übereinstimmung mit den geltenden Zertifikatsrichtlinien unabhängig von anderen Organisationen sein MÜSSEN,
- alle Mitarbeiter, die mit der Generierung und Sperrung von Zertifikaten betraut sind, in der Ausübung ihrer Tätigkeit frei von finanziellem oder anderem Druck sein MÜSSEN, der das Vertrauen in die vom TSP erbrachten Dienstleistungen beeinträchtigen könnte. Dies gilt sowohl für alle Mitarbeiter in vertrauenswürdigen Rollen als auch für die leitenden Angestellten und Führungskräfte.

Die TSP MÜSSEN diese Struktur, die die Unparteilichkeit des Betriebs gewährleistet, dokumentieren.

Die Rolleninhaber MÜSSEN darauf hingewiesen werden, dass Sie nur in der zugewiesenen Rolle handeln dürfen, wenn Sie Aufgaben ausführen, die der Rolle zugewiesen sind.

Die Vergabe der erforderlichen Berechtigungen MUSS nach dem „Least Privilege“-Prinzip erfolgen, d.h. alle Berechtigungen MÜSSEN auf das erforderliche Minimum beschränkt werden.

Nach Beendigung des Arbeitsverhältnisses eines Mitarbeiters in einer vertrauenswürdigen Rolle MÜSSEN dessen Zugriffsberechtigungen innerhalb von 24 Stunden entzogen werden.

[EVCP] Die Identifizierung von Personen, die mit einer vertrauenswürdigen Rolle betraut werden sollen, MUSS persönlich unter Vorlage eines amtlichen Ausweises erfolgen.

Wenn vertrauenswürdige Rollen oder Teile davon an Dritte übertragen werden (z.B. externe RAs, siehe Kap. 1.3.2), MÜSSEN vom TSP die Verantwortlichkeiten und Regelungen klar definiert und entsprechende Vereinbarungen mit den Dritten getroffen werden, um sicherzustellen, dass alle vom TSP vorgegebenen Regelungen auch von den Dritten eingehalten werden.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Es MÜSSEN folgende Rollen voneinander getrennt werden:

- Management des TSP,
- IT-Sicherheitsbeauftragter und/oder interner Auditor,

- RA,
- Administrator und/oder CA-Operator.

Darüber hinaus DÜRFEN die Personen in o.g. Rollen NICHT gleichzeitig auch Antragsteller für Endteilnehmerzertifikate sein, ausgenommen davon sind Anträge für eigene Zertifikate des TSP sowie Zertifikate für die Mitarbeiter des TSP. Die Ausnahmen MÜSSEN die TSP in ihren CPS beschreiben.

5.3 Personelle Maßnahmen

5.3.1 Qualifikationen, Erfahrung und Freigaben

Das Management der TSP MUSS über

- Erfahrung oder Schulung in Bezug auf die angebotenen Dienste des TSP,
- Vertrautheit mit Sicherheitsverfahren für Personal mit Sicherheitsverantwortung und
- Erfahrung mit Informationssicherheit und Risikobewertung, die ausreicht, um Managementfunktionen auszuführen

verfügen.

Die TSP MÜSSEN vor der Einstellung einer Person deren Identität und Vertrauenswürdigkeit überprüfen.

Die Mitarbeiter der TSP MÜSSEN aufgrund ihrer Erfahrung und/oder geeigneten Schulungen über hinreichendes Expertenwissen und Qualifikationen für die Ausübung ihrer Tätigkeit verfügen. Darüber hinaus MÜSSEN die Mitarbeiter für die Ausübung ihrer Tätigkeit angemessen zu allgemeinen Sicherheits- und Datenschutzbestimmungen sowie den konkreten Vorgaben des ISMS des TSP geschult sein.

5.3.2 Verfahren zur Hintergrundprüfung

Keine Vorgabe.

[EVCP] Die TSP MÜSSEN sicherstellen, dass Personal, welches mit einer vertrauenswürdigen Rolle betraut werden soll, erfolgreich eine Hintergrundüberprüfung absolviert hat, in der

- die vorherige Beschäftigung,
- die beruflichen Referenzen,
- der Bildungsabschluss sowie
- ein amtliches Führungszeugnis

geprüft wurden.

[3145] [VS-NfD] Die TSP MÜSSEN sicherstellen, dass Personen, welche mit kritischen oder sicherheitsrelevanten Prozessen betraut werden sollen, erfolgreich eine Sicherheitsüberprüfung absolviert haben. Sollte sich bei der Sicherheitsüberprüfung herausstellen, dass eine Person für eine Straftat, welche seine Eignung für die vorgesehene Rolle beeinträchtigt, verurteilt worden ist, DARF diese Person NICHT mit dieser Rolle betraut werden.

[VS-NfD] Die o.g. Sicherheitsüberprüfung nach [3145] MUSS mindestens gemäß [SÜG] Level Ü2/Sabotageschutz absolviert werden.

5.3.3 Schulungsanforderungen

Keine Vorgabe (siehe dazu Kap. 5.3.1).

[SSL] Die TSP MÜSSEN alle mit der Validierung der Zertifikatsanträge betrauten Mitarbeiter zu folgenden Themen schulen (lassen):

- grundlegende Kenntnisse zu PKI, Authentifizierungs- und Überprüfungsrichtlinien und -verfahren,
- allgemeine Bedrohungen für den Informationsüberprüfungsprozess, einschließlich Phishing und Social-Engineering,
- relevante CP und/oder CPS sowie die [BR].

Die TSP MÜSSEN Nachweise zu diesen Schulungen führen und dokumentieren, dass jeder mit der Validierung betraute Mitarbeiter über das erforderliche Know-How verfügt, bevor dieser die Tätigkeiten übernimmt.

Darüber hinaus MÜSSEN die TSP von allen Validierungsspezialisten verlangen, dass sie eine von der Zertifizierungsstelle bereitgestellte Prüfung der in den [BR] aufgeführten Anforderungen zur Überprüfung von Informationen bestehen.

5.3.4 Nachschulungsintervalle und -anforderungen

Die TSP SOLLTEN ihre Mitarbeiter regelmäßig (mindestens jährlich) zu aktuellen Bedrohungen und Sicherheitspraktiken schulen.

Die TSP MÜSSEN durch geeignete regelmäßige Schulungen sicherstellen, dass Personal in vertrauenswürdigen Rollen das erforderliche Know-How dauerhaft aufrechterhält.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Keine Vorgabe.

5.3.6 Sanktionen bei unbefugten Handlungen

Das Personal der TSP MUSS rechenschaftspflichtig für sein Handeln sein. Es MÜSSEN angemessene Sanktionen gegen Personen, die gegen die Vorgaben des TSP verstoßen, verhängt werden.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Die in Kap. 5.3 aufgeführten Anforderungen gelten, sofern anwendbar, analog für vom TSP beauftragte Dritte.

[SSL] Die TSP MÜSSEN überprüfen, ob das an der Ausstellung von Zertifikaten beteiligte Personal von Dritten die Schulungs- und Qualifikationsanforderungen gemäß Kap. 5.3.3 sowie die Anforderungen für die Aufbewahrung von Dokumenten und die Protokollierung von Ereignissen gemäß Kap. 5.4.1 erfüllen.

[3145] Die TSP MÜSSEN gegenüber beteiligten Dritten deren Verantwortlichkeiten sowie die relevanten Praktiken klar definieren und geeignete Vorkehrungen treffen, um sicherzustellen, dass diese von den Dritten umgesetzt werden.

5.3.8 Dokumentation, die dem Personal zur Verfügung gestellt wird.

Den Rolleninhabern MÜSSEN Rollenbeschreibungen zur Verfügung gestellt werden, die neben den sich aus der Rolle ergebenden Verantwortungen und Pflichten mindestens die erforderlichen

- (minimalen) Berechtigungen,
- Aufgabentrennungen,
- Vier-Augen-Prinzipien,
- Hintergrundprüfungen sowie
- Schulungs- und Sensibilisierungsmaßnahmen

enthalten.

Wo erforderlich, MÜSSEN diese Rollenbeschreibungen zwischen allgemeinen Rollen und TSP-spezifischen Rollen unterscheiden.

5.4 Protokollierungsverfahren

5.4.1 Arten von Ereignissen, die protokolliert werden

5.4.1.1 Aktivitäten von Personen

Die TSP MÜSSEN die folgenden Aktivitäten der Mitarbeiter des TSP sowie der externen RAs aufzeichnen:

- Alle Aktivitäten im Zusammenhang mit der Bearbeitung von Anträgen auf Ausstellung, Erneuerung und Sperrung von Zertifikaten,
- Alle Aktivitäten im Zusammenhang mit dem Lebenszyklus von Root- und CA-Zertifikaten und -Schlüsseln, dazu zählen mindestens Schlüsselgenerierung, -Speicherung, -Backup, -Wiederherstellung, -Archivierung und -Zerstörung, Generierung und Sperrung der Root- und CA-Zertifikate sowie der Lebenszyklus der HSM.

[SSL] Ergänzend zu obiger Auflistung MÜSSEN die TSP folgende Aktivitäten aufzeichnen:

- Validierungen gemäß den [BR],
- Telefongespräche (Datum, Uhrzeit, Telefonnummer, Gesprächspartner, Ergebnisse), sofern diese im Rahmen der Validierungsaktivitäten erfolgt sind.

[QCP-n-qscd] [QCP-l-qscd] Ergänzend zu obiger Auflistung MÜSSEN die TSP alle Ereignisse im Zusammenhang mit der Erstellung von QSCDs aufzeichnen.

5.4.1.2 Technische Systemereignisse

Die TSP MÜSSEN die folgenden technischen Ereignisse inkl. Angabe der präzisen Zeit, der Identität des Auslösers (sofern anwendbar) und der Beschreibung des Ereignisses protokollieren:

- alle wesentlichen Ereignisse im Zertifikats- und Schlüsselmanagement,
- alle Sicherheitsereignisse an den Systemen, insbesondere Änderungen der Sicherheitsrichtlinien der Systeme, das Starten und Herunterfahren der Systeme, Systemabstürze und Hardwarefehler, Uhrzeitsynchronisationsereignisse, Firewall- und Router-Aktivitäten sowie PKI-Systemzugriffsversuche.

Hinweis: Die Zeit, die zum Aufzeichnen der o.g. Ereignisse verwendet wird, muss mindestens einmal täglich synchronisiert werden (UTC).

[SSL] Die TSP SOLLTEN OCSP-Anfragen zu nicht vergebenen Seriennummern protokollieren.

Darüber hinaus MÜSSEN die TSP alle (physikalischen) Ein- und Ausgänge zu den Sicherheitszonen protokollieren. Die Protokolleinträge MÜSSEN mindestens das Datum und die Uhrzeit des Eintrags, einen Verweis auf die Person oder das System, welches den Eintrag generiert hat, sowie eine Beschreibung des Ereignisses enthalten.

5.4.2 Häufigkeit der Log-Verarbeitung

Die in Kap. 5.4.1 aufgeführten Ereignisse MÜSSEN kontinuierlich protokolliert werden.

Die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten MÜSSEN nur im Bedarfsfall ausgewertet werden, z.B. bei Problemmeldungen, in Gerichtsverfahren oder auf Anfrage interner und externer Auditoren).

Die Logdaten zu den in Kap. 5.4.1.2 aufgeführten Ereignissen MÜSSEN wie folgt ausgewertet werden:

- Sicherheitsrelevante Ereignissen MÜSSEN wie in Kap. 6.6.2 beschrieben ausgewertet werden,
- alle anderen Logdaten MÜSSEN nur im Bedarfsfall ausgewertet werden, z.B. bei Fehlerbehebungs- oder Analysetätigkeiten.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten MÜSSEN unter Berücksichtigung der Datenschutzvorgaben vom TSP über einen angemessenen Zeitraum aufbewahrt werden, der sowohl zur Gewährleistung der Kontinuität der Dienste des TSP als auch ggf. aufgrund gesetzlicher Bestimmungen erforderlich ist. Die TSP MÜSSEN die Aufbewahrungsdauern in ihren CPS beschreiben, siehe dazu auch Kap. 5.5.2.

Diese Pflicht zur Aufbewahrung gilt auch über die Beendigung eines Dienstes oder des TSP hinaus. Im Beendigungsplan MUSS daher festgelegt werden, welche Informationen wohin übergeben werden und wie auf diese Informationen zugegriffen werden kann, siehe dazu auch Kap. 5.8.

5.4.4 Schutz der Audit-Protokolle

Die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten MÜSSEN vertraulich und integritätsgesichert aufbewahrt und so geschützt werden, dass diese nicht einfach zerstört oder gelöscht werden können. Die TSP MÜSSEN in ihren CPS beschreiben, wie der Schutz dieser Aufzeichnungen sichergestellt wird.

[SSL] [SMIME] Die TSP MÜSSEN die Aufbewahrung der Aufzeichnungen überwachen (z.B. in internen Audits).

[3145] Die TSP MÜSSEN die technischen Systemereignisse gemäß Kap. 5.4.1.2 in einem separaten manipulationssicheren System, d.h. nicht nur in dem System, in dem die Ereignisse protokolliert werden, speichern.

5.4.5 Backup-Verfahren für Audit-Protokolle

Die TSP MÜSSEN Sicherungsverfahren festlegen, die erforderlich sind, um die in Kap. 5.4.4 aufgeführten Schutzziele über die in Kap. 5.4.3 aufgeführten Aufbewahrungszeiträume zu erreichen.

5.4.6 Audit-Sammelsystem

Keine Vorgabe.

[3145] Die Protokolldateien SOLLTEN nicht auf den Servern gespeichert werden, die nur für die Verwaltung der Zertifikate verwendet werden. Sie SOLLTEN über eine gesicherte Verbindung auf Server exportiert werden, die für die Speicherung von Protokolldateien vorgesehen sind. Dessen Datenbank MUSS so gestaltet sein, dass Einträge nur hinzugefügt, jedoch nicht gelöscht werden können, die Größe der Datenbank MUSS dementsprechend ausgelegt sein.

5.4.7 Benachrichtigung der Person, die ein Ereignis ausgelöst hat

Keine Vorgabe.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Vorgabe.

5.5 Archivierung von Aufzeichnungen

[3145] Die TSP MÜSSEN die Aufzeichnungen so archivieren, dass sie in der Lage sind, alle ausgestellten Zertifikate eindeutig einem registrierten Antragsteller zuordnen zu können.

Darüber hinaus MUSS eine Nachverfolgung möglich sein, um zu verhindern, dass betrügerische oder manipulierte Zertifikate erzeugt werden.

5.5.1 Art der archivierten Datensätze

Die TSP MÜSSEN mindestens folgende Daten archivieren:

- alle Registrierungsinformationen, einschließlich
  - der vom Antragsteller im Rahmen der Beantragung einer Ausstellung, Sperrung oder Verlängerung vorgelegte Dokumente,
  - falls zutreffend der Identifikationsdaten von Identifikationsdokumenten,
  - dem Aufbewahrungsort der Kopien von Anträgen (inkl. erforderlicher Anlagen) und Ausweisdokumenten
  - spezifische Wünsche im Antrag, (wie z. B. Zustimmung zur Veröffentlichung des Zertifikats),
  - falls vorhanden die Methode zur Validierung von Ausweisdokumenten,
  - die Identität der RA (inkl. des RA-Mitarbeiters), die den Antrag geprüft, freigegeben oder abgelehnt hat.
- alle wesentlichen Ereignisse zum Lebenszyklus der Zertifikate (Beantragung, Prüfung, Freigabe, Ablehnung, Ausstellung, Akzeptanz, Sperrung, Erneuerung, Anpassung)
- alle veröffentlichten CP bzw. CPS,
- Zertifizierungsunterlagen und Auditberichte,
- ggf. weitere Informationen, die zur Gewährleistung der Kontinuität der Dienste erforderlich sind.
- ggf. weitere Informationen, die vom TSP ausgegeben und empfangen wurden, und als Beweismittel in Gerichtsverfahren benötigt werden könnten.

Die TSP DÜRFEN unter Berücksichtigung der relevanten Datenschutzaspekte weitere Daten archivieren und MÜSSEN in ihrem CPS sowie den Nutzungsbedingungen beschreiben, welche Daten archiviert werden.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die TSP MÜSSEN die Daten zu einem Zertifikat für mindestens 7 Jahre nach Ablauf der Gültigkeit des Zertifikats archivieren und MÜSSEN den Aufbewahrungszeitraum (ggf. je Zertifikatstyp) in ihrem CPS sowie den Nutzungsbedingungen beschreiben.

5.5.3 Schutz von Archiven

Die in Kap. 5.5.1 aufgeführten Informationen MÜSSEN vertraulich und integritätsgesichert aufbewahrt und so geschützt werden, dass diese nicht einfach zerstört oder gelöscht werden können. Die TSP MÜSSEN in ihren CPS beschreiben, wie der Schutz der archivierten Informationen sichergestellt wird.

[EVCP] Die TSP MÜSSEN die Archivierung der Informationen überwachen (z.B. in internen Audits).

5.5.4 Backup-Verfahren für Archive

Die TSP MÜSSEN Sicherungsverfahren festlegen, die erforderlich sind, um die in Kap. 5.5.3 aufgeführten Schutzziele über die in Kap. 5.5.2 aufgeführten Zeiträume zu erreichen.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Alle in Kap. 5.5.1 aufgeführten wesentlichen Ereignisse zum Lebenszyklus der Zertifikate MÜSSEN mit Angabe von Datum und Uhrzeit archiviert werden.

5.5.6 Archivsystem (intern oder extern)

Keine Vorgabe.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Die in Kap. 5.5.1 aufgeführten archivierten Daten sowie die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten MÜSSEN im Bedarfsfall (z.B. bei Problemmeldungen oder in Gerichtsverfahren) geprüft und ggf. als Beweismittel herausgegeben werden und MÜSSEN auf Anfrage internen und externen Auditoren zur Verfügung gestellt werden.

5.6 Schlüsselwechsel

Vor Ablauf eines CA-Zertifikats MÜSSEN die TSP, sofern sie ihre Dienste fortsetzen wollen, rechtzeitig ein neues CA-Zertifikat gemäß den aktuellen Versionen dieser CP und dem CPS des TSP beantragen. Die TSP SOLLTEN dabei den Zeitraum zwischen der Veröffentlichung des neuen CA-Zertifikats und der Außerbetriebnahme des ablaufenden CA-Zertifikats hinreichend groß wählen, so dass für die Endteilnehmer keine Unterbrechung in deren Betrieb entsteht.

5.7 Kompromittierung und Notfall-Wiederherstellung

5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

Die TSP MÜSSEN die Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen sowie zur Wiederherstellung nach Ausfällen oder Katastrophen in ihrer Notfalldokumentation beschreiben.

Die Notfalldokumentation MUSS folgende Aspekte beinhalten:

- Notfallvorsorge
  - Vorgaben zum Backup kritischen kryptografischen Materials an einem anderen Standort,
  - Vorgaben zum regelmäßigen Backup aller relevanten Daten des TSP, die zur Wiederaufnahme des CA-Betriebs nach einem Notfall erforderlich sind, an sicheren, vorzugsweise entfernt auseinander liegenden Orten,
  - Entfernung des Hauptstandorts zu den Standorten, die zur Wiederherstellung des Geschäftsbetriebs genutzt werden können,
- Benennung aller beteiligten Rollen und Eskalationsstufen,
- Verantwortung aller Beteiligten,
- Voraussetzungen, unter denen aus einem Vorfall ein Notfall wird,
- Notfallprozesse,
- Rückfall-Prozesse,
- Wiederaufnahmeverfahren,
- Prozesse zur Meldung
  - von Sicherheitsverletzungen an die zuständigen Behörden oder sonstige relevanten Beteiligten,
  - von Sicherheitsverletzungen, die sich nachteilig auf natürliche oder juristische Person auswirken, an die betroffenen Personen (unverzüglich),
  - von Datenschutzvorfällen an die zuständigen Behörden oder sonstige relevanten Beteiligten (innerhalb von 24 Stunden),
- Entscheidungsmöglichkeiten zum Umgang mit gefundenen Schwachstellen (Minderung oder begründete Akzeptanz)
- Zielvorgaben zur Behebung kritischer Schwachstellen (innerhalb 48 Stunden)
- Zielvorgaben für die Wiederherstellungszeit,
- Nachbereitung inkl. Ursachenermittlung zur Vermeidung von Wiederholungen,
- Reviewzyklen des Notfallplans (mindestens jährlich),
- Sensibilisierungs- und Schulungsanforderungen,
- Regelmäßige Notfallübungen (mindestens jährlich),
- Plan zur Wiederherstellung des Betriebs nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse,
- Festlegung akzeptabler Ausfall- und Wiederherstellungszeiten,
- Planungsunterlagen für die Sicherung der Geschäftsräume während eines Desasters und der Wiederherstellung an diesem Standort oder an einem anderen Standort.
- Verfahren zur größtmöglichen Sicherung des beeinträchtigten Standorts während des Zeitraums nach einer Katastrophe und vor der Wiederherstellung am ursprünglichen oder an einem anderen Standort.

Die TSP MÜSSEN ihre Notfalldokumentation den Auditoren auf Anfrage offenlegen.

[VS-NfD] Der Notfallplan MUSS vom Sicherheitsbeauftragten freigegeben werden.

Die TSP MÜSSEN Verfahren zur Meldung von Vorfällen festlegen und sicherstellen, dass diese den Mitarbeitern bekannt sind und genutzt werden.

[SSL] [SMIME] Die TSP MÜSSEN Verstöße gegen die Mozilla Root Store Policy unverzüglich in Form eines Vorfallberichts („Bugzilla“) an Mozilla melden und SOLLTEN die Ausgabe der betroffenen Zertifikatstypen einstellen, bis die Ursache für den Verstoß behoben ist.

Die TSP MÜSSEN zur Minimierung möglicher Schäden in angemessener Zeit auf Vorfälle, die von Personen gemeldet werden und auf Alarme, die von den Systemen gemeldet werden (siehe Kap. 6.6.2) reagieren. Potenziell sicherheitskritischen Vorfällen MUSS unverzüglich durch Mitarbeiter in vertrauenswürdigen Rollen nachgegangen werden.

5.7.2 Wiederherstellung bei Beschädigung von Computern, Software oder Daten

Siehe Kap. 5.7.1.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

Die TSP MÜSSEN die Kompromittierung, den Verdacht auf Kompromittierung und den Verlust eines privaten CA-Schlüssels als Notfall in ihrer Notfalldokumentation festlegen und die daraus resultierenden Aktivitäten beschreiben.

Im Falle einer Kompromittierung eines CA-Schlüssels MÜSSEN die TSP das CA-Zertifikat sperren (lassen) und alle Betroffenen (Endteilnehmer sowie alle Weiteren, mit denen die TSP Vereinbarungen getroffen haben) informieren. Darüber hinaus MÜSSEN die TSP vertrauenden Dritten die Informationen verfügbar machen und anzeigen, dass den von der betroffenen CA ausgestellten Zertifikaten und Statusauskünften nicht mehr vertraut werden kann.

[QCP] Die TSP MÜSSEN im CPS beschreiben, wie die Statusinformationen zu Endteilnehmerzertifikaten im Falle der Kompromittierung eines CA-Schlüssels bereitgestellt werden.

[3145] Im Falle des Verdachts einer Kompromittierung eines CA-Schlüssels DÜRFEN die TSP den betroffenen Schlüssel bis zur endgültigen Klärung NICHT mehr benutzen.

5.7.4 Geschäftsfortführung nach einem Notfall

Siehe Kap. 5.7.1.

5.8 Einstellung des CA oder RA Betriebes

Die TSP MÜSSEN die Vorkehrungen, die sie zur Beendigung von Diensten treffen, in den CPS beschreiben, mindestens sind das

- die Information aller Betroffenen,
- der Umgang mit Statusauskünften zu nicht abgelaufenen Zertifikaten und,
- wenn möglich, die Übertragung der Pflichten an Andere.

[QCP] Die TSP MÜSSEN im CPS beschreiben, wie Statusinformationen nach der Beendigung der Dienste des TSP bereitgestellt werden.

Die TSP MÜSSEN einen aktuellen Beendigungsplan vorhalten.

Mögliche Störungen für Endteilnehmer und vertrauende Dritte MÜSSEN durch die Einstellung der Dienste des TSP minimiert werden, insbesondere MÜSSEN die Sperr- und Statusdienste (durch andere Stellen) weitergeführt werden.

[3145] Anstelle der Fortführung der Dienste durch eine andere Stelle DARF der TSP den Betrieb aller Dienste einstellen, sofern eine sichere Einstellung aller Dienste garantiert werden kann.

Vor der Einstellung eines Dienstes MÜSSEN die TSP

- alle Betroffenen informieren (Endteilnehmer, ggf. zuständige Aufsichtsbehörden, ggf. TSP denen Cross-Zertifikate ausgestellt wurden sowie weitere Betroffene mit denen der TSP Verträge hat),
- vertrauenden Dritten die Information über die Beendigung bereitstellen,
- die Vereinbarungen mit externen RAs beenden,
- eine zuverlässige Stelle verpflichten, alle Informationen die erforderlich sind, um den Betrieb des TSP nachzuweisen, für einen angemessenen und ggf. mit den Endteilnehmern und Anderen vereinbarten Zeitraum aufzubewahren. Dazu zählen mindestens:
    - Registrierungsinformationen,
    - Zertifikatsstatusinformationen,
    - Ereignisprotokollarchive,
- die privaten CA-Schlüssel zerstören oder so außer Betrieb nehmen, dass diese nicht wiederverwendet werden können,
- die CA-Zertifikate sperren,
- ggf. ausgestellte Crosszertifikate sperren.

Die TSP MÜSSEN entweder ihr CA-Zertifikat für einen angemessenen Zeitraum nach Beendigung selbst noch bereitstellen oder eine andere Stelle dazu verpflichten.

Darüber hinaus SOLLTEN die TSP bei Einstellung eines Dienstes nach Möglichkeit Vorkehrungen treffen, um die Bereitstellung der Dienste für seine bestehenden Kunden auf einen anderen TSP zu übertragen.

[3145] Die TSP MÜSSEN alle Schlüssel, Zertifikate und Kundendaten löschen.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Alle Schlüssel MÜSSEN den in Kap. 6.1.5 und 6.1.6 aufgeführten Algorithmen, Schlüssellängen und Qualitätsanforderungen genügen. Die technischen und organisatorischen Vorgaben zur Generierung der verschiedenen Schlüssel werden nachfolgend aufgeführt.

6.1.1.1 Generierung von Root-CA-Schlüsselpaaren

Root-CA-Schlüsselpaare MÜSSEN in einem Kryptomodul gemäß Kap. 6.2.1 in der sicheren Umgebung des Trust Centers generiert werden.

Die beteiligten Rollen sowie deren Aufgaben und Verantwortlichkeiten vor, während und nach der Schlüsselzeremonie MÜSSEN festgelegt und dokumentiert sein.

Die einzelnen Schritte der Schlüsselzeremonie MÜSSEN einem festgelegten Protokoll folgen und in diesem dokumentiert werden.

Die Generierung DARF NICHT vor der Beantragung durch einen Mitarbeiter des Root-Programms und Freigabe durch den Leiter des Trust Centers oder einen von diesem benannten Vertreter erfolgen und MUSS durch mindestens zwei, von den o.g. Personen verschiedene, vertrauenswürdige Mitarbeiter des Root-TSP durchgeführt werden. Es gelten dabei folgende Anforderungen:

- Jeder der beiden Mitarbeiter MUSS Kenntnis von einem Teil der zur Schlüsselgenerierung erforderlichen Aktivierungsdaten haben und DARF NICHT Kenntnis über die kompletten Aktivierungsdaten haben.
- Die beiden Mitarbeiter MÜSSEN in unterschiedlichen Rollen agieren.

Sowohl ein interner als auch ein qualifizierter externer Auditor (siehe Kap.8.2) MÜSSEN die Schlüsselzeremonie überwachen und deren korrekte Durchführung im Protokoll bestätigen.

Darüber hinaus MUSS der externe Auditor (siehe Kap. 8.2) in seinem Bericht die Einhaltung aller Vorgaben sowie die Wahrung der Integrität und Vertraulichkeit der Schlüssel bestätigen.

6.1.1.2 Generierung von Sub-CA-Schlüsselpaaren

Sub-CA-Schlüsselpaare MÜSSEN in einem Kryptomodul gemäß Kap. 6.2.1 in der sicheren Umgebung der Sub-CA, die diese Schlüssel nutzen möchte, generiert werden.

Die beteiligten Rollen sowie deren Aufgaben und Verantwortlichkeiten vor, während und nach der Schlüsselzeremonie MÜSSEN festgelegt und dokumentiert sein.

Die einzelnen Schritte der Schlüsselzeremonie MÜSSEN einem festgelegten Generierungsprotokoll folgen und in diesem dokumentiert werden.

Die Generierung MUSS durch mindestens zwei vertrauenswürdige Mitarbeiter des TSP erfolgen, Jeder der beiden Mitarbeiter MUSS Kenntnis von einem Teil der zur Schlüsselgenerierung erforderlichen Aktivierungsdaten haben und DARF NICHT Kenntnis über die kompletten Aktivierungsdaten haben.

Zum Nachweis der Authentizität und der Integrität MUSS der Hashwert des generierten öffentlichen Schlüssels oder des Zertifikatsrequests, der den öffentlichen Schlüssel beinhaltet, im Generierungsprotokoll aufgenommen und bei der Zertifikatsbeantragung (siehe Kap. 4.1) übergeben werden.

[TSEC-CA] Die Schlüsselzeremonie MUSS durch den Produktverantwortlichen oder ein von ihm benannter Vertreter sowie einen unabhängigen Auditor überwacht werden. Es DARF sich dabei um einen erfahrenen internen Auditor der Sub-CA handeln. Wenn möglich SOLLTE ein qualifizierter externer Auditor (gemäß Kap. 8.2) hinzugezogen oder die Schlüsselzeremonie zur späteren Prüfung per Video aufgezeichnet werden. Die Einhaltung aller Vorgaben sowie die Wahrung der Integrität und Vertraulichkeit der Schlüssel MUSS durch den Auditor in dessen Bericht bestätigt werden.

[DFN-CA] Die Schlüsselzeremonie für Schlüssel, zu denen Sub-CA-Zertifikate einer Root-CA der Telekom beantragt werden sollen, MUSS von einem qualifizierten externen Auditor (gemäß Kap. 8.2) überwacht werden. Die Einhaltung aller Vorgaben sowie die Wahrung der Integrität und Vertraulichkeit der Schlüssel MUSS durch den Auditor in dessen Bericht bestätigt werden.

6.1.1.3 Generierung von RA-Schlüsselpaaren

Die TSP MÜSSEN RA Schlüsselpaare in kryptografischen Modulen gemäß Kap. 6.2.1 generieren.

6.1.1.4 Generierung von Endteilnehmer-Schlüsselpaaren

Teilnehmer-Schlüsselpaare DÜRFEN entweder durch die Sub-CA oder den Teilnehmer selbst generiert werden.

Wenn Teilnehmer-Schlüssel durch die Teilnehmer generiert werden, so muss die Sub-CA die Teilnehmer über die zu verwendenden zulässigen Algorithmen und Schlüssellängen informieren.

Wenn Teilnehmer-Schlüssel durch die Sub-CA erzeugt werden, so muss die Sub-CA die Schlüssel auf eine sichere Art und Weise generieren und bis zur Zertifikatserzeugung vorhalten, so dass die Integrität und Vertraulichkeit sichergestellt werden. Die Schlüssel MÜSSEN zum Zeitpunkt der Generierung als geeignet für die gesamte Nutzungsdauer und die Verwendungszwecke angesehen werden.

[SSL] Teilnehmer-Schlüssel, die zur Authentisierung von Servern genutzt werden können (d.h. wenn die Zertifikate zu diesen Schlüsseln die extendedKeyUsage „id-kp-serverAuth“ oder „anyExtendedKeyUsage“ enthalten sollen), DÜRFEN NICHT durch den TSP generiert werden.

[QCP] Teilnehmer-Schlüsselpaare MÜSSEN durch ein QSCD erzeugt werden.

[3145] TSP, die Teilnehmer-Schlüssel für kryptografischen Token als Speichermedium der Schlüssel generieren

- SOLLTEN die Schlüssel durch den Token selbst generieren lassen,
- MÜSSEN außerhalb des Tokens erzeugte Schlüssel sofort nach dem Einbringen in den Token löschen, sofern der TSP keine Sicherung der Teilnehmer-Schlüssel anbietet.

6.1.2 Bereitstellung der privaten Schlüssel an die Endteilnehmer

TSP, die Schlüssel der Endteilnehmer generieren, MÜSSEN folgende Vorgaben berücksichtigen:

- Die Schlüssel MÜSSEN dem Endteilnehmer so übergeben werden, dass die Wahrung der Vertraulichkeit und Integrität sichergestellt und eine unautorisierte Nutzung ausgeschlossen ist.
- Nach der Übergabe der Schlüssel an den Endteilnehmer MÜSSEN alle Kopien der Schlüssel in den Systemen des TSP gelöscht werden, es sei denn die Schlüssel sollen im Auftrag des Endteilnehmers beim TSP hinterlegt werden (siehe Kap. 6.2.3).
- Wenn die Schlüssel den Endteilnehmern mittels personalisierter sicherer kryptografischer Geräte (z.B. Smartcard) übergeben werden, so MUSS die Übergabe der Geräte und der zugehörigen Aktivierungsdaten getrennt voneinander erfolgen.

[LCP] [NCP] TSP, welche die Schlüssel der Endteilnehmer generieren, MÜSSEN diese auf sicherem Weg dem registrierten Zertifikatsinhaber übergeben, es sei denn sie verwalten die Schlüssel selbst im Auftrag des Endteilnehmers.

[NCP+] TSP, welche die Schlüssel der Endteilnehmer generieren, MÜSSEN sicherstellen, dass diese auf einem sicheren kryptografischen Gerät (z.B. Smartcard) auf sichere Art und Weise bereitgestellt werden. Die Geräte MÜSSEN auf sicherem Weg dem registrierten Zertifikatsinhaber übergeben werden, es sei denn der TSP verwaltet die Schlüssel selbst im Auftrag des Endteilnehmers. Im letztgenannten Fall MUSS der TSP sicherstellen, dass er die Schlüssel unter alleiniger Kontrolle hat.

[QCP-n-qscd] [QCP-l-qscd] TSP, welche QSCD von Endteilnehmern managen, MÜSSEN sicherstellen, dass diese unter der alleinigen Kontrolle durch den Endteilnehmer genutzt werden können.

6.1.3 Übergabe öffentlicher Endteilnehmerschlüssel an die TSP

Keine Vorgabe.

[SSL] Die TSP SOLLTEN in ihrem CPS oder in einem im CPS referenzierten Dokument das Format und die Methoden der akzeptierten elektronischen Zertifikatsrequests festlegen.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

Die TSP MÜSSEN ihre Root- und CA-Zertifikate allgemein zugänglich in integrer und authentischer Form bereitstellten. Bei Root-CA-Zertifikaten MÜSSEN zusätzlich weitere Prüfmechanismen vorgesehen werden, wie z.B. eine Prüfung des Hashwerts des Zertifikats gegen eine vertrauenswürdige Quelle.

6.1.5 Schlüssellängen

Die TSP MÜSSEN Schlüssel gemäß den nachfolgend aufgeführten Anforderungen generieren und DÜRFEN NICHT von Sub-CAs oder Endteilnehmern generierte Schlüssel akzeptieren, die nicht diesen Anforderungen genügen. Sollten die verwendeten Schlüssellängen aufgrund neuer Erkenntnisse oder Vorgaben für den Verwendungszweck nicht mehr ausreichen, so MÜSSEN die TSP ihre Sub-CAs und / oder Endteilnehmer und vertrauende Dritte darüber informieren und einen Zeitplan zur Sperrung der Zertifikate sowie zur Migration auf hinreichend lange Schlüssel festlegen.

Die Schlüssel aller Zertifikate aller Hierarchieebenen MÜSSEN den Anforderungen aus [SOGIS] genügen. Dementsprechend MÜSSEN folgende Mindestanforderungen beachtet werden:

- RSA: Die Schlüssel SOLLTEN eine Länge von mindestens 3.000 Bit haben (Recommendation gem. [SOGIS]). Schlüssel mit einer Länge von mehr als 1.900 Bit und weniger als 3.000 Bit DÜRFEN noch bis 2025 verwendet werden (Legacy gem. [SOGIS]).
- ECC: Es SOLLTEN Schlüssel aus folgenden Kurven verwendet werden (Recommendation gem. [SOGIS]):
    - BrainpoolP256r1
    - BrainpoolP384r1
    - BrainpoolP512r1
    - NIST P-256
    - NIST P-384
    - NIST P-521

[SSL] [SMIME] RSA-Schlüssel MÜSSEN mindestens 2048 Bit lang sein, die Länge des Modulus muss durch 8 teilbar sein.

EC-Schlüssel MÜSSEN aus folgenden Kurven verwendet werden:

- NIST P-256
- NIST P-384

[VS-NfD] Es gelten die Anforderungen aus [TR2102-1].

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Keine Vorgabe.

[SSL] Folgende Anforderungen an die Schlüssel MÜSSEN durch die TSP bei den von ihnen selbst generierten Schlüssel umgesetzt bzw. bei den ihnen vorgelegten Schlüsseln geprüft werden:

- RSA: Der Wert des Exponenten MUSS eine ungerade Zahl größer oder gleich 3 sein und SOLLTE im Bereich von 2^{16} und 2^{256}-1 liegen.
- RSA: Der Wert des Modulus MUSS eine ungerade Zahl sein, die nicht die Potenz einer Primzahl ist und keine Faktoren hat, die kleiner als 752 sind.
- ECC: Der TSP SOLLTE die Schlüssel entweder mit der ECC-Routine zur vollständigen Validierung öffentlicher Schlüssel oder mit der ECC-Routine zur teilweisen Validierung öffentlicher Schlüssel prüfen.

6.1.7 Schlüsselverwendung

6.1.7.1 Root-CA

Die Verwendung des privaten Schlüssels einer Root-CA MUSS auf die im korrespondierenden Root-CA-Zertifikat im Attribut keyUsage (siehe Kap. 7.1.2) aufgeführten Verwendungszwecke beschränkt werden.

[SSL] Die zu den Root-CA-Zertifikaten korrespondierenden privaten Schlüssel DÜRFEN NICHT zur Signatur von Zertifikaten verwendet werden, außer

- zur Signatur des Root-CA-Zertifikats selbst,
- zur Signatur von Sub-CA- und Cross-Zertifikaten,
- zur Signatur von Infrastrukturzertifikaten, z.B. für administrative Rollen oder Betriebsgeräte,
- zur Signatur von OCSP-Signer-Zertifikaten.

6.1.7.2 Sub-CA

Die Verwendung des privaten Schlüssels einer Sub-CA MUSS auf das Ausstellen von Zertifikaten und/oder die Signatur von Statusinformationen beschränkt werden. Dabei MÜSSEN die im korrespondierenden Sub-CA-Zertifikat im Attribut keyUsage (siehe Kap. 7.1.2) aufgeführten Verwendungszwecke berücksichtigt werden.

[SSL] [SMIME] Die Verwendung des privaten Schlüssels einer Sub-CA zur Signatur von Endteilnehmerzertifikaten MUSS auf die Signatur von Zertifikaten beschränkt werden, die den im korrespondierenden Sub-CA-Zertifikat im Attribut extendedKeyUsage (siehe Kap. 7.1.2) aufgeführten Verwendungszwecken entsprechen.

6.1.7.3 Endteilnehmer

Die Verwendung des privaten Schlüssels eines Endteilnehmers MUSS auf die im korrespondierenden Endteilnehmer-Zertifikat in den Attributen keyUsage und/oder extendedKeyUsage (siehe Kap. 7.1.2) aufgeführten Verwendungszwecke beschränkt werden.

Die TSP MÜSSEN in den CPS sowie den Nutzungsbedingungen die zugelassenen Verwendungszwecke aufführen.

[QCP-n-qcsd] Wenn ein TSP die QSCD eines Endteilnehmers managt, MUSS die Verwendung des privaten Schlüssels auf die Erzeugung elektronischer Signaturen beschränkt werden.

[QCP-l-qcsd] Wenn ein TSP die QSCD eines Endteilnehmers managt, MUSS die Verwendung des privaten Schlüssels auf die Erzeugung elektronischer Siegel beschränkt werden.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

Zum Schutz der privaten Schlüssel aller Hierarchieebenen MÜSSEN die TSP hinreichende Sicherheitsmaßnahmen treffen oder, im Falle der Endteilnehmerschlüssel, welche die TSP nicht managen, vorgeben.

Die Vorgaben zur Generierung der Schlüssel sowie ggf. zur Übergabe der vom TSP generierten privaten Schlüssel der Endteilnehmer sind in Kap. 6.1 beschrieben. Die nachfolgenden Kapitel treffen Vorgaben für Nutzung, ggf. Hinterlegung, Backup und Archivierung sowie Außerbetriebnahme und ggf. Zerstörung der Schlüssel, die in kryptografischen Modulen (HSM, Smartcards, sonstige Token) genutzt werden.

Auf Endteilnehmerschlüssel, die nicht in kryptografischen Modulen genutzt werden, wird an dieser Stelle nicht weiter eingegangen, die Maßnahmen und Vorgaben dazu MÜSSEN die TSP in ihren CPS und ggf. Nutzungsbedingungen beschreiben.

6.2.1 Standards und Kontrollen für kryptografische Module

Die Root- und Sub-CA- sowie die RA-Schlüssel MÜSSEN in kryptografischen Modulen erzeugt werden, die entweder nach CC EAL 4 oder höher oder nach einem vergleichbaren Standard evaluiert sind oder nach FIPS 1402-2 Level 3 zertifiziert sind.

Die TSP MÜSSEN sicherstellen, dass die kryptografischen Module bei Lagerung und Transport nicht manipuliert werden.

[VS-NfD] Die kryptografischen Module, in denen die Schlüssel der Sub-CAs generiert und betrieben werden, MÜSSEN vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die VS-NfD-Nutzung zugelassen sein.

Alle kryptografischen Module MÜSSEN gemäß den Vorgaben der Zertifizierungsdokumentation oder in vergleichbarer Konfiguration mit gleichem Sicherheitsniveau betrieben werden.

[QCP-n-qscd] [QCP-l-qscd] Die QSCD MÜSSEN zertifiziert sein. Die TSP MÜSSEN den Zertifizierungsstatus der QSCD bis zum Ablauf der Gültigkeit der Endteilnehmerzertifikate monitoren und entsprechende Maßnahmen einleiten, wenn sich der Zertifizierungsstatus vor Ablauf der Endteilnehmerzertifikate ändert.

6.2.2 Mehrpersonenkontrolle über private Schlüssel (n von m)

Keine Vorgabe.

[QCP-n-qscd] [QCP-l-qscd] Die Nutzung privater Endteilnehmerschlüssel MUSS in der alleinigen Kontrolle des Endteilnehmers liegen, unabhängig davon ob er die QSCD selbst besitzt oder diese durch einen TSP in seinem Auftrag managen lässt.

6.2.3 Hinterlegung privater Schlüssel

Keine Vorgabe.

6.2.4 Sicherung privater Schlüssel

Die privaten Schlüssel der Root- und Sub-CAs MÜSSEN in einer sicheren Umgebung gesichert werden, dabei MUSS für die Sicherung der Schlüssel bzgl. Zugriff, Manipulation und Verlust das gleiche Sicherheitsniveau gelten wie für die im Betrieb befindlichen privaten Schlüssel.

Die Sicherung sowie ggf. die Rücksicherung MÜSSEN im Rahmen einer Key-Zeremonie erfolgen, es gelten dabei die gleichen Bedingungen wie bei der Schlüsselgenerierung (siehe Kap. 6.1.1.1 bzw. 6.1.1.2). Darüber hinaus MUSS sichergestellt sein, dass der Zugriff auf die Sicherungen mindestens zwei vertrauenswürdige Mitarbeiter des TSP erfordert.

[3145] TSP, die Schlüssel im Auftrag der Endteilnehmer sichern, MÜSSEN

- die Endteilnehmerschlüssel verschlüsselt ablegen,
- zur Verschlüsselung der Endteilnehmerschlüssel jeweils individuelle Geheimnisse verwenden, die von der Sub-CA selbst generiert werden,
- die zur Verschlüsselung verwendeten individuellen Geheimnisse ebenfalls verschlüsseln und getrennt von den Endteilnehmerschlüsseln sicher speichern, so dass deren Integrität und Vertraulichkeit gewährleistet ist,
- die Endteilnehmer im Falle eines Rücksicherungswunsches sicher identifizieren (in Anlehnung an die Identifizierung bei Antragsstellung, siehe Kap. 4.2.1),
- die Sicherung dem Endteilnehmer so übergeben, wie die originalen Schlüssel (siehe Kap. 6.1.2)

[VS-NfD] TSP, die Schlüssel im Auftrag der Endteilnehmer sichern,

- MÜSSEN ergänzend zu den o.g. Vorgaben zu [3145] die Wiederherstellungsmaßnahmen und -Richtlinien durch den Sicherheitsbeauftragten freigeben lassen und
- DÜRFEN NICHT andere Schlüssel als die Verschlüsselungsschlüssel der Endteilnehmer sichern.

6.2.5 Archivierung privater Schlüssel

Keine Vorgabe.

[SSL] Andere Parteien als der TSP, der eine Sub-CA betreibt, DÜRFEN die privaten Schlüssel der Sub-CA nicht ohne die Erlaubnis des TSP archivieren. Ebenso DÜRFEN andere Parteien als der Endteilnehmer selbst NICHT die privaten Schlüssel des Endteilnehmers ohne dessen Erlaubnis archivieren.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Wenn Root- oder CA-Schlüssel außerhalb eines kryptografischen Moduls gemäß Kap. 6.2.1 aufbewahrt werden, so MÜSSEN diese so aufbewahrt werden, dass ein zur Speicherung innerhalb eines kryptografischen Moduls vergleichbares Sicherheitsniveau sichergestellt ist. Der Im- und Export von Schlüsseln MUSS einer Key-Zeremonie mindestens im Vier-Augen-Prinzip erfolgen. es gelten dabei die gleichen Bedingungen wie bei der Schlüsselgenerierung (siehe Kap. 6.1.1.1 bzw. 6.1.1.2).

[3145] Bei einem Defekt eines kryptografischen Moduls, welches zur Speicherung und Nutzung privater Schlüssel einer Sub-CA verwendet wird, MÜSSEN die privaten Schlüssel gemäß den o.g. Vorgaben in ein neues kryptografisches Modul übertragen werden.

6.2.7 Speicherung privater Schlüssel in kryptografischen Modulen

Die privaten Schlüssel der Root- und Sub-CAs MÜSSEN in kryptografischen Modulen gemäß Kap. 6.1.1, 6.2.1 und 6.2.2 generiert, gespeichert und genutzt werden.

[NCP+] Die privaten Schlüssel der Endteilnehmer MÜSSEN in sicheren kryptografischen Modulen gespeichert und genutzt werden.

[QCP-n-qscd] [QCP-l-qscd] Die privaten Schlüssel der Endteilnehmer MÜSSEN in zertifizierten QSCD gemäß Kap. 6.2.1 generiert, gespeichert und genutzt werden.

6.2.8 Methoden zur Aktivierung privater Schlüssel

TSP, die Schlüssel für Endteilnehmer erzeugen und diesen übergeben, MÜSSEN sicherstellen, dass deren Aktivierung durch die Endteilnehmer auf sichere Art und Weise erfolgt. Die TSP MÜSSEN die erforderlichen Maßnahmen und Vorgaben in ihren CPS und ggf. den Nutzungsbedingungen beschreiben.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

TSP, die Schlüssel für Endteilnehmer erzeugen und diesen mittels kryptografischer Module (z.B. Smartcards) übergeben, MÜSSEN sicherstellen, dass deren Deaktivierung und ggf. Reaktivierung durch die Endteilnehmer auf sichere Art und Weise erfolgen. Die TSP MÜSSEN die erforderlichen Maßnahmen und Vorgaben in ihren CPS und ggf. den Nutzungsbedingungen beschreiben.

6.2.10 Methoden zur Zerstörung privater Schlüssel

Die privaten Schlüssel einer Root- oder Sub-CA MÜSSEN am Ende des Lebenszyklus des korrespondierenden Root- oder Sub-CA-Zertifikats, d.h. mit Ablauf der Gültigkeitsdauer, der Sperrung oder der Außerbetriebnahme des Sub-CA-Zertifikats oder der Beendigung des Dienstes zerstört werden. Die Zerstörung der Schlüssel MUSS in einer Key-Zeremonie erfolgen und alle Kopien der Schlüssel berücksichtigen. Es gelten dabei, sofern anwendbar, die gleichen Anforderungen wie bei der Generierung der Schlüssel (siehe Kap. 6.1.1.1 bzw. 6.1.1.2).

Wenn kryptografische Module am Ende ihrer Nutzungsdauer oder aufgrund eines Defekts außer Betrieb genommen werden, so MÜSSEN alle privaten Schlüssel, die in dem Modul gespeichert sind, zerstört werden. Die Zerstörung betrifft nicht die Kopien der privaten Schlüssel, sofern die Schlüssel in anderen bzw. neuen kryptografischen Modulen noch weiter genutzt werden sollen.

[VS-NfD] Sollte ein TSP keine hinreichenden Nachweise über die Zerstörung eines privaten Sub-CA-Schlüssels liefern können, so MUSS das korrespondierende Sub-CA-Zertifikat gesperrt werden.

6.2.11 Bewertung kryptografischer Module

Die TSP MÜSSEN kryptografische Module vor der Beschaffung bzgl. ihrer Nutzbarkeit und der Erfüllung aller Anforderungen bewerten.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des öffentlichen Schlüssels

Keine Vorgabe.

6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Für die Schlüssel aller Hierarchiestufen gilt, dass diese nur so lange genutzt werden dürfen, wie diese inkl. der zur Zertifikatssignatur verwendeten Algorithmen als hinreichend sicher gemäß Kap. 6.1.5 und 6.1.6 angesehen werden können.

6.3.2.1 Root-CA

Keine Vorgaben für die Zertifikatsgültigkeitsdauer der Root-CAs.

Der private Schlüssel einer Root-CA DARF nach Ende des Lebenszyklus des korrespondierenden Root-CA-Zertifikats, d.h. mit Ablauf der Gültigkeitsdauer oder der Außerbetriebnahme des Zertifikats oder der Beendigung des Dienstes, NICHT mehr verwendet werden.

Zur Gewährleistung eines ununterbrochenen Betriebs MUSS der Root-TSP rechtzeitig vor Ablauf eines Root-CA-Zertifikats oder dem Ende der Nutzbarkeit der Schlüssel ein Folgezertifikat ausstellen.

6.3.2.2 Sub-CA

Die Gültigkeitsdauer eines Sub-CA-Zertifikats DARF die Gültigkeitsdauer des Zertifikats der ausstellenden Root-CA nicht überschreiten („Schalenmodell“).

[SMIME] Die Gültigkeitsdauer eines Sub-CA-Zertifikats SOLLTE NICHT größer als 10 Jahre und DARF NICHT größer als 20 Jahre sein.

Die privaten Schlüssel einer Sub-CA DÜRFEN nach Ende des Lebenszyklus des korrespondierenden Sub-CA-Zertifikats, d.h. mit Ablauf der Gültigkeitsdauer, der Sperrung oder der Außerbetriebnahme des Zertifikats oder der Beendigung des Dienstes, NICHT mehr verwendet werden.

Zur Gewährleistung eines ununterbrochenen Betriebs MÜSSEN die TSP rechtzeitig vor Ablauf eines Sub-CA-Zertifikats oder dem Ende der Nutzbarkeit der Schlüssel ein Folgezertifikat beantragen. Die TSP MÜSSEN die Fristen zur Ausstellung der Folgezertifikate in ihren CPS beschreiben.

[3145] Ergänzend dazu MUSS die Nutzung des privaten Schlüssels einer Sub-CA, z.B. durch Deaktivierung, verhindert werden, wenn

- dieser erst zu einem definierten Zeitpunkt verwendet werden soll (z.B. für die Zukunft geplante Inbetriebnahme eines neuen Sub-CA-Zertifikats),
- dieser für einen bestimmten Zeitraum aufgrund eines speziellen Anwendungsfalls nicht verwendet werden soll.

6.3.2.3 Endteilnehmer

Die Gültigkeitsdauer eines Endteilnehmerzertifikats DARF die Gültigkeitsdauer des Zertifikats der ausstellenden Sub-CA nicht überschreiten („Schalenmodell“).

[QCP] Für qualifizierte Zertifikate gilt abweichend das Kettenmodell, d.h. die Endteilnehmerzertifikate DÜRFEN länger gültig sein als das Gültigkeitsende des Zertifikats der ausstellenden Sub-CA.

[SSL] Endteilnehmerzertifikate SOLLTEN NICHT länger als 397 Tage gültig sein und DÜRFEN NICHT länger als 398 Tage gültig sein.

[SMIME] Endteilnehmerzertifikate DÜRFEN NICHT länger als 27 Monate gültig sein.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

TSP, die Endteilnehmerzertifikate auf kryptografischen Modulen (z.B. Smartcards) ausgeben, welche mit individuellen Aktivierungsdaten (z.B. PINs) versehen werden, MÜSSEN die Aktivierungsdaten auf sichere Art und Weise generieren und in den kryptografischen Modulen einstellen.

6.4.2 Schutz der Aktivierungsdaten

Die vom TSP erzeugten Aktivierungsdaten (siehe Kap. 6.4.1) MÜSSEN von der Erzeugung bis zur Übergabe an den Endteilnehmer so geschützt werden, dass deren Integrität und Vertraulichkeit gewahrt bleibt.

6.4.3 Andere Aspekte der Aktivierungsdaten

Die vom TSP erzeugten Aktivierungsdaten (siehe Kap. 6.4.1) MÜSSEN dem Endteilnehmer getrennt von den kryptografischen Modulen zeitversetzt oder über verschiedene Wege übermittelt werden.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Anmerkung: Die nachfolgend aufgeführten Anforderungen gelten, sofern anwendbar, analog für vom TSP beauftragte Dritte.

Die TSP MÜSSEN die für das Zertifikatsmanagement sowie die Status- und Verzeichnisdienste erforderlichen Systeme dem Schadenspotential entsprechend schützen.

Die TSP MÜSSEN die Accounts der für den Betrieb der kritischen Systeme erforderlichen vertrauenswürdigen Rollen (siehe Kap. 5.2.1) so managen, dass der Zugriff auf die Systeme und Daten auf die für diese Rollen identifizierten und authentifizierten Personen (siehe Kap. 5.2.3) mit den minimal erforderlichen Berechtigungen beschränkt wird. Die TSP MÜSSEN diese Accounts so managen, dass sie in angemessener Zeit geändert oder gelöscht werden.

Die TSP MÜSSEN für die Accounts, welche direkt die Erstellung von Zertifikaten auslösen können, eine Multi-Faktor-Authentisierung umsetzen.

Die Systeme MÜSSEN die geforderte Trennung von vertrauenswürdigen Rollen (siehe Kap. 5.2.4) technisch unterstützen.

Administrationssysteme, die zur Umsetzung der Sicherheitsrichtlinien verwendet werden, DÜRFEN NICHT für andere Zwecke verwendet werden.

[SMIME] Die TSP MÜSSEN eine Multi-Faktor-Authentisierung umsetzen für

- alle Accounts der internen und externen RAs,
- alle Accounts, über die technische Kontrollen zur Beschränkung vorab genehmigter Domänen oder E-Mail-Adressen eingestellt werden.

[SSL] [SMIME] Die TSP MÜSSEN

- die Accounts der zugriffsberechtigten Personen mindestens alle drei Monate überprüfen und nicht mehr benötigte Accounts deaktivieren.
- eine Multi-Faktor-Authentisierung bei allen Systemen umsetzen, die eine Multi-Faktor-Authentisierung unterstützen,
- die Authentifizierungsschlüssel und Passworte der privilegierten Accounts der CA-Systeme ändern, wenn sich die Berechtigung einer Person zum administrativen Zugriff auf die Systeme ändert oder entzogen wird,
- für vertrauenswürdige Rollen sicherstellen, dass sich diese zur Nachvollziehbarkeit mit persönlichen Accounts an den Systemen anmelden,
- für vertrauenswürdige Rollen, die sich mittels Benutzername und Passwort an den Systemen anmelden, sofern technisch möglich, die nachfolgend aufgeführten Maßnahmen umsetzen:
  - für Accounts, auf die nur in sicheren Umgebungen zugegriffen werden kann, MÜSSEN Passwörter mit mindestens 12 Zeichen Länge gefordert werden,
  - für Authentifizierungen, die eine Zonengrenze in eine Sicherheitszone überschreiten, ist eine Multi-Faktor-Authentifizierung erforderlich,
  - Für Konten, auf die von außerhalb einer Sicherheitszone zugegriffen werden kann, sind Kennwörter mit mindestens acht Zeichen erforderlich, bei denen es sich nicht um eines der vorherigen vier Kennwörter des Benutzers handelt und es ist eine Kontosperre nach fünf fehlgeschlagenen Zugriffsversuchen (s.u.),
  - Bei der Entwicklung von Passwort-Richtlinien SOLLTEN die TSP die Passwort-Richtlinien in NIST 800-63B Anhang A berücksichtigen,
  - wenn ein TSP eine Passwortrichtlinie hat, welche eine routinemäßige periodische Passwortänderungen erfordert, DARF dieser Zeitraum NICHT weniger als zwei Jahre betragen,
- die Personen in vertrauenswürdigen Rollen verpflichten, sich von ihrem Account abzumelden oder ihren Arbeitsplatz zu sperren, wenn sie nicht mehr in der Rolle tätig sind,
- entweder die Arbeitsplätze so konfigurieren, dass diese automatisch nach einer festgelegten Zeit der Inaktivität des Nutzers gesperrt werden oder die relevanten Anwendungen so konfigurieren, dass diese automatisch nach einer festgelegten Zeit der Inaktivität des Nutzers zur Abmeldung des Accounts führen,
- den Zugang zu CA-Systemen nach fünf fehlgeschlagenen Anmeldeversuchen sperren, vorausgesetzt, dass das CA-System dies Maßnahme unterstützt, die Maßnahme nicht für Denial of Service-Angriffe genutzt werden kann und die Maßnahme nicht die Sicherheit dieser Authentifizierungskontrolle schwächt,
- eine Multi-Faktor-Authentisierung oder eine Mehr-Personen-Authentifizierung für den administrativen Zugriff auf kritische Systeme sicherstellen,
- eine Multifaktor-Authentisierung für alle Accounts der vertrauenswürdigen Rollen an den CA-Systemen, die von außerhalb der sicheren Umgebungen erreichbar sind, sicherstellen,
- remote-Zugriffe auf kritische Systeme nur dann zulassen, wenn diese von Systemen ausgehen, die dem TSP gehören oder vom TSP kontrolliert werden und die temporär über einen verschlüsselten Kanal auf Basis einer Multifaktor-Authentisierung gegenüber einem gesicherten System im Netzwerk des TSP aufgebaut werden, welches die Verbindung zu den kritischen Systemen vermittelt.

Die TSP MÜSSEN vertrauenswürdige Systeme einsetzen, welche die technische Sicherheit und Zuverlässigkeit der von den Systemen unterstützten Prozesse sicherstellen.

Die CA-, Zertifikatsmanagement-, Sicherheits- und Frontend-Systeme sowie, falls anwendbar, weitere interne Systeme zur Unterstützung des Betriebs, MÜSSEN gehärtet sein, d.h. sie MÜSSEN so konfiguriert werden, dass die für den Betrieb der CAs nicht benötigten Accounts, Dienste, Protokolle und Ports deaktiviert werden.

Die Systeme MÜSSEN mit einem Integritätsschutz versehen sein, der vor Viren, Schadcode und dem Einspielen unerlaubter Software schützt.

Die Systeme MÜSSEN so dimensioniert sein, dass sie hinreichend performant sind und einen ununterbrochenen Betrieb gewährleisten.

Die TSP MÜSSEN die zur Zertifikatserzeugung und ggf. -Sperrung erfassten Daten inkl. der Protokolldaten gemäß Kap. 5.4.1 so sichern, dass deren Integrität, Vertraulichkeit und Verfügbarkeit über den gesamten Aufbewahrungszeitraum sichergestellt ist.

Die TSP MÜSSEN für die Produktivumgebung und die Test- bzw. Entwicklungsumgebung getrennte Systeme verwenden.

6.5.2 Sicherheitsbewertung von Computern

Keine Vorgabe.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Steuerung der Systementwicklung

Die TSP MÜSSEN bereits in der Entwurfs- und Anforderungsspezifikationsphase eines Systementwicklungsprojekts eine Analyse der Sicherheitsanforderungen durchführen, um sicherzustellen, dass die Sicherheit der Systeme von vorneherein berücksichtigt wird.

6.6.2 Maßnahmen des Sicherheitsmanagements

Alle Releases, Patches und kurzfristigen Bugfixes sowie Änderungen der Konfiguration, welche die Sicherheitsrichtlinien betreffen, MÜSSEN über geregelte Changemanagement-Prozesse abgewickelt und dokumentiert werden.

Alle Änderungen, die sich auf das vom TSP festgelegte Sicherheitsniveau auswirken, MÜSSEN von der Leitung des TSP freigegeben werden.

Die TSP MÜSSEN sicherstellen, dass

- Sicherheitspatches in einer angemessenen Zeit, spätestens jedoch innerhalb von 6 Monaten, eingespielt werden,
- Sicherheitspatches nicht eingespielt werden, wenn diese zusätzliche Schwachstellen oder Instabilitäten mit sich bringen, welche den Vorteil des Patches überwiegen,
- die Gründe für das Nicht-Einspielen von Sicherheitspatches dokumentiert werden.

Die TSP MÜSSEN die Systeme bzgl. folgender Aktivitäten überwachen und geeignete Alarmierungsfunktionen implementieren:

- Sicherheitsrelevante Systemereignisse, dazu zählen:
  - erfolgreiche und erfolglose Zugriffsversuche auf die Zertifikatssysteme,
  - durchgeführte Tätigkeiten an den Zertifikats- und Sicherheitssystemen,
  - Starten und Abschalten der Protokollierungsfunktionen,
- Verfügbarkeit und Nutzung der benötigten Dienste,

[SSL] [SMIME] Ergänzend zu den vorgenannten Ereignissen MÜSSEN folgende Aktivitäten überwacht werden:

- Änderungen von Sicherheitsprofilen,
- Installation, Aktualisierung und Entfernung von Software auf einem Zertifikatssystem,
- Systemabstürze, Hardware-Ausfälle und andere Anomalien,
- Firewall und Router-Aktivitäten und
- Zu- und Austritte in und aus den Betriebsräumen der Zertifikatsmanagementsysteme.

Die TSP SOLLTEN bei der Überwachung die Sensibilität aller gesammelten oder analysierten Informationen berücksichtigen.

Die TSP MÜSSEN die Konfiguration der Systeme kontinuierlich auf Änderungen, die nicht auf Basis eines autorisierten Change durchgeführt wurden, überwachen und ggf. alarmieren.

[NCP] Die TSP MÜSSEN den Kapazitätsbedarf der Systeme überwachen und Prognosen für den zukünftigen Kapazitätsbedarf erstellen, um sicherzustellen, dass angemessene Verarbeitungsleistungen und Speicherkapazitäten zur Verfügung stehen.

Die TSP SOLLTEN die Datensicherungen regelmäßig testen, um sicherzustellen, dass diese den Anforderungen des Notfallplans genügen. Die Datensicherungs- und Rücksicherungsfunktionen MÜSSEN von den dafür vorgesehen vertrauenswürdigen Rollen durchgeführt werden.

6.6.3 Sicherheitskontrollen während des Lebenszyklus

Die TSP MÜSSEN geeignete Sicherheitskontrollen für die Verwaltung aller kryptographischen Schlüssel und kryptographischen Geräte während ihres gesamten Lebenszyklus umsetzen.

6.7 Netzwerk-Sicherheitskontrollen

Die TSP MÜSSEN ihre internen Netze und Systeme vor unautorisierten Zugriffen und Angriffen schützen, z.B. durch Firewalls. Die TSP MÜSSEN ihre Netzwerkkomponenten (bspw. Firewalls, Router) so konfigurieren, dass alle nicht benötigten Protokolle und Zugänge deaktiviert sind.

[SSL] [SMIME] Die TSP MÜSSEN Intrusion Detection- (IDS) und Intrusion-Prevention-Systeme (IPS) implementieren, die sie selbst unter Kontrolle haben oder an vertrauenswürdige Rollen Dritter delegiert haben.

[3145] Wenn ein IDS verwendet wird, MÜSSEN die vom IDS aufgezeichneten Protokolldateien bei jedem Vorfall sowie regelmäßig in einem vom TSP festgelegten Zeitraum ausgewertet werden.

Die TSP MÜSSEN ihre Systeme in Netzwerke oder Zonen auf der Grundlage einer Risikobewertung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehung zwischen vertrauenswürdigen Systemen und Diensten segmentieren.

[VS-NfD] Die TSP MÜSSEN bei der Netzwerktrennung [ISI LANA] als Leitfaden anwenden.

Alle für den Betrieb der TSP kritischen Systeme MÜSSEN in sicheren oder hochsicheren Zonen untergebracht werden. Die Root-CA-Systeme MÜSSEN in hochsicheren Zonen untergebracht werden und offline bzw. von allen anderen Netzen getrennt betrieben werden. Die TSP MÜSSEN Sicherheitsverfahren implementieren und konfigurieren, welche die Systeme und die Kommunikation zwischen Systemen innerhalb von Sicherheitszonen schützt.

Die TSP MÜSSEN die Netzwerke zur Administration der Systeme von den operativen Netzwerken separieren.

Innerhalb einer Zone MÜSSEN für alle Systeme die gleichen Sicherheitsanforderungen gelten.

Zwischen den Zonen MÜSSEN Sicherheitssysteme implementiert werden, welche die Systeme und Kommunikation innerhalb der sicheren Zonen sowie die Kommunikation mit den Systemen außerhalb der Zonen schätzen. Die Verbindungen MÜSSEN so eingeschränkt werden, dass nur die zum Betrieb erforderlichen Verbindungen möglich sind, nicht benötigte Verbindungen MÜSSEN explizit verboten oder deaktiviert werden. Alle Netzwerkgeräte an den Zonengrenzen (Firewalls, Router, Switches, Gateways oder sonstige Geräte) MÜSSEN so konfiguriert werden, dass ausschließlich die Dienste, Protokolle, Ports und Kommunikationsbeziehungen zugelassen werden, die für den Betrieb der CAs erforderlich sind.

Die TSP MÜSSEN die o.g. Regeln regelmäßig überprüfen.

Für die Kommunikation zwischen verschiedenen vertrauenswürdigen Systemen MÜSSEN vertrauenswürdige Kanäle genutzt werden, die sich logisch von anderen Kommunikationskanälen unterscheiden und eine sichere Identifizierung ihrer Endpunkte sowie die Integrität und Vertraulichkeit der übertragenen Daten gewährleisten.

Sofern eine hohe Verfügbarkeit des externen Zugriffs auf die Systeme des TSP gefordert ist, MÜSSEN die externen Netzwerkverbindungen redundant aufgebaut sein.

Die TSP MÜSSEN regelmäßige Schwachstellenprüfungen an öffentlichen und privaten IP-Adressen, die vom TSP identifiziert wurden, durchführen oder durchführen lassen. Die Schwachstellenprüfungen MÜSSEN von Personen oder Organisationen durchgeführt werden, die über die für einen zuverlässigen Bericht erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die TSP MÜSSEN die Durchführung der Schwachstellenprüfung mit Angabe der Qualifikation der prüfenden Person oder Organisation dokumentieren.

Die TSP MÜSSEN ihre Systeme bei Inbetriebnahme oder bei signifikanten Änderungen an der Infrastruktur oder den Anwendungen Penetrationstests unterziehen. Die Penetrationstests MÜSSEN von Personen oder Organisationen durchgeführt werden, die über die für einen zuverlässigen Bericht erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen

Grundsätze und Unabhängigkeit verfügen. Die TSP MÜSSEN die Durchführung der Penetrationstests mit Angabe der Qualifikation der prüfenden Person oder Organisation dokumentieren.

[SSL] [SMIME] Die TSP MÜSSEN die o.g. Schwachstellenprüfungen

- innerhalb einer Woche auf Anfrage des CA/Browser-Forums,
- bei signifikanten Änderungen an der Infrastruktur oder den Anwendungen und
- mindestens alle drei Monate

durchführen (lassen).

Die TSP MÜSSEN die o.g. Penetrationstests mindestens jährlich durchführen (lassen).

Die TSP MÜSSEN innerhalb von 96 Stunden nach der Entdeckung einer kritischen Schwachstelle

- diese Schwachstelle beheben oder
- wenn eine Behebung der Schwachstelle innerhalb von 96 Stunden nicht möglich ist, einen Plan zur Minderung der Schwachstelle, inkl. einer Priorisierung anhand der betroffenen Systeme, erstellen oder
- die faktische Grundlage für die Entscheidung des TSP dokumentieren, dass die Schwachstelle nicht behoben werden muss, weil entweder der TSP mit der Einstufung nicht einverstanden ist oder es sich nicht um eine Schwachstelle handelt („False Positive“) oder die Ausnutzung der Schwachstelle durch kompensierende Kontrollen oder das Fehlen von Bedrohungen verhindert wird oder andere ähnliche Gründe vorliegen.

[3145] Die TSP MÜSSEN die o.g. Penetrationstests regelmäßig in einem vom TSP festgelegten Zeitraum durchführen (lassen)

Lokale Netzwerkkomponenten (z.B. Router) MÜSSEN in physikalisch und logisch sicheren Umgebungen installiert sein. Deren Konfigurationen MÜSSEN regelmäßig auf Übereinstimmung mit den vom TSP definierten Anforderungen geprüft werden.

6.8 Zeitstempel

Keine Vorgabe.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

Die nachfolgenden Kapitel beschreiben die Anforderungen an die Zertifikatsprofile. Ergänzend dazu gelten folgende Anforderungen:

- Die Zertifikatsprofile MÜSSEN dem RFC5280 sowie den Empfehlungen der ITU-T X.509 (https://www.itu.int/rec/T-REC-X.509/) entsprechen und in den CPS der TSP beschrieben werden.
- Die Seriennummern der Zertifikate MÜSSEN mit einem kryptographisch sicheren Zufallszahlengenerator erstellt werden. Sie MÜSSEN größer als Null (positiver Integerwert) sein und DÜRFEN eine maximale Länge von 160 Bit NICHT überschreiten. Jede Seriennummer DARF je Aussteller NICHT mehrfach verwendet werden.
- Bzgl. der Gültigkeitsdauern der Zertifikate wird auf Kap. 6.3.2 verwiesen.
- Pre-Zertifikate gemäß RFC 6962 (“Certificate Transparency”) gelten nicht als gültige Zertifikate im Sinne des RFC 5280.
- Die aufgezeigten Zertifikatsprofile gelten für alle Zertifikate, die ab dem Gültigkeitsbeginn dieser CP ausgestellt werden. Bereits ausgestellte Zertifikate mit Profilen gemäß älterer Anforderungen behalten ihre Gültigkeit, sofern nicht explizit auf deren Ungültigkeit hingewiesen wird. (Bestandschutz)

[SSL] [SMIME] Die Seriennummern MÜSSEN mindestens 64 Bit groß sein.

7.1.1 Versionsnummer

Alle X509-Zertifikate MÜSSEN in der Version 3 (mit dem Wert „2“) ausgestellt werden.

7.1.2 Zertifikatserweiterungen

Die folgende Tabelle gibt einen Überblick über obligatorische und optionale Zertifikatserweiterungen für Root-CA-, Sub-CA-, Endteilnehmer- und OCSP-Signer-Zertifikate[1]. Erweiterungen, die dort nicht aufgeführt sind, DÜRFEN NICHT verwendet werden. Zur Kennzeichnung gelten folgende Konventionen:

- **M** (mandatorisch): Diese Erweiterung MUSS gesetzt sein.
  (M) Diese Erweiterung MUSS unter bestimmten Umständen gesetzt werden.
- **O** (optional): Diese Erweiterung DARF gesetzt sein.
- **S** (sollte): Diese Erweiterung SOLLTE gesetzt werden
- **SN** (sollte nicht): Diese Erweiterung SOLLTE NICHT gesetzt sein.
- **N** (nicht erlaubt): Diese Erweiterung DARF NICHT gesetzt sein.
- **K** (kritisch): Diese Erweiterung MUSS, wenn sie gesetzt ist, als kritisch markiert werden.
  (K) Diese Erweiterung DARF als kritisch markiert werden.
  Hinweis: Grundsätzlich DÜRFEN Erweiterungen NICHT als kritisch markiert werden, wenn es nicht explizit erlaubt ist oder gefordert wird.

[1] CRL-Signer-Zertifikate werden nicht aufgeführt, da die CRLs von den CAs direkt ausgestellt werden.

- ***(nn)*** Verweis auf die der auf die Tabelle folgenden Beschreibung der zu setzenden Parameter bzw. Inhalte. Verweise in der Spalte „Erweiterung gem. RFC5280“ bedeuten, dass die aufgeführten Vorgaben übergreifend für alle Zertifikatstypen gelten

Tabelle 6 - Zertifikatserweiterungen

Erweiterung gem. RFC5280 (OID)	**Root-CA-Zertifikat**	**Sub-CA-Zertifikat**	**Endteilnehmer-Zertifikat**	**OCSP-Signer**
AuthorityKeyIdentifier (2.5.29.35)	O (01)	M (01)	M (01)	M (01)
SubjectKeyIdentifier (2.5.29.14)	M (02) (03)	M (02) (03)	S	S
KeyUsage K (2.5.29.15)	M (04)	M (04)	M, [SSL] O (05) (06)	M
CertificatePolicies (2.5.29.32)	SN	O, [SSL] [EVCP] M (07) (08)	M (07) (09) (10)	O (07)
subjectAltName (2.5.29.17)	O (11)	O (11)	O, [SSL] M (11) (12)	O (11)
BasicConstraints (2.5.29.19)	M (13) K	M (13) K	O (14) **(K)**	O **(K)**
NameConstraints K (2.5.29.30)	N	(M) (15)	N	N
ExtendedKeyUsage (2.5.29.37)	N	SN, [SSL] [SMIME] M (16) (17)	(M) (18) (19)	M (20)
cRLDistributionPoints (2.5.29.31)	(M) (21)	(M) (22)	(M) (23)	O[2]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	(M) (24)	(M) (24) (25)	M (26) (27)	O[2]
qcStatements (1.3.6.1.5.5.7.1.3)	N	N	N, [QCP] M (28)	N
IssuerAlternativeName (2.5.29.18)	SN	SN	O	SN
SubjectDirectoryAttributes (2.5.29.9)	SN	SN	O	N
No-Check (1.3.6.1.5.5.7.48.1.5)	N	N	N	(M)[2]
cabfOrganizationIdentifier (2.23.140.3.1)	N	N	N, [EVCP] (M) (29)	N

Nachfolgend werden die in den Erweiterungen zu verwendenden Inhalte und Parameter aufgelistet, sofern dazu über die Standards hinausgehende ergänzende Anforderungen existieren.

AuthorityKeyIdentifier

(01) Es MUSS der „keyIdentifier“ gem. RFC5280 #4.2.1.1 gesetzt werden.

[SSL] Es DÜRFEN die Attribute “authorityCertIssuer” und “authorityCertSerialNumber” NICHT gesetzt werden.

[2] Siehe dazu Kap. 7.3

SubjectKeyIdentifier

(02) Es MUSS der „keyIdentifier“ gem. RFC5280 #4.2.1.1 gesetzt werden.

(03) In einem Root- oder Sub-CA-Zertifikat MUSS der SubjectKeyIdentifier dem AuthorityKeyIdentifier in den von dieser CA ausgestellten Zertifikaten entsprechen.

KeyUsage

(04) In einem Root- oder Sub-CA-Zertifikat MÜSSEN die Bits für keyCertSign oder cRLSign gesetzt sein. Das Bit für digitalSignature MUSS gesetzt sein, wenn mit diesem Zertifikat auch OCSP-Antworten signiert werden sollen, sonst DARF es NICHT gesetzt sein.

(05) In Endteilnehmer-Zertifikaten DÜRFEN die Bits für keyCertSign und cRLSign NICHT gesetzt sein. Wenn die Erweiterung „ExtendedKeyUsage“ gesetzt ist, MÜSSEN die Bits der KeyUsage konsistent zu den Parametern der ExtendedKeyUsage gem. RFC5280, Kap. 4.2.1.12 gesetzt werden.

(06) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten für natürliche oder juristische Personen (nicht SSL-Serverzertifikate) MUSS eine der folgenden Varianten der KeyUsage gesetzt werden:

a) nonRepudiation
b) nonRepudiation und digitialSignature
c) digitialSignature
d) digitialSignature und [keyEncipherment oder keyAgreement]
e) keyEncipherment oder keyAgreement
f) nonrepudiation und digitialSignature und [keyEncipherment oder keyAgreement]

Um eine gemischte Verwendung von Schlüsseln zu vermeiden, SOLLTEN nur die Varianten a), c) oder e) genutzt werden.

In Zertifikaten, mit denen die Verpflichtung zu signierten Inhalten bestätigt wird, MUSS eine der Varianten a), b) oder f) genutzt werden, davon SOLLTE Variante a) genutzt werden.

certificatePolicies

(07) Es SOLLEN grundsätzlich nur OIDs verwendet werden. Wenn die alleinige Nutzung von OIDs unzureichend ist, DÜRFEN zusätzlich die Qualifier „cPSuri“ oder „userNotice“ gesetzt werden. Eine OID DARF NICHT mehrfach in der Erweiterung „certificatePolicies“ gesetzt werden.

(08) [SSL] [TSEC-CA] In Sub-CA-Zertifikaten DARF eine OID enthalten sein, welche die Einhaltung der Baseline-Reuirements des CA/Browser Forums bestätigt. Dazu DÜRFEN entweder die vom CA/Browser reservierten OIDs oder eigene OIDs des TSP, die in dem relevanten CPS des TSP beschrieben sind, verwendet werden. Die OID für „anyPolicy“ (2.5.29.32.0) DARF gesetzt werden.

(08) [SSL] [DFN-CA] In Sub-CA-Zertifikaten MUSS mindestens eine OID enthalten sein, welche die Einhaltung der Baseline-Requirements des CA/Browser Forums bestätigt. Dazu können entweder die vom CA/Browser reservierten OIDs oder eigene OIDs des TSP, die in dem relevanten CPS des TSP beschrieben sind, verwendet werden. Die OID für „anyPolicy“ (2.5.29.32.0) DARF NICHT gesetzt werden. Es DARF der Qualifier „cPSuri“ mit einem Verweis (http URL) zur dieser Certificate Policy gesetzt werden.

(08) [EVCP] [DFN-CA] In Sub-CA-Zertifikaten MUSS mindestens eine OID enthalten sein, welche die umgesetzte EV-Policy des TSP beschreibt. Darüber hinaus MUSS die Referenz auf das CPS der Root-CA enthalten sein (OID 1.3.6.1.5.5.7.2.1 sowie eine http-URL). Die OID für „anyPolicy“ (2.5.29.32.0) DARF gesetzt werden.

(09) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten für natürliche oder juristische Personen (nicht SSL-Serverzertifikate) MUSS mindestens eine OID einer Certificate Policy enthalten sein, welche die von dem TSP durchgeführten Praktiken und Verfahren widerspiegelt. Es DÜRFEN die von ETSI reservierten OIDs verwendet werden:

- [NCP] 0.4.0.2042.1.1
- [NCP+] 0.4.0.2042.1.2
- [LCP] 0.4.0.2042.1.3
- [QCP-n] 0.4.0.194112.1.0
- [QCP-l] 0.4.0.194112.1.1
- [QCP-n-qscd] 0.4.0.194112.1.2
- [QCP-l-qscd] 0.4.0.194112.1.3
- [QCP-w] 0.4.0.194112.1.4

(10) [SSL] In Endteilnehmerzertifikaten MUSS mindestens eine der nachfolgenden vom CA/Browser Forum reservierten OIDs enthalten sein:

- [EVCP] 2.23.140.1.1
- [DVCP] 2.23.140.1.2.1
- [OVCP] 2.23.140.1.2.2
- [IVCP] 2.23.140.1.2.3
- EV Code Signing 2.23.140.1.3
- Non-EV Code Signing 2.23.140.1.4.1

Darüber hinaus DÜRFEN eigene OIDs des TSP, die in dem relevanten CPS des TSP beschrieben sind, und/oder nachfolgende von ETSI reservierte OIDs verwendet werden:

- [EVCP] 0.4.0.2042.1.4
- [DVCP] 0.4.0.2042.1.6
- [OVCP] 0.4.0.2042.1.7
- [IVCP] 0.4.0.2042.1.8

(10) [EVCP] In Endteilnehmerzertifikaten MÜSSEN die zutreffende OID der EV-Policy des TSP und die Referenz auf das relevante CPS des TSP (OID 1.3.6.1.5.5.7.2.1 sowie eine http-URL) gesetzt werden.

subjectAltName

(11) Es DARF in den Zertifikaten aller Hierarchieebenen die Erweiterung „subjectAltName“ gesetzt werden. Wenn diese gesetzt wird, MÜSSEN alle prüfbaren[3] Inhalte vom TSP geprüft worden sein.

(12) [SSL] In Endteilnehmerzertifikaten MUSS mindestens ein Eintrag in die Erweiterung „subjectAltName“ aufgenommen werden. Zulässige Angaben sind FQDNs (als „dNSName“) oder IP-Adressen von Servern (als „iPAddress“). Wildcard FQDNs DÜRFEN eingetragen werden. Die FQDNs DÜRFEN NICHT nur aus Metazeichen bestehen und DÜRFEN das Zeichen „Underscore“ („_“) NICHT enthalten. Reservierte IP-Adressen oder interne Namen DÜRFEN NICHT eingetragen werden.

(12) [EVCP] Die in Endteilnehmerzertifikaten aufgenommenen FQDNs MÜSSEN dem Endteilnehmer gehören oder von ihm kontrolliert werden und mit dessen Dienst verknüpft sind.

BasicConstraints

(13) In Root- und Sub-CA-Zertifikaten MUSS das „cA“-Flag auf „true“ gesetzt sein. In Sub-CA-Zertifikaten DARF eine maximale Pfadlänge in „pathLenConstraints“ angegeben werden, in Root-CA-Zertifikaten SOLLTE diese Angabe NICHT gemacht werden.

(14) In Endteilnehmerzertifikaten MUSS das „cA“-Flag auf „false“ gesetzt sein. Das Feld „pathLenConstraints“ DARF NICHT gesetzt werden.

NameConstraints

(15) [SSL] [SMIME] In Sub-CA-Zertifikaten DÜRFEN Namensbeschränkungen aufgenommen werden, sie MÜSSEN aufgenommen werden, wenn die Zertifikate technisch beschränkt werden sollen. Für weitere Details wird auf Kap. 7.1.5 verwiesen.

extendedKeyUsage

(16) [SSL] In Sub-CA-Zertifikaten[4] MUSS die OID 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) eingetragen werden. Es DARF darüber hinaus die OID 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) eingetragen werden. Die OIDs 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection), 1.3.6.1.5.5.7.3.3 (id-kp-codeSigning), 1.3.6.1.5.5.7.3.8 (id-kp-timeStamping), and 2.5.29.37.0 (anyExtendedKeyUsage) DÜRFEN NICHT aufgenommen werden, andere OIDs SOLLTEN NICHT aufgenommen werden.

[3] Nicht prüfbar sind z.B. Angaben wie der User Principal Name (UPN) für Microsoft Smartcard Logon
[4] Diese Anforderung gilt für alle Sub-CA Zertifikate, die nach dem 01.01.2019 ausgestellt werden und gilt nicht für Cross-Zertifikate.

(17) [SMIME] In Sub-CA-Zertifikaten[4] MUSS die OID 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection) eingetragen werden. Es DÜRFEN weitere OIDs eingetragen werden, jedoch DÜRFEN die OIDs 2.5.29.37.0 (anyExtendedKeyUsage), 1.3.6.1.5.5.7.3.3 (id-kp-codeSigning), 1.3.6.1.5.5.7.3.8 (id-kp-timeStamping) und 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) DÜRFEN NICHT aufgenommen werden.

Anmerkung: In Sub-CA-Zertifikaten unterhalb der öffentlichen Telekom Roots, die nicht zur Ausstellung von TLS-Zertifikaten verwendet werden, DARF die OID 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) NICHT gesetzt werden.

(18) [SSL] In Endteilnehmer-Zertifikaten MUSS die OID 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) oder die OID 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) eingetragen werden, es DÜRFEN auch beide OIDs eingetragen werden. Weitere OIDs DÜRFEN NICHT eingetragen werden

(19) [SMIME] In Endteilnehmer-Zertifikaten MUSS die OID 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection) eingetragen werden. Darüber hinaus DÜRFEN weitere OIDs eingetragen werden, die OIDs 2.5.29.37.0 (anyExtendedKeyUsage), 1.3.6.1.5.5.7.3.3 (id-kp-codeSigning), 1.3.6.1.5.5.7.3.8 (id-kp-timeStamping) und 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) DÜRFEN NICHT eingetragen werden.

(20) In OCSP-Signer-Zertifikaten MUSS die OID 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning) eingetragen werden.

cRLDistributionPoints

(21) In Root- und Sub-CA-Zertifikaten MUSS die Erweiterung cRLDistributionPoints gesetzt werden, wenn für diese Zertifikate keine OCSP-Auskünfte bereitgestellt werden, ansonsten DARF diese Erweiterung gesetzt werden.

(22) [SSL] [SMIME] In Sub-CA-Zertifikaten MUSS die Erweiterung cRLDistributionPoints mit mindestens einer http-URL im Feld distributionPoints gesetzt werden.

(23) [SSL] [SMIME] In Endteilnehmerzertifikaten MUSS die Erweiterung cRLDistributionPoints mit mindestens einer http-URL im Feld distributionPoints gesetzt werden.

(23) [3145] [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten DARF die Erweiterung cRLDistributionPoints gesetzt werden. Wenn sie gesetzt wird, MUSS sie mindestens eine http- oder ldap-URL im Feld distributionPoints enthalten.

authorityInfoAccess

(24) In Root- und Sub-CA-Zertifikaten MUSS die Erweiterung authorityInfoAccess gesetzt werden, wenn für diese Zertifikate keine Sperrlisten bereitgestellt werden, ansonsten DARF diese Erweiterung gesetzt werden.

(25) [SSL] In Sub-CA-Zertifikaten MUSS die http-URL des OCSP-Responders enthalten (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)). Darüber hinaus SOLLTE auch die http-URL des relevanten Root-CA-Zertifikats enthalten sein (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).

(26) In Endteilnehmer-Zertifikaten MUSS die Erweiterung authorityInfoAccess gesetzt werden und MUSS mindestens die http-URL des OCSP-Responders enthalten (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)).

(27) [LCP] [NCP] [NCP+] [QCP] [SMIME] In Endteilnehmer-Zertifikaten MUSS die Erweiterung authorityInfoAccess zusätzlich die http-URL des relevanten Sub-CA-Zertifikats (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)) enthalten.

(27) [SSL] In Endteilnehmer-Zertifikaten SOLLTE die Erweiterung authorityInfoAccess zusätzlich die http-URL des relevanten Sub-CA-Zertifikats (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)) enthalten.

qcStatements

(28) [QCP] In Endteilnehmer-Zertifikaten MÜSSEN folgende QC Statements gesetzt werden:

- 0.4.0.1862.1.1 (QcCompliance, esi4-qcStatement-1)
- 0.4.0.1862.1.5 (QcPDS, esi4-qcStatement-5)
- 0.4.0.1862.1.6 (QcType (esi4-qcStatement-6)

Das QC Statement 0.4.0.1862.1.6 MUSS mit einem der folgenden Werte gesetzt werden.

- 0.4.0.1862.1.6.1 qct-esign
- 0.4.0.1862.1.6.2 qct-eseal
- 0.4.0.1862.1.6.3 qct-web

Darüber hinaus DÜRFEN folgende QC Statements gesetzt werden:

- 0.4.0.1862.1.2 (QcLimitValue, esi4-qcStatement-2)
- 0.4.0.1862.1.3 (QcRetentionPeriod, esi4-qcStatement-3)

Folgendes QCStatement DARF NICHT gesetzt werden:

- 0.4.0.1862.1.7 (QcCClegislation statement, esi4-qcStatement-7)

Bzgl. der zu verwendenden Syntax der QC Statements MÜSSEN die Vorgaben aus ETSI EN 319 412-5 [ETS4125] berücksichtigt werden.

(28) [QCP-n-qscd] [QCP-l-qscd] In Endteilnehmer-Zertifikaten MUSS das QC Statement 0.4.0.1862.1.4 (id-etsi-qcs-QcSSCD, esi4-qcStatement-4) gesetzt werden.

cabfOrganizationIdentifier

(29) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut cabfOrganizationIdentifier gesetzt werden, wenn im Subject-DN das Attribut organizationIdentifier gesetzt ist und MUSS eine Referenzierung auf eine Registrierung des Zertifikatsinhabers enthalten. Bzgl. der Syntax sei auf [CABFEV] verwiesen.

7.1.3 Algorithmen-OID

Root- oder Sub-CA-Zertifikate, die auf einem RSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate einen der folgenden Signaturalgorithmen verwenden:

- sha256WithRSAEncryption, OID 1.2.840.113549.1.1.11,
  Hex-codierter Wert des AlgorithmIdentifier: 300d06092a864886f70d01010b0500
- sha384WithRSAEncryption, OID 1.2.840.113549.1.1.12,
  Hex-codierter Wert des AlgorithmIdentifier: 300d06092a864886f70d01010c0500
- sha512WithRSAEncryption, OID 1.2.840.113549.1.1.13,
  Hex-codierter Wert des AlgorithmIdentifier: 300d06092a864886f70d01010d0500
- RSASSA-PSS, OID 1.2.840.113549.1.1.10
  - MGF-1 with SHA-256, and a salt length of 32 bytes, Hex-codierter Wert des AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d0609608648016503040201050 0a11c301a06092a864886f70d010108300d060960864801650304020105 00a203020120
  - MGF-1 with SHA-384, and a salt length of 48 bytes, Hex-codierter Wert des AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d0609608648016503040202050 0a11c301a06092a864886f70d010108300d060960864801650304020205 00a203020130
  - MGF-1 with SHA-512, and a salt length of 64 bytes, Hex-codierter Wert des AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d0609608648016503040203050 0a11c301a06092a864886f70d010108300d060960864801650304020305 00a203020140

Root- oder Sub-CA-Zertifikate, die auf einem P256-ECDSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate den folgenden Signaturalgorithmus verwenden:

- ecdsa-with-SHA256, OID 1.2.840.10045.4.3.2,
  Hex-codierter Wert des AlgorithmIdentifier: 300a06082a8648ce3d040302

Root- oder Sub-CA-Zertifikate, die auf einem P384-ECDSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate den folgenden Signaturalgorithmus verwenden:

- ecdsa-with-SHA384, OID 1.2.840.10045.4.3.3,
  Hex-codierter Wert des AlgorithmIdentifier: 300a06082a8648ce3d040303

Bei Zertifikaten, die auf RSA-Schlüsseln basieren, MUSS die OID 1.2.840.113549.1.1.1 (rsaEncryption) mit NULL-Parameter in der subjectPublicKeyInfo gesetzt werden. Der Hex-codierte Wert des AlgorithmIdentifier MUSS dem Wert 300d06092a864886f70d0101010500 entsprechen.

Bei Zertifikaten, die auf ECDSA-Schlüsseln basieren, MÜSSEN die OID 1.2.840.10045.2.1 (ecPublicKey) ohne NULL-Parameter und in Abhängigkeit der verwendeten Kurve einer der folgenden OIDs der subjectPublicKeyInfo gesetzt werden:

- P256: OID 1.2.840.10045.3.1.7 (prime256v1), Hex-codierter Wert des AlgorithmIdentifier: 301306072a8648ce3d020106082a8648ce3d030107
- P384: OID 1.3.132.0.34 (secp384r1), Hex-codierter Wert des AlgorithmIdentifier: 301006072a8648ce3d020106052b81040022

Die TSP MÜSSEN in ihren CPS die von ihnen verwendeten Algorithmen und Parameter aufführen.

7.1.4 Namensformen

Grundsätzliches:

- Der Name des Ausstellers in einem Zertifikat („Issuer-DN“) MUSS dem „Subject-DN“ des ausstellenden Zertifikats „Byte-für-Byte“ entsprechen.
- In Root- und Sub-CA-Zertifikaten DÜRFEN Attribute NICHT gesetzt werden, wenn Sie nicht ausdrücklich gefordert sind, d.h. grundsätzlich gilt „default deny“.
- In Root- und Sub-CA-Zertifikaten DÜRFEN alle Attribute NICHT mehr als einmal gesetzt werden.
- In Endteilnehmerzertifikaten DÜRFEN die Attribute commonName, orgnaizationIdentifier, organizationName und countryName NICHT mehr als einmal gesetzt werden.
- In die Subject-DN DÜRFEN nicht verifizierte Informationen des Zertifikatsinhabers NICHT aufgenommen werden.
- Die Subject-DN MÜSSEN für jeden Zertifikatsinhaber eindeutig sein, es DÜRFEN aber mehrere Zertifikate mit gleichem Subject-DN für einen Zertifikatsinhaber ausgestellt werden.
- Testzertifikate MÜSSEN eindeutig als solche im Subject-DN gekennzeichnet werden.

Die folgende Tabelle gibt einen Überblick über obligatorische und optionale Zertifikatserweiterungen für Root-CA-, Sub-CA-, Endteilnehmer- und OCSP-Signer-Zertifikate[5]. Erweiterungen, die dort nicht aufgeführt sind, DÜRFEN NICHT verwendet werden. Zur Kennzeichnung gelten folgende Konventionen:

- **M** (mandatorisch): Dieses Attribut MUSS gesetzt sein.
  (M) Dieses Attribut MUSS nur unter bestimmten Umständen gesetzt werden.
- **O** (optional): Dieses Attribut DARF gesetzt werden.
- **S** (sollte): Dieses Attribut SOLLTE gesetzt werden
- **SN** (sollte nicht): Dieses Attribut SOLLTE NICHT gesetzt sein.
- **N** (nicht erlaubt): Dieses Attribut DARF NICHT gesetzt sein.
- ***(nn)*** Verweis auf die der auf die Tabelle folgenden Beschreibung der zu setzenden Inhalte. Verweise in der Spalte „Subject-DN Attribut“ bedeuten, dass die aufgeführten Vorgaben übergreifend für alle Zertifikatstypen gelten.

[5] CRL-Signer-Zertifikate werden nicht aufgeführt, da die CRLs von den CAs direkt ausgestellt werden

Tabelle 7 - Namensformen

Subject-DN Attribut (OID)	Root-CA-Zertifikat	Sub-CA-Zertifikat	Endteilnehmer-Zertifikat	OCSP-Signer
commonName (2.5.4.3)	M (01)	M (01)	M, [SSL] [EVCP] O (02)	M
serialNumber (2.5.4.5)	N	N	(M) (03)	O
givenName (2.5.4.42)	N	N	(M) (04) (05)	N
surname (2.5.4.4)	N	N	(M) (06) (07)	N
pseudonym (2.5.4.65)	N	N	(M) (08)	N
streetAddress (2.5.4.9)	N	N	O (09)	O
localityName (2.5.4.7)	N	N	(M) (10)	O
stateOrProvinceName (2.5.4.8)	N	N	(M) (11)	O
postalCode (2.5.4.17)	N	N	(M) (12)	O
businessCategory (2.5.4.15)	N	N	(M) (13)	N
organizationalUnitName (2.5.4.11)	N	N	O (14)	O
organizationIdentifier (2.5.4.97)	N	(S) (15)	(M) (16) (17)	O
jurisdictionOfIncorporation-LocalityName (1.3.6.1.4.1.311.60.2.1.1)	N	N	(M) (18)	N
jurisdictionOfIncorporation-StateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	N	N	(M) (19)	N
jurisdictionOfIncorporation-CountryName (1.3.6.1.4.1.311.60.2.1.3)	N	N	(M) (20)	N
organizationName (2.5.4.10)	M (21)	M (21)	(M) (22) (23)	M
countryName (2.5.4.6)	M	M	M [SSL] [EVCP] (M) (24)	M
Sonstige Attribute	N	N	O, [EVCP] N	N

Nachfolgend werden die in den Attributen zu verwendenden Inhalte aufgelistet, sofern dazu über die Standards hinausgehende ergänzende Anforderungen existieren.

commonName

(01) [SSL] In Root- oder Sub-CA-Zertifikaten MUSS das Attribut commonName einen über alle von der ausstellenden CA erzeugten Zertifikate hinweg eindeutigen Namen enthalten. Der commonName MUSS einen gebräuchlichen Namen (d.h. nicht unbedingt der vollständige registrierte Name) des TSP beinhalten und in einer für den Markt des TSP gebräuchlichen Sprache gewählt werden.

(01) [SSL] [SMIME] In Root-CA-Zertifikaten DÜRFEN die Namen NICHT wiederverwendet werden, d.h. in Folgezertifikaten MÜSSEN andere Namen vergeben werden.

(02) [SSL] In Endteilnehmerzertifikaten DARF das Attribut commonName gesetzt werden. Wenn es gesetzt wird, MUSS es genau eine IP-Adresse oder einen FQDN enthalten, die/der auch im SubjectAltName enthalten ist. Interne Namen oder reservierte IP-Adressen DÜRFEN NICHT gesetzt werden.

(02) [EVCP] In Endteilnehmerzertifikaten DARF das Attribut commonName gesetzt werden. Wenn es gesetzt wird, MUSS es genau einen Domainnamen enthalten, den der Zertifikatsinhaber besitzt oder unter seiner Kontrolle hat und der mit dem Server des Zertifikatsinhabers verbunden ist. Der Server kann dem Zertifikatsinhaber oder einem Dritten (z.B. Hosting-Dienstleister) gehören oder von diesem betrieben werden. Widcard-Zertifikate DÜRFEN NICHT ausgestellt werden, mit Ausnahme von „onion“-Zertifikaten[6].

serialNumber

(03) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten MUSS das Attribut serialNumber gesetzt werden, wenn die Attribute countryName, commonName sowie givenName und surname oder oder pseudonym nicht ausreichen, um die Eindeutigkeit des Namens zu gewährleisten.

(03) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut serialNumber wie folgt gesetzt werden:

- Private Organisation: Das Attribut serialNumber MUSS die juristisch zugewiesene Nummer (Gründungsnummer oder eine ähnliche Nummer) des Zertifikatsinhabers enthalten. Wenn keine solche Nummer vergeben wurde, MUSS das Datum der Gründung in einem gängigen Datumsformate in diesem Feld gesetzt werden.
- Behörde: Für Behörden, die keine Registrierungsnummer oder kein Gründungsdatum haben, MUSS die CA eine geeignete Beschreibung in das Attribut serialNumber aufnehmen, um anzuzeigen, dass es sich bei dem Zertifikatsinhaber um eine Behörde handelt.
- Unternehmen: In das Attribut serialNumber MUSS die Registrierungsnummer des Unternehmens eingetragen werden. Wenn keine solche Nummer vergeben wurde, MUSS das Datum der Gründung in einem gängigen Datumsformate gesetzt werden.
- Nicht-kommerzielle Organisationen: keine Vorgabe.

Bzgl. der Syntax der serialNumber gibt es keine Vorgaben.

givenName

(04) [SSL] In Endteilnehmerzertifikaten für natürliche Personen DARF das Attribut givenName gesetzt werden, ansonsten DARF es NICHT gesetzt werden. Wenn das Attribut givenName gesetzt wird, MUSS es zusammen mit dem Attribut surname den Namen des Zertifikatsinhabers enthalten und es MUSS die Policy OID 2.23.140.1.2.3 gesetzt sein.

(05) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten für natürliche Personen MÜSSEN entweder die Attribute surname und givenName oder das Attribut pseudonym gesetzt werden, in Endteilnehmerzertifikaten für juristische Personen DÜRFEN diese Felder NICHT gesetzt werden.

[6] Siehe Appendix F der CABF EV Guidelines

surname

(06) [SSL] In Endteilnehmerzertifikaten DARF das Attribut surname gesetzt werden, ansonsten DARF es NICHT gesetzt werden. Wenn das Attribut surname gesetzt wird, MUSS es zusammen mit dem Attribut givenName den Namen des Zertifikatsinhabers enthalten und es MUSS die Policy OID 2.23.140.1.2.3 gesetzt sein.

(07) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten für natürliche Personen MÜSSEN entweder die Attribute surname und givenName oder das Attribut pseudonym gesetzt werden, in Endteilnehmerzertifikaten für juristische Personen DÜRFEN diese Felder NICHT gesetzt werden.

pseudonym

(08) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten für natürliche Personen MUSS das Attribut pseudonym gesetzt werden, wenn die Attribute surname und givenName nicht gesetzt sind, ansonsten DARF das Attribut pseudonym NICHT gesetzt werden.

streetAddress

(09) [SSL] [EVCP] In Endteilnehmerzertifikaten DARF das Attribut streetAddress gesetzt werden, wenn die Attribute surname und givenName oder organizatioName gesetzt sind, ansonsten DARF das Attribut streetAddress NICHT gesetzt werden.

(09) [EVCP] Wenn das Attribut streetAddress gesetzt wird, MUSS es die physikalische Adresse des Geschäftssitzes des Zertifikatsinhabers enthalten.

localityName

(10) [SSL] [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut localityName gesetzt werden, wenn die Attribute surname und givenName oder organizatioName gesetzt sind und das Attribut stateOrProvinceName nicht gesetzt ist. Es DARF gesetzt werden, wenn das Attribut stateOrProvinceName und die Attribute surname und givenName oder organizatioName gesetzt sind. Es DARF NICHT gesetzt werden, wenn die Attribute surname und givenName oder organizatioName nicht gesetzt sind.

Hinweis: Wenn das Attribut countryName den Code „XX“ enthält, DARF das Attribut localityName den Ort und / oder das Bundesland bzw. die Provinz des Zertifikatsinhabers enthalten.

(10) [EVCP] Wenn das Attribut gesetzt wird, MUSS es die physikalische Adresse des Geschäftssitzes des Zertifikatsinhabers enthalten.

stateOrProvinceName

(11) [SSL] [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut stateOrProvinceName gesetzt werden, wenn die Attribute surname und givenName oder organizatioName gesetzt sind und das Attribut localityName nicht gesetzt ist. Das Attribut stateOrProvinceName DARF gesetzt werden, wenn die Attribute localityName, surname und givenName oder organizatioName gesetzt sind. Es DARF NICHT gesetzt werden, wenn die Attribute surname und givenName oder organizatioName nicht gesetzt sind.

(11) [EVCP] Wenn das Attribut gesetzt wird, MUSS es die physikalische Adresse des Geschäftssitzes des Zertifikatsinhabers enthalten.

postalCode

(12) [SSL] [EVCP] In Endteilnehmerzertifikaten DARF das Attribut postalCode gesetzt werden, wenn die Attribute surname und givenName oder organizatioName gesetzt sind. Es DARF NICHT gesetzt werden, wenn die Attribute surname und givenName oder organizatioName nicht gesetzt sind.

(12) [EVCP] Wenn das Attribut gesetzt wird, MUSS es die physikalische Adresse des Geschäftssitzes des Zertifikatsinhabers enthalten.

businessCategory

(13) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut businessCategory mit dem Zutreffenden[7] der folgenden Werte gesetzt werden:

- Private Organization,
- Government Entity,
- Business Entity oder
- Non-Commercial Entity.

organizationalUnitName

(14) [SSL] [EVCP] In Endteilnehmerzertifikaten DARF das Attribut organizationalUnitName gesetzt werden, wenn die Attribute organizationName, givenName, surname, localityName und countryName gesetzt sind.

(14) [EVCP] Das Attribut organizationalUnitName DARF NICHT nur Metazeichen wie ".", "-", Leerzeichen oder andere Hinweise darauf enthalten, dass der Wert nicht vorhanden, unvollständig oder nichtzutreffend ist.

[7] Siehe CABF EV Guidelines #8.5

organizationIdentifier

(15) [LCP] [NCP] [NCP+] [QCP] In Sub-CA-Zertifikaten SOLLTE das Attribut organizationIdentifier gesetzt werden und eine Registrierungsnummer des Zertifikatsinhabers nach folgendem Schema enthalten:

- drei Zeichen für das Registrierungsschema (VAT oder NTR) oder zwei Zeichen eines Landesspezifischen Registrierungsschemas gefolgt von einem Doppelpunkt,
- zwei Zeichen für den Ländercode[8],
- einen Bindestrich („-“),
- Referenz, die gemäß dem identifizierten Registrierungsschema zugewiesen wurde.

[SSL] In Sub-CA-Zertifikaten DARF das Attribut organizationIdentifier NICHT gesetzt werden.

(16) [EVCP] In Endteilnehmerzertifikaten für juristische Personen DARF das Attribut organizationIdentifier gesetzt werden. Wenn es gesetzt wird, MUSS es eine Referenz auf die Registrierung der juristischen Person wie folgt beinhalten:

- drei Zeichen für den Identifier des Registrierungsschemas (VAT, NTR oder PSD)
- zwei Zeichen für den Ländercode[8],
- einen Bindestrich („-“),
- Referenz, die gemäß dem identifizierten Registrierungsschema zugewiesen wurde.

(17) [LCP] [NCP] [NCP+] [QCP-l] In Endteilnehmerzertifikaten für juristische Personen MUSS der organizationIdentifier gesetzt werden und MUSS eine Referenz auf die Registrierung der juristischen Person wie folgt beinhalten:

- drei Zeichen für das Registrierungsschema (VAT oder NTR) oder zwei Zeichen eines Landesspezifischen Registrierungsschemas gefolgt von einem Doppelpunkt,
- zwei Zeichen für den Ländercode[8],
- einen Bindestrich („-“),
- Referenz, die gemäß dem identifizierten Registrierungsschema zugewiesen wurde.

jurisdictionOfIncorporationLocalityName

(18) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut jurisdictionOfIncorporationLocalityName gesetzt werden, wenn die Registrierungsinstanz auf kommunaler Ebene agiert. Wenn die Registrierungsinstanz auf nationaler Ebene oder auf Ebene der Bundesländer agiert, DARF das Attribut jurisdictionOfIncorporationStateOrProvinceName NICHT gesetzt werden.

[8] ISO 3166 country codes,bei NTR ggf. auch zwei Zeichen für country sowie zwei Zeichen für state or province, getrennt durch ein “+”

jurisdictionOfIncorporationStateOrProvinceName

(19) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut jurisdictionOfIncorporationStateOrProvinceName gesetzt werden, wenn die Registrierungsinstanz auf Ebene eines Bundeslands oder auf kommunaler Ebene agiert. Wenn die Registrierungsinstanz auf nationaler Ebene agiert, DARF das Attribut jurisdictionOfIncorporationStateOrProvinceName NICHT gesetzt werden.

jurisdictionOfIncorporationCountryName

(20) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut jurisdictionOfIncorporationCountryName gesetzt werden[8].

organizationName

(21) [SSL] In Root- oder Sub-CA-Zertifikaten MUSS das Attribut organizationName gesetzt werden und es MUSS den vollständigen registrierten Namen des TSP enthalten.

(22) [SSL] In Endteilnehmerzertifikaten DARF das Attribut organizationName gesetzt werden. Wenn es gesetzt wird, muss es den verifizierten Namen oder Handelsnamen („DBA“) des Zertifikatsinhabers enthalten. Dieser darf in leicht abgeänderter Form (z.B. gebräuchliche Abkürzungen oder Verwendungen) gesetzt werden, sofern dieses nachvollziehbar ist.

(22) [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut organizationName gesetzt werden und MUSS den vollen juristischen Namen des Zertifikatsinhabers enthalten. Es DÜRFEN gebräuchliche und unmissverständliche Abkürzungen verwendet werden, oder, um die maximale Länge von 64 Zeichen nicht zu überschreiten, auch unkritische Namensbestandteile weggelassen werden, sofern der Name noch unmissverständlich erkennbar ist. Sollte das nicht möglich sein, so DARF das beantragte Zertifikat NICHT ausgestellt werden. Es DARF ein Alias oder DBA am Anfang des Felds aufgenommen werden, wenn danach noch der volle juristische Name hinzugefügt wird.

(23) [LCP] [NCP] [NCP+] [QCP-l] In Endteilnehmerzertifikaten für juristische Personen MUSS das Attribut organizationName gesetzt werden und es MUSS den vollen juristischen Namen des Zertifikatsinhabers enthalten.

countryName

(24) [SSL] [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut countryName gesetzt werden, wenn die Attribute surname und givenName oder organizatioName gesetzt sind, ansonsten DARF es gesetzt werden.

(24) [EVCP] Wenn das Attribut gesetzt wird, MUSS es die physikalische Adresse des Geschäftssitzes des Zertifikatsinhabers enthalten.

Bzgl. der Kodierung des countryName für Länder, die nicht durch einen zweistelligen Countrycode repräsentiert werden, sein auf die ISO 3166-1 verwiesen.

7.1.5 Namensbeschränkungen

In Root-CA-Zertifikaten und Endteilnehmer-Zertifikaten DÜRFEN Namensbeschränkungen NICHT gesetzt werden. In Sub-CA-Zertifikaten DÜRFEN Namensbeschränkungen enthalten sein.

[SSL] [SMIME] In Sub-CA-Zertifikaten MÜSSEN Namensbeschränkungen gesetzt werden, wenn die Sub-CA-Zertifikate technisch beschränkt werden sollen. In diesem Fall MUSS auch die Erweiterung extendedKeyUsage mit einem der Werte „id-kp-serverAuth“ oder „id-kp-emailProtection“ gesetzt werden. Wenn die Erweiterung extendedKeyUsage mit dem Wert „id-kp-serverAuth“ gesetzt ist, muss die Erweiterung nameConstraints Einschränkungen für dNSName, iPAddress und/oder DirectoryName enthalten. Wenn die Erweiterung extendedKeyUsage mit dem Wert „id-kp- emailProtection“ gesetzt ist, muss die Erweiterung nameConstraints Einschränkungen für rfc822Name mit mindestens einem erlaubten Namen enthalten.

7.1.6 OIDs der Erweiterung „Certificate Policies“

Siehe Kap. 7.1.2.

7.1.7 Verwendung der Erweiterung „Policy Constraints“

Keine Vorgabe.

[LCP, NCP, NCP+, QCP] In Endteilnehmerzertifikaten DARF die Erweiterung Policy Constraints NICHT gesetzt werden.

7.1.8 Syntax und Semantik der „Policy Qualifier“

Die Policy Qualifier MÜSSEN konform zum RFC 5280 mit den in Kap. 7.1.2 festgelegten Inhalten gesetzt werden.

7.1.9 Verarbeitungssemantik für die kritische Erweiterung „Certificate Policies“

Die Erweiterung Certificate Policies DARF NICHT als kritisch markiert werden, so dass es im Ermessen der Zertifikatsnutzer liegt, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

Alle Sperrlisten MÜSSEN den Anforderungen des RFC 5280 genügen und entweder von der CA selbst oder einem CRL-Signer signiert werden, dessen Zertifikat von der CA ausgestellt wurde.

7.2.1 Versionsnummer(n)

Alle Sperrlisten MÜSSEN im Format X.509 Version 2 ausgestellt werden.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Alle Sperrlisten MÜSSEN mindestens die Sperrlistenerweiterungen AuthorityKeyIdentifier und cRLNumber enthalten.

Die von der Root-CA ausgestellten ARLs MÜSSEN die Sperrlisteneintragserweiterung reasonCode enthalten.

[QCP] Wenn abgelaufene Zertifikate nicht aus der Sperrliste entfernt werden, muss die Sperrliste die Erweiterung "ExpiredCertsOnCRL" enthalten. Wenn abgelaufene Zertifikate aus der Sperrliste entfernt werden, darf die Sperrliste die Erweiterung "ExpiredCertsOnCRL" nicht enthalten.

Alle Erweiterungen DÜRFEN NICHT als kritisch markiert werden.

7.3 OCSP-Profil

Alle OCSP-Antworten MÜSSEN den Anforderungen des RFC 6960 genügen und entweder von der CA selbst oder einem OCSP-Signer signiert werden, dessen Zertifikat von der CA ausgestellt wurde.

Wenn die OCSP-Antworten durch einen eigens dafür vorgesehenen OCSP-Signer signiert werden, so MUSS gemäß RFC 6960 für das OCSP-Signer-Zertifikat eine der folgenden Varianten gewählt werden:

- Der TSP DARF festlegen, dass dem OCSP-Signer für die Lebensdauer des OCSP-Signer-Zertifikats vertraut werden kann. In diesem Fall MUSS die Erweiterung id-pkix-ocsp-nocheck im OCSP-Signer-Zertifikat gesetzt werden und den Wert NULL enthalten. Die Erweiterungen cRLDistributionPoints und authorityInfoAccess SOLLTEN in diesem Fall im OCSP-Signer-Zertifikat NICHT gesetzt werden und das OCSP-Signer-Zertifikat SOLLTE aufgrund der fehlenden Prüfmöglichkeit seines Status eine kurze Gültigkeitsdauer haben und regelmäßig erneuert werden.
- Der TSP DARF eine Prüfmöglichkeit des OCSP-Signer-Zertifikats in den Erweiterungen cRLDistributionPoints und/oder authorityInfoAccess festlegen.
- Der TSP DARF festlegen, dass er keine Methode zu Prüfung des Status des OCSP-Signers defeiniert und somit dem Prüfenden die Entscheidung überlässt, ob und wie er den Status des OCSP-Signer-Zertifikats prüft.

[SSL] Wenn die OCSP-Antworten durch einen eigens dafür vorgesehenen OCSP-Signer signiert werden, so MUSS für das OCSP-Signer-Zertifikat die erste der oben aufgeführten Varianten gewählt werden, d.h. es MUSS die Erweiterung id-pkix-ocsp-nocheck im OCSP-Signer-Zertifikat gesetzt werden und den Wert NULL enthalten.

7.3.1 Versionsnummer(n)

Es MUSS OCSP in der Version 1 (Wert „0“) gemäß RFC 6960 eingesetzt werden.

7.3.2 OCSP-Erweiterungen

Keine Vorgabe.

[QCP] Die Erweiterung „ArchiveCutOff“ soll in der Antwort mit dem Zeitpunkt des Gültigkeitsbeginns des referenzierten CA-Zertifikats gesetzt werden.

8 AUDITS UND ANDERE BEWERTUNGSKRITERIEN

Keine Vorgabe.

[SSL] [SMIME] Root- und Sub-CA-Zertifikate sowie Cross-Zertifikate, die geeignet sind, weitere Sub-CA-Zertifikate auszustellen, MÜSSEN entweder technisch beschränkt werden (siehe Kap. 7.1.2 und 7.1.5) oder öffentlich bekannt gegeben und in Übereinstimmung mit allen Anforderungen dieses Kapitels vollständig geprüft werden.

8.1 Häufigkeit und Art der Prüfungen

8.1.1 Selbstüberprüfung

Keine Vorgabe.

[SSL] Die TSP MÜSSEN in dem Zeitraum, in dem sie Endteilnehmerzertifikate ausstellen, durch geeignete Selbstüberprüfungen die Einhaltung der Vorgaben dieser CP und der anwendbaren CPS sowie ihre Servicequalität kontrollieren. Diese Selbstüberprüfungen MÜSSEN mindestens vierteljährlich erfolgen und MÜSSEN stichprobenartig eine zufällige Auswahl von mindestens drei Prozent der Endteilnehmerzertifikate[9] umfassen, die seit der letzten Selbstüberprüfung ausgestellt wurden.

Für TSP, welche technisch beschränkte Sub-CAs ausstellen, gelten die o.g. Anforderungen analog, d.h. diese MÜSSEN von allen technisch beschränkten Sub-CAs ausgestellte Endteilnehmerzertifikate in gleicher Art und Weise prüfen.

[EVCP] Abweichend zu den vorgenannten Anforderungen zu [SSL] MÜSSEN die TSP laufend Selbstüberprüfungen durchführen.

8.1.2 Prüfungen durch externe Auditoren

Keine Vorgabe.

[SSL] [SMIME] Die TSP MÜSSEN in einer ununterbrochenen Folge von Audit-Perioden gemäß eines in Kap. 8.4 gelisteten und für [SSL] bzw. [SMIME] anwendbaren Auditschemas geprüft werden („Period-of-time-Audits“), dabei DARF eine Periode die Zeitdauer von einem Jahr NICHT überschreiten.

TSP, die noch nicht in einem Period-of-time-Audit geprüft wurden, MÜSSEN zu einem Zeitpunkt innerhalb von 12 Monaten vor der Ausgabe von öffentlichen Zertifikaten eine Prüfung der Bereitschaft zur Ausgabe von Zertifikaten in Übereinstimmung mit dem entsprechenden Auditschema durchführen („Point-in-time Audit“). Nach Ausgabe des ersten öffentlichen Zertifikats MUSS der TSP innerhalb von 90 Tagen vollständig in einem Period-of-time-Audit geprüft werden.

[9] mindestens ein Zertifikat, sofern weniger als 33 Zertifikate ausgestellt wurden

TSP, die bereits in einem Period-of-time-Audit geprüft wurden benötigen kein Point-in-time-Audit vor der Ausstellung von Zertifikaten.

Anmerkung: “Point-in-time”-Audits DÜRFN genutzt werden, um z.B. nachzuweisen, dass in einem vorangegangenen Audit gefundene Abweichungen behoben wurden, sie DÜRFEN aber NICHT ein Period-of-time-Audit ersetzen.

[EVCP] Die o.g. Anforderungen zu [SSL] [SMIME] gelten analog für [EVCP] unter Anwendung der in Kap. 8.4 gelisteten und für [EVCP] anwendbaren Auditschemata. Darüber hinaus MUSS bei [EVCP] immer innerhalb von 12 Monaten vor der ersten Ausgabe von EV-Zertifikaten ein Point-in-time-Audit erfolgen, unabhängig davon, ob bereits ein Period-of-time-Audit erfolgt ist oder nicht.

[3145] Die TSP MÜSSEN jährlich von einem unabhängigen externen ISO27001-Auditor geprüft werden.

8.1.3 Prüfungen von Unterauftragnehmern und delegierten Dritten

Keine Vorgabe.

[SSL] Analog zur Selbstüberprüfung gemäß Kap. 8.1.1 MÜSSEN die TSP mindestens vierteljährlich Zertifikate prüfen, welche von delegierten Dritten ausgestellt wurden oder Informationen enthalten, welche von delegierten Dritten geprüft wurden, es sei denn, der delegierte Dritte wird selbst gemäß Kap. 8.1.2 geprüft. Für diese Prüfung MÜSSEN die TSP einen eigenen Validierungsspezialisten einsetzen.

Darüber hinaus MÜSSEN die TSP die Praktiken und Verfahren aller delegierten Dritten mindestens jährlich bzgl. der Einhaltung der Anforderungen dieser CP und der anwendbaren CPS überprüfen.

[3145] Unterauftragnehmer oder delegierte Dritte MÜSSEN in den anwendbaren Bereichen in demselben Umfang gemäß den Anforderungen aus [3145] geprüft werden, wie der Betrieb des TSP selbst. Diese Anforderung MUSS vertraglich mit den Unterauftragnehmern oder delegierten Dritten vereinbart werden.

8.2 Identität/Qualifikation der Prüfer

Interne Auditoren, welche die Selbstüberprüfungen gemäß Kap. 8.1.1 sowie die Prüfungen von Unterauftragnehmern und delegierten Dritten gemäß Kap. 8.1.3 durchführen, MÜSSEN über hinreichende Erfahrung als Auditoren und Expertise zu PKI-Technologien und -Prozessen verfügen.

[SSL] [SMIME] Bei den externen Prüfern, welche die Prüfungen gemäß Kap. 8.1.2 durchführen, MUSS es sich um qualifizierte Auditoren handeln, die über folgende Qualifikationen und Fähigkeiten verfügen:

- sie MÜSSEN unabhängig vom Prüfgegenstand sein,
- sie MÜSSEN Prüfungen durchführen können, welche die in geeigneten Prüfungsschemata gemäß Kap. 8.4 festgelegten Kriterien erfüllen,
- sie MÜSSEN Personen beschäftigen, die kompetent in der Prüfung von PKI-Technologien, Informationssicherheits-Tools und -Techniken, Informationstechnologien und Sicherheitsüberprüfungen sind und die Funktion der Bestätigung als Drittpartei beherrschen,
- sie MÜSSEN durch Gesetz, staatliche Vorschriften oder berufsethische Regeln gebunden sein und
- sie MÜSSEN eine Berufshaftpflicht-, Fehler- und Unterlassungsversicherung mit einer Deckungssumme von mindestens einer Million US-Dollar unterhalten.

Für Prüfungen gemäß der ETSI-Standards MÜSSEN die Prüfer darüber hinaus gemäß ISO 17065 unter Anwendung der in ETSI EN 319 403 festgelegten Anforderungen akkreditiert sein.

Für Prüfungen gemäß der Webtrust-Standards MÜSSEN die Prüfer darüber hinaus von WebTrust lizensiert sein.

[QCP] Die TSP MÜSSEN von Konformitätsbewertungsstellen geprüft werden, welche die Voraussetzungen aus ETSI EN 319 403 erfüllen.

8.3 Beziehung des Prüfers zur geprüften Stelle

Externe Prüfer, welche die Prüfungen gemäß Kap. 8.1.2 durchführen, MÜSSEN unabhängig von der geprüften Stelle und dem Prüfgegenstand sein.

Für interne Auditoren MUSS die Rollentrennung gemäß Kap. 5.2.4 beachtet werden.

8.4 Abgedeckte Bereiche der Prüfung

Keine Vorgabe.

[SSL] [SMIME] Die TSP MÜSSEN gemäß einem der folgenden Schemata geprüft werden:

- WebTrust Principles and Criteria for Certification Authorities ab Version 2.1 inkl. WebTrust for CAs SSL Baseline with Network Security ab Version 2.3
- ETSI EN 319 411-1 ab Version 1.2.2 oder ETSI 319 411-2 ab Version 2.2.2

[SSL] anwendbare Policies der o.g. ETSI Dokumente sind
- LCP in Verbindung mit DVCP oder OVCP oder
- QCP-w.

[SMIME] anwendbare Policies der o.g. ETSI Dokumente sind
- LCP,
- NCP,
- NCP+,

- QCP-l,
- QCP-l-qscd,
- QCP-n oder
- QCP-n-qscd.

[EVCP] Der Root-TSP und die TSP MÜSSEN gemäß einem der folgenden Schemen geprüft werden:

- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL ab Version 1.6.2,
- ETSI EN 319 411-1 ab Version 1.2.2, bei Anwendung von QCP-w zusätzlich ETSI 319 411-2 ab Version 2.2.2
  Anwendbare Policies der o.g. ETSI Dokumente sind
  - NCP in Verbindung mit EVCP oder
  - QCP-w in Verbindung mit EVCP

[3145] Der Auditprozess MUSS das ISMS und die Anforderungen der [TR3145] umfassen

8.5 Maßnahmen infolge von Mängeln

Mängel MÜSSEN in den von den internen oder externen Prüfern festgelegten Fristen beseitigt werden.

[SSL] [SMIME] Mängel, die gegen die [BR], [MSRP], [MOZRP], [GGLRP] oder [APLRP] verstoßen, MÜSSEN den betroffenen Root-Programmen gemeldet werden. Sofern fehlerhafte Zertifikate bemängelt werden, MÜSSEN die Sperrgründe und -Fristen gemäß Kap. 4.9.1 berücksichtigt werden.

8.6 Mitteilung der Ergebnisse

Keine Vorgabe.

[SSL] [SMIME] Die TSP MÜSSEN die von den externen Prüfern erstellten Audit-Bescheinigungen aller technisch nicht beschränkten Root- und Sub-CAs in der „Common CA Database“ (CCADB) veröffentlichen.

Die TSP SOLLTEN diese Bescheinigungen innerhalb von drei Monaten nach Ende der Prüfung veröffentlichen. Im Falle einer Verzögerung von mehr als drei Monaten MÜSSEN die TSP ein von dem externen Prüfer unterzeichnetes Erläuterungsschreiben vorlegen.

Die externen Prüfer MÜSSEN bei der Erstellung der Audit-Bescheinigungen die Vorgaben an die Form und Inhalte aus Kap. 5.1 der CCADB-Policy („Audit Statement Content“, siehe https://www.ccadb.org/policy) berücksichtigen.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

9.1.1 Gebühren für die Ausstellung oder Erneuerung von Zertifikaten

Keine Vorgabe.

9.1.2 Gebühren für den Zertifikatszugang

Keine Vorgabe.

9.1.3 Gebühren für den Zugang zu Sperr- oder Statusinformationen

Keine Vorgabe.

9.1.4 Gebühren für andere Dienstleistungen

Keine Vorgabe.

9.1.5 Rückerstattungsrichtlinie

Keine Vorgabe.

9.2 Finanzielle Verantwortlichkeiten

Die TSP MÜSSEN über die finanzielle Stabilität und Ressourcen verfügen, die zu einem zu dieser CP konformen Betrieb inkl. einer geplanten Einstellung gemäß Kap. 5.8 erforderlich sind. Darüber hinaus MÜSSEN die TSP, soweit dies im Rahmen der geltenden Insolvenzgesetze möglich ist, Vereinbarungen zur Deckung der Kosten treffen, um die Mindestanforderungen gemäß Kap. 5.8 im Insolvenzfall erfüllen zu können.

9.2.1 Versicherungsschutz

Die TSP MÜSSEN eine angemessene Haftpflichtversicherung gemäß geltendem Recht abschließen, wenn sie nicht über hinreichende finanzielle Ressourcen zur Absicherung etwaiger Haftungsforderungen aufgrund vorsätzlicher oder fahrlässiger Handlungen verfügen.

[EVCP] Die TSP MÜSSEN eine in Bezug auf ihre Leistungen und Verpflichtungen gemäß dieser CP folgende Haftpflichtversicherungen abschließen:

- eine allgemeine Haftpflichtversicherung mit einer Deckungssumme von mindestens 2 Mio. US-Dollar, sowie
- eine Berufshaftpflichtversicherung mit einer Deckungssumme von mindestens 5 Mio. US-Dollar, welche Schadensersatzansprüche aufgrund
  - einer Handlung, eines Fehlers oder einer Unterlassung,
  - einer unbeabsichtigten Vertragsverletzung,
  - einer Vernachlässigung bei der Ausstellung oder dem Betrieb von EV-Zertifikaten,
  - einer Verletzung der Eigentumsrechte Dritter (ausgenommen Urheberrechts- und Markenrechtsverletzung),
  - einer Verletzung der Privatsphäre oder
  - einer Verletzung der Werbung

  abdeckt.

Diese Versicherung MUSS bei einem Unternehmen abgeschlossen sein, das in der aktuellen Ausgabe des „Best's Insurance Guide“ ein Rating von mindestens „A“ aufweist.

9.2.2 Sonstige Vermögensgegenstände

Keine Vorgabe.

9.2.3 Versicherungs- oder Garantiedeckung für Endteilnehmer

Keine Vorgabe.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang an vertraulichen Informationen

Keine Vorgabe.

9.3.2 Umfang an nicht vertraulichen Informationen

Keine Vorgabe.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die TSP MÜSSEN vertrauliche Geschäftsinformationen ihrer Klassifizierung entsprechend angemessen schützen.

9.4 Schutz von personenbezogenen Daten

9.4.1 Datenschutzkonzept

Die TSP MÜSSEN die Vorgaben des Bundesdatenschutzgesetzes [BDSG] beachten und DÜRFEN NICHT Daten erheben, die zur Erbringung der Dienstleistung nicht relevant oder angemessen sind.

Die TSP MÜSSEN in ihren Datenschutzkonzepten beschreiben, wie sie Vorgaben des [BDSG] bzgl. der im Registrierungsprozess erhobenen Daten umsetzen. Die TSP MÜSSEN zum Schutz der personenbezogenen Daten geeignete technische und organisatorische Maßnahmen

- zur Wahrung der Integrität und Vertraulichkeit bei der Übermittlung und Speicherung,
- gegen eine unerlaubte oder unrechtmäßige Verarbeitung,
- gegen einen zufälligen Verlust oder die zufällige Zerstörung oder Beschädigung

dieser Daten ergreifen.

9.4.2 Als privat zu behandelnde Informationen

Die TSP MPÜSSEN in ihren CPS die als privat zu behandelnde Informationen beschreiben.

9.4.3 Nicht als privat geltende Informationen

Die TSP MPÜSSEN in ihren CPS die nicht als privat geltende Informationen beschreiben.

9.4.4 Verantwortung für den Schutz privater Informationen

Die TSP MÜSSEN in ihren CPS die Verantwortung für den Schutz privater Informationen beschreiben.

9.4.5 Benachrichtigung und Zustimmung zur Verwendung privater Informationen

Die TSP MÜSSEN in ihren CPS die Methoden zur Benachrichtigung der Betroffenen sowie die Einholung der Zustimmung zur Verwendung privater Informationen beschreiben.

9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

Die TSP MÜSSEN in ihren CPS die Bedingungen zur Offenlegung personenbezogener Daten im Rahmen von Gerichts- oder Verwaltungsverfahren beschreiben.

9.4.7 Andere Umstände der Offenlegung von Informationen

Keine Vorgabe.

9.5 Urheberrecht

Keine Vorgabe.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der TSP

Die TSP MÜSSEN zuverlässig sein und ihre Dienste auf vertrauenswürdige und legale Art und Weise konform zu dieser CP und ihren CPS betreiben.

Die TSP MÜSSEN die Gesamtverantwortung für die Einhaltung der Konformität zu dieser CP und ihren CPS auch dann behalten, wenn sie Tätigkeiten an Unterauftragnehmer oder Dritte auslagern. Die TSP MÜSSEN dazu die Aufgaben der Dritten und die damit verbundenen Verfahrensweisen, Verantwortlichkeiten und Haftungsbedingungen festlegen und diese vertraglich verpflichten, alle geforderten Maßnahmen umsetzen.

[3145] Wenn Dritte im Rahmen des Identifizierungs- und Registrierungsverfahrens Dienstleistungen für einen TSP erbringen, MUSS der TSP für diese das Sicherheitsniveau "hoch" gewährleisten und die Zuverlässigkeit des Dritten sowie die Vertrauenswürdigkeit des vom Dritten eingesetzten Personal verlangen. Hierzu MUSS der TSP mit dem Dritten eine unterzeichnete Vereinbarung abschließen, die darüber hinaus auch die im vorherigen Absatz aufgeführten Aspekte beinhaltet.

Die von den TSP betriebenen Dienste DÜRFEN NICHT diskriminierend sein und SOLLTEN allen Antragstellern zugänglich gemacht werden,

- deren Tätigkeiten in den von den Diensten angegebenen Tätigkeitsbereich fallen und
- die sich damit einverstanden erklären, ihren in den Geschäftsbedingungen des TSP festgelegten Verpflichtungen nachzukommen.

Die den Endteilnehmern angebotenen Dienste und Produkte MÜSSEN soweit möglich auch Menschen mit Behinderungen zugänglich gemacht werden, anwendbare Standards zur Barrierefreiheit aus ETSI EN 301 549 SOLLTEN berücksichtigt werden.

Die TSP MÜSSEN Dritten die Möglichkeit bieten, alle angebotenen Zertifikatstypen zu überprüfen und zu testen, z.B. durch Veröffentlichung von PKCS#12-Zertifikaten auf ihrer Website.

Vor Abschluss eines Vertragsverhältnisses mit einem Endteilnehmer MÜSSEN die TSP den Endteilnehmer über die Nutzungsbedingungen zur Verwendung der Zertifikate gemäß Kap. 9.6.3 informieren.

[SSL] Der Root-TSP MUSS verantwortlich sein für

- die Leistungen und Gewährleistungen der TSP,
- die Einhaltung dieser CP durch die TSP,
- alle Verbindlichkeiten und Freistellungsverpflichtungen der TSP gemäß diesen Anforderungen,

als ob er selbst der TSP wäre, der die Zertifikate ausstellt.

Die TSP MÜSSEN für jedes von ihnen ausgestellte Zertifikat sowohl den Endteilnehmern, den Anbietern der Anwendungssoftware, mit denen der Root-TSP eine Vereinbarung zur Aufnahme der Root-Zertifikate in die Trusted Rootstores getroffen hat, als auch allen vertrauenden Dritten garantieren, dass

- der Endteilnehmer das Recht hat, die im Zertifikat (im subjectDistinguishedName und/oder subjectAltName) aufgeführten Domainnamen oder IP-Adressen zu verwenden,
- sofern anwendbar, der Vertreter des Endteilnehmers autorisiert war, das Zertifikat im Namen des Endteilnehmers zu beantragen,
- sie von den Endteilnehmern zur Ausstellung der Zertifikate autorisiert waren,
- die Richtigkeit aller im Zertifikat aufgenommenen Inhalte, mit Ausnahme der Angaben im Attribut organizationalUnitName, überprüft wurde und die Angaben im Attribut organizationalUnitName wahrscheinlich nicht irreführend sind,
- der Antragsteller gemäß Kap. 3.2 identifiziert wurde,
- sie, sofern der Endteilnehmer nicht mit dem TSP verbunden ist, mit dem Endteilnehmer einen rechtsgültigen und durchsetzbaren Vertrag, der alle relevanten Anforderungen erfüllt, abgeschlossen haben,
- sofern der Endteilnehmer mit dem TSP verbunden ist, ein Vertreter des Antragstellers die Nutzungsbedingungen anerkannt hat,
- sie mindestens bis zum Ablaufdatum des Zertifikats Statusdienste gemäß Kap. 4.10 betreiben und Statusinformationen rund um die Uhr öffentlich bereitstellen,
- sie ein Zertifikat bei Vorliegen eines der im CPS aufgeführten Sperrgründe sperren,
- sie während der gesamten Gültigkeitsdauer eines Zertifikats die Anforderungen dieser CP sowie ihrer eigenen CPS einhalten.

Die TSP MÜSSEN die zur Einhaltung der vorgenannten Zertifikatsgarantien erforderlichen Prozesse und Maßnahmen in ihren CPS beschreiben.

Die TSP SOLLTEN einen geeigneten Kommunikationskanal zu allen Endteilnehmern haben, um diese im Bedarfsfall über Änderungen zu informieren.

Die TSP MÜSSEN sicherstellen, dass die Verträge mit den Endteilnehmern inkl. der Nutzungsbedingungen (siehe Kap. 9.6.3) rechtlich durchsetzbar sind. Die Akzeptanz der Vereinbarung DARF, sofern rechtlich durchsetzbar, elektronisch erfolgen. Die TSP DÜRFEN für jedes Zertifikat eine eigene Vereinbarung oder auch eine Vereinbarung, die für mehrere Zertifikate gilt, akzeptieren.

[EVCP] Ein TSP MUSS für jedes ausgestellte EV-Zertifikat gewährleisten, dass

- er sich bei einer Gründungs- oder Registrierungsagentur in der Gründungs- oder Registrierungsgerichtsbarkeit des Endteilnehmers vergewissert hat, dass der Endteilnehmer als rechtlich gültige Organisation oder gültiges Unternehmen existiert,
- der Name des Endteilnehmers zum Zeitpunkt der Ausstellung des Zertifikats mit dem Namen in den offiziellen Registrierungsunterlagen übereinstimmt und im Falle eines enthaltenen Pseudonyms auch dieses ordnungsgemäß in der Gerichtsbarkeit des Geschäftssitzes ordnungsgemäß registriert ist,
- er alle zumutbaren Schritte unternommen, um zu überprüfen, ob
  - der Endteilnehmer zum Zeitpunkt der Ausstellung des Zertifikats das Recht hat, alle im Zertifikat aufgeführten Domainnamen zu verwenden,
  - der Endteilnehmer die Ausstellung des Zertifikats genehmigt hat,
  - alle anderen Informationen im Zertifikat zum Zeitpunkt der Ausstellung des Zertifikats korrekt waren,

- er mit einem Endteilnehmer, der nicht mit ihm verbunden ist, eine rechtsgültige und durchsetzbare Vereinbarung getroffen hat, die alle Anforderungen aus [EVCG] berücksichtigt.

[QCP] TSP, welche private Schlüssel der Endteilnehmer während der Gültigkeitsdauer der korrespondierenden Zertifikate verwalten, SOLLTEN dies in ihren CPS beschreiben. Darüber hinaus DARF diese Information auch im Zertifikat des Endteilnehmers aufgeführt werden.

9.6.2 Zusicherungen und Gewährleistungen externer RAs

Siehe Kap. 5.3.7, 6.5.1 und 9.6.1.

9.6.3 Zusicherungen und Gewährleistungen der Endteilnehmer

Die TSP MÜSSEN gegenüber den Endteilnehmern die Nutzungsbedingungen für die Endteilnehmerzertifikate festlegen und von den Endteilnehmern vor der Ausstellung der Zertifikate deren Akzeptanz bestätigen lassen. Diese Nutzungsbedingungen MÜSSEN mindestens folgende Verpflichtungen des Endteilnehmers berücksichtigen:

a) eine Verpflichtung, dem TSP genaue und vollständige Informationen zu liefern,
b) eine Verpflichtung, das Schlüsselpaar nur in Übereinstimmung mit etwaigen Einschränkungen, die dem Endteilnehmer mitgeteilt wurden, zu verwenden,
c) ein Verbot der unerlaubten Nutzung der privaten Endteilnehmer-Schlüssel,
d) eine Verpflichtung, den TSP unverzüglich zu benachrichtigen, wenn während der Gültigkeitsdauer eines Zertifikats eines der folgenden Ereignisse eintritt:
   - ein privater Schlüssel ist verloren gegangen, gestohlen oder möglicherweise kompromittiert worden,
   - die Kontrolle über einen privaten Schlüssel ist verloren gegangen, z.B. aufgrund einer Kompromittierung von Aktivierungsdaten (z. B. PIN-Code) oder aus anderen Gründen,
   - es werden Inkorrektheiten oder notwendige Änderungen der Zertifikatsinhalte festgestellt,
e) eine Verpflichtung, nach Kompromittierung eiens privaten Schlüssels die Verwendung dieses Schlüssels, mit Ausnahme der Schlüsselentschlüsselung, sofort und dauerhaft einzustellen,
f) eine Verpflichtung, ein Zertifikat unverzüglich zu sperren oder sperren zu lassen, wenn ein Sperrgrund gemäß Kap. 4.9.1.2 vorliegt.
g) eine Verpflichtung, nach Sperrung des Endteilnehmerzertifikats die Verwendung des korrespondierenden privaten Schlüssels, mit Ausnahme der Schlüsselentschlüsselung, sofort und dauerhaft einzustellen,
h) eine Verpflichtung, nach Bekanntwerden der Kompromittierung der ausstellenden Sub-CA die Verwendung des privaten Endteilnehmer-Schlüssels, mit Ausnahme der Schlüsselentschlüsselung, sofort und dauerhaft einzustellen,
i) für den Fall, dass ein Endteilnehmer seine Schlüssel selbst generiert:
   eine Verpflichtung zur Generierung der Schlüssel unter Verwendung geeigneter Algorithmen und Schlüssellängen gemäß Kap. 6.1.5,
j) für den Fall, dass ein Endteilnehmer eine natürliche Person ist und seine Schlüssel selbst generiert und diese für eine „Verpflichtung zu signierten Inhalten“ (siehe Kap. 7.1.2 (06) bzgl. KeyUsage „nonRedudiation“) genutzt werden:

eine Verpflichtung, dass der private Schlüssel unter der alleinigen Kontrolle des Endteilnehmers aufbewahrt wird,

k) für den Fall, dass ein Endteilnehmer eine juristische Person ist und seine Schlüssel selbst generiert und diese für eine „Verpflichtung zu signierten Inhalten“ (siehe Kap. 7.1.2 (06) bzgl. KeyUsage „nonRedudiation“) genutzt werden:
eine Verpflichtung, den privaten Schlüssel unter der Kontrolle des Endteilnehmers zu halten,

l) [NCP+] eine Verpflichtung, den privaten Schlüssel für kryptografische Funktionen nur innerhalb sicherer kryptografischer Module zu verwenden,

m) [NCP+] für den Fall, dass die Schlüssel unter der Kontrolle des Endteilnehmers generiert werden: eine Verpflichtung, die Schlüssel innerhalb des sicheren kryptografischen Moduls zu generieren,

n) [SSL] eine Verpflichtung, alle angemessenen Maßnahmen zu ergreifen, um die Vertraulichkeit und Kontrolle über die privaten Schlüssel und Aktivierungsdaten zu gewährleisten,

o) [SSL] eine Verpflichtung, den Inhalt des Zertifikats auf Richtigkeit zu überprüfen,

p) [SSL] eine Verpflichtung, das Zertifikat nur auf Servern zu installieren, auf die unter den im Zertifikatsattribut subjectAltName aufgeführten Namen zugegriffen werden kann,

q) [SSL] eine Verpflichtung, das Zertifikat ausschließlich in Übereinstimmung mit allen geltenden Gesetzen und in Übereinstimmung mit der abgeschlossenen Vereinbarung und den Nutzungsbedingungen zu nutzen,

r) [SSL] eine Verpflichtung, innerhalb eines bestimmten Zeitraums auf die Anweisungen des TSP bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauch zu reagieren,

s) [SSL] eine Verpflichtung zu akzeptieren, dass ein TSP berechtigt ist, ein Zertifikat sofort zu sperren, wenn ein Sperrgrund gemäß Kap. 4.9.1.2 vorliegt,

t) [3145] eine Verpflichtung, jede Änderung der Registrierungsdaten dem TSP mitzuteilen und spätestens nach Ablauf der unter rr) festgelegten Frist zu bestätigen, dass die Registrierungsdaten noch gültig sind,

u) [3145] für den Fall, dass ein Endteilnehmer die Schlüssel selbst generiert:
- eine Verpflichtung, die Schlüssel gemäß den Vorgaben zu generieren und aufzubewahren (siehe dazu auch ss) und tt)),
- eine Verpflichtung, die Schlüssel vor unerlaubtem Zugriff und Manipulation zu schützen,

v) [3145] für den Fall, dass die TSP die Schlüssel der Endteilnehmer auf Token generieren und übergeben: eine Verpflichtung zur Meldung einer Kompromittierung der Aktivierungsdaten im Rahmen der Tokenübergabe, was zu einer Sperrung des Zertifikats führt,

w) [3145] eine Verpflichtung, das Endteilnehmerzertifikat sowie das ausstellende Sub-CA-Zertifikat zu prüfen,

x) [QCP-n-qscd] eine Verpflichtung, elektronische Signaturen ausschließlich mittels QSCD zu erzeugen,

y) [QCP-n-qscd] eine Verpflichtung, den Schlüssel unter seiner alleinigen Kontrolle zu halten,

z) [QCP-l-qscd] eine Verpflichtung, den Schlüssel unter der Kontrolle des Subjekts des Zertifikats zu halten,

aa) [QCP-n-qscd] eine Verpflichtung, den Schlüssel ausschließlich zur Erzeugung elektronischer Signaturen zu nutzen,
bb) [QCP-l-qscd] eine Verpflichtung, den Schlüssel ausschließlich zur Erzeugung elektronischer Siegel zu nutzen.

Darüber hinaus MÜSSEN die Nutzungsbedingungen Informationen zu folgenden Aspekten enthalten:

cc) die anwendbare Policy gemäß ETSI EN 319 411-1 bzw. -2,
dd) eine Information, was als Akzeptanz des Zertifikats gilt,
ee) der Zeitraum, über den die Aufzeichnungen (siehe Kap. 5.5.2) aufbewahrt werden,
ff) die Anforderungen an vertrauende Dritte gemäß Kap. 9.6.4,
gg) ob und wenn ja, auf welche Art und Weise die Anforderungen dieser CP ergänzt oder weiter einschränkt werden,
hh) alle Beschränkungen der Nutzung des angebotenen Dienstes,
ii) die Haftungsbeschränkungen der TSP,
jj) das anwendbare Recht,
kk) die Verfahren bei Beschwerden und zur Streitbeilegung,
ll) Häufigkeit und zugrundeliegende Auditschemata der Auditierungen der TSP gemäß Kap. 8.1 und 8.4,
mm) Kontaktinformationen des TSP,
nn) Aussagen zur Verfügbarkeit der bereitgestellten Dienste,

oo) [3145] die Art und Weise, wie die Endteilnehmer die Registrierungsdaten übertragen können,
pp) [3145] Regelungen zur Akzeptanz neuer Versionen der Nutzungsbedingungen durch die Endteilnehmer in Übereinstimmung mit den geltenden Gesetzen,
qq) [3145] eine Definition der verschiedenen Rollen der Endteilnehmer (z.B. Antragsteller, Subjekt des Zertifikats), der verschiedenen möglichen Subjekte eines Zertifikats (z.B. natürliche Personen, natürliche Personen in Verbindung mit einer juristischen Person, juristische Personen), sowie weiterer bedeutender Rollen in den Zertifikatsmanagementprozessen,
rr) [3145] eine Frist, nach deren Ablauf die Endteilnehmer bestätigen müssen, dass ihre Registrierungsdaten weiterhin gültig sind (siehe dazu auch 0),
ss) [3145] weitere Vorgaben an die Endteilnehmer in Abhängigkeit des geforderten Sicherheitsniveaus (z.B. Virenschutz, Firewalls sowie regelmäßiges Einspielen von Sicherheitsupdates der Betriebssysteme, angemessener Schutz der Schlüssel und Aktivierungsdaten, Nutzung von sicheren kryptografischen Modulen bei hohem Sicherheitsniveau),
tt) [3145] für den Fall, dass ein Endteilnehmer die Schlüssel selbst generiert: die Anforderungen an die zur Schlüsselgenerierung verwendete Hard- und Software,
uu) [3145] für den Fall, dass die TSP die Schlüssel der Endteilnehmer generieren: der Prozess der Schlüsselübergabe,
vv) [3145] für den Fall, dass die TSP die Schlüssel der Endteilnehmer auf Token generieren und übergeben: der Prozess der Übergabe der Token,
ww) [3145] der Prozess der Veröffentlichung neuer Sub-CA-Zertifikate,
xx) [3145] die Voraussetzungen für eine Zertifikatserneuerung mit oder ohne Schlüsselwechsel sowie für die Ausstellung eines Ersatzzertifikats,

yy) [3145] Informationen über den Prozess der Beendigung eines TSP oder einer RA (siehe Kap. 5.8),
zz) [3145] Informationen über die Fristen zur Umsetzung von Sperrungen und deren Wirksamkeit in den Statusdiensten,
aaa) Informationen über die Fristen der regelmäßigen Updates der Statusdienste.

Für den Fall, dass der Antragsteller nicht das Subjekt des Zertifikats ist und das Subjekt des Zertifikats eine natürliche oder juristische Person ist

1) MÜSSEN für das Subjekt des Zertifikats die o.g. Verpflichtungen c), d), e), f), g), h) j) und l) gelten und für den Fall, dass das Subjekt des Zertifikats eine Person ist, MUSS diese drüber informiert werden,
2) MUSS die Vereinbarung mit dem Endteilnehmer aus zwei Teilen bestehen,
   a) Der erste Teil MUSS vom Antragsteller unterzeichnet werden und MUSS folgende Aspekte berücksichtigen:
      i) Zustimmung zu den Verpflichtungen des Antragstellers,
      ii) Zustimmung zur Nutzung eines sicheren kryptografischen Moduls, sofern das gefordert ist,
      iii) Zustimmung zur Verarbeitung der erhobenen Daten und, sofern anwendbar, die Weitergabe dieser Daten an vom TSP beauftragte Dritte, inkl. einer Weitergabe der Daten im Falle einer Beendigung des Dienstes,
      iv) Bedingungen zur Veröffentlichung des Zertifikats auf Verlangen des Antragstellers unter Zustimmung des Subjekts des Zertifikats,
      v) Bestätigung der Korrektheit aller im Zertifikat aufzunehmenden Daten,
      vi) Verpflichtungen, die für das Subjekt des Zertifikats gelten (informativ).
   b) Der zweite Teil MUSS vom Subjekt des Zertifikats unterzeichnet werden und MUSS folgende Aspekte berücksichtigen:
      i) Zustimmung zu den Verpflichtungen des Subjekts des Zertifikats (siehe 1)),
      ii) Zustimmung zur Nutzung eines sicheren kryptografischen Moduls, sofern das gefordert ist,
      iii) Zustimmung zur Verarbeitung der erhobenen Daten und, sofern anwendbar, die Weitergabe dieser Daten an vom TSP beauftragte Dritte, inkl. einer Weitergabe der Daten im Falle einer Beendigung des Dienstes.

   Anmerkung: Die beiden Teile der Vereinbarung DÜRFEN zusammen von einer Person unterschrieben werden, wenn der Antragsteller zugleich ein offizieller Vertreter der juristischen Person ist, welche auch das Subjekt des Zertifikats darstellt oder wenn der der offizielle Vertreter des Unterzeichners auch gelichzeitig das Subjekt des Zertifikats darstellt.

[3145] Die Nutzungsbedingungen MÜSSEN den Endteilnehmern dauerhaft auf integre Art und Weise bereitgestellt werden.

Bei relevanten Änderungen MÜSSEN die Nutzungsbedingungen angepasst, mit einer neuen Versionsnummer und/oder einem neuen Datum versehen werden und den Endteilnehmern und vertrauenden Dritten auf angemessene Art und Weise bereitgestellt werden. Die Akzeptanz einer neuen Version durch die Endteilnehmer MUSS von den TSP geprüft werden.

9.6.4 Zusicherungen und Gewährleistungen vertrauender Dritter

Die TSP MÜSSEN in den Nutzungsbedingungen (siehe dazu auch Kap. 9.6.3) folgende Empfehlungen für vertrauende Dritte aufnehmen: Vertrauende Dritte SOLLTEN

- die Gültigkeit der Zertifikate über die angebotenen Statusdienste gemäß Kap. 4.9.10 und 4.10 prüfen,
- die in den Nutzungsbedingungen oder im Zertifikat aufgeführten Beschränkungen zur Nutzung der Zertifikate berücksichtigen,
- alle weiteren Vorsichtsmaßnahmen treffen, die sich für Dritte aus Vereinbarungen oder anderweitigen Vorschriften ergeben.

9.6.5 Zusicherungen und Gewährleistungen sonstiger Teilnehmer

Keine Vorgabe.

9.7 Gewährleistungsausschlüsse

Siehe Kap. 9.6.

9.8 Haftungsbeschränkungen

Die TSP MÜSSEN gemäß Artikel 13 der EU-Verordnung 910/2014 („eIDAS“) für alle einer natürlichen oder juristischen Person vorsätzlich oder fahrlässig zugefügten Schäden haften.

Die TSP DÜRFEN ihre Haftung im Einklang mit geltendem Recht beschränken. Sie MÜSSEN ihre Haftungsbeschränkungen in ihren CPS sowie den Nutzungsbedingungen beschrieben, siehe dazu auch Kap. 9.6.3 Abs. ii).

[SSL] Für den Fall, dass die TSP Aufgaben an Dritte auslagern, DÜRFEN sie die Haftung vertraglich mit dem Dritten im Innenverhältnis entsprechend der Aufgaben aufteilen, sie MÜSSEN jedoch im Außenverhältnis die Gesamtverantwortung entsprechend dieser CP und ihrer CPS behalten.

[EVCP] Die TSP DÜRFEN ihre Haftung gegenüber Endteilnehmern oder vertrauenden Dritten für rechtlich anerkannte und nachweisbare Ansprüche NICHT auf einen Geldbetrag von weniger als zweitausend US-Dollar pro Endteilnehmer oder vertrauenden Dritten pro Endteilnehmerzertifikat beschränken.

9.9 Schadensersatz

Keine Vorgabe.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Keine Vorgabe.

9.10.2 Beendigung

Siehe Kap. 5.8 und 9.2.

9.10.3 Auswirkungen der Beendigung und Fortführung

Keine Vorgabe.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Vorgabe.

9.12 Änderungen

Die TSP MÜSSEN relevante Änderungen den Endteilnehmern und vertrauenden Dritten und, sofern anwendbar, Bewertungsstellen und Aufsichts- oder andere Regulierungsbehörden mitteilen, siehe dazu auch Kap. 1.5.4, 9.6.1 und 9.6.3.

9.12.1 Verfahren für Änderungen

Keine Vorgabe.

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Keine Vorgabe.

9.12.3 Umstände, unter denen der OID geändert werden muss

Keine Vorgabe.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Die TSP MÜSSEN Richtlinien und Verfahren zur Beilegung von Beschwerden und Streitigkeiten, die von den Endteilnehmern oder vertrauenden Dritten zu den bereitgestellten

Diensten eingehen, festlegen und in ihren CPS sowie den Nutzungsbedingungen (Siehe Kap. 9.6.3 Abs. kk)) beschreiben.

9.14 Geltendes Recht

Die TSP MÜSSEN in ihren CPS das deutsche Recht als geltendes Recht festlegen.

9.15 Einhaltung geltenden Rechts

Die TSP MÜSSEN sicherstellen, dass sie geltendes Recht einhalten und bei Bedarf Nachweise darüber vorlegen, wie sie die geltenden rechtlichen Anforderungen erfüllt.

9.16 Verschiedene Bestimmungen

9.16.1 Gesamte Vereinbarung

Keine Vorgabe.

9.16.2 Zuordnung

Keine Vorgabe.

9.16.3 Salvatorische Klausel

Keine Vorgabe.

[SSL] Im Falle eines Konflikts zwischen [BR] und einem Gesetz DARF ein TSP jede widersprüchliche Anforderung so weit modifizieren, wie es notwendig ist, um die Anforderung gültig und legal zu machen. Dies gilt nur für Operationen oder Zertifikatsausstellungen, die diesem Gesetz unterliegen. In einem solchen Fall MUSS der TSP in Kap. 9.16.3 seines CPS einen detaillierten Verweis auf das Gesetz, das eine Änderung dieser Anforderungen gemäß diesem Abschnitt erfordert, sowie die vom TSP durchgeführte spezifische Änderung dieser Anforderungen aufnehmen und vor der Ausstellung eines Zertifikats gemäß der geänderten Anforderung das CA/Browser Forum über die relevanten Passagen des geänderten Kapitels informieren (siehe dazu [BR]#9.16.3).

Die vorgenommenen Modifikationen MÜSSEN eingestellt werden, sobald das für diese Modifikation herangezogene Gesetz nicht mehr gilt oder die Anforderungen der [BR] so geändert wurden, dass es möglich ist, sie und das Gesetz gleichzeitig zu erfüllen. Eine angemessene Änderung der Praxis, eine Änderung des CPS des TSP und eine Mitteilung an das CA/Browser Forum MÜSSEN innerhalb von 90 Tagen erfolgen.

9.16.4 Rechtsdurchsetzung

Keine Vorgabe.

9.16.5 Höhere Gewalt

Keine Vorgabe.

9.17 Sonstige Bestimmungen

Keine Vorgabe.