Deutsche Telekom Security GmbH
Trust Center Certificate Policy

Version: 02.00

Gültig ab: 02.03.2022

Status: Freigabe

Letztes Review: 28.02.2022

ÄNDERUNGSHISTORIE

Tabelle 1 - Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
01.00	15.03.2021	Telekom Security	Initialversion basierend auf [BR] 1.7.3, [NSG] 1.5, [EVCG] 1.7.4, [ETS401] 2.2.1, [ETS411-1] 1.2.2, [ETS411-2] 2.2.0, [ETS412-1] 1.1.1, [ETS412-2] 2.1.1, [ETS412-3] 1.1.1, [ETS412-4] 1.1.1, [ETS412-5] 2.2.3, [ETS312] 1.3.1, [TR3145] 1.1, [TR3145VS] 1.0
01.01	15.04.2021	Telekom Security	Update: [BR] 1.7.4 *- nicht veröffentlicht -*
01.02	13.07.2021	Telekom Security	Update: [ETS411-1] 1.3.1, [ETS412-1] 1.4.4, [ETS412-2] 2.2.1, [ETS412-3] 1.2.1, [ETS412-5] 2.3.1 *- nicht veröffentlicht -*
01.03	30.08.2021	Telekom Security	Update: [BR] 1.7.5 - 1.7.9, [NSG] 1.6 - 1.7 *- nicht veröffentlicht -*
01.04	13.09.2021	Telekom Security	Update: [EVCG] 1.7.5 - 1.7.8 *- nicht veröffentlicht -*
01.05	25.10.2021	Telekom Security	Update: [BR] 1.8.0 *- nicht veröffentlicht -*
01.06	02.12.2021	Telekom Security	Update: [ETS411-2] 2.4.1, [ETS412-4] 1.2.1 *- nicht veröffentlicht -*
02.00	01.03.2022	Telekom Security	Jährliche Revision, Update: [BR] 1.8.1

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS

1 EINLEITUNG

1.1 Überblick

Die Deutsche Telekom Security GmbH (nachfolgend „Telekom Security“ genannt) betreibt zur Abbildung am Markt angebotener PKI-Produkte und kundenindividueller PKI-Lösungen mehrere Vertrauensdienste (Trust Services)[1] zur Ausgabe von Zertifikaten und tritt somit als „Vertrauensdiensteanbieter“ (VDA) bzw. „Trust Service Provider“ (TSP)[1] auf.

Als TSP betreibt die Telekom Security in ihrem Trust Center verschiedene Wurzelzertifizierungsstellen (Root Certification Authorities, Root-CAs) sowie verschiedene untergeordnete Zertifizierungsstellen (Subordinate Certification Authorities, Sub-CAs) für die Ausgabe von Zertifikaten, sowohl für Kunden als auch Mitarbeiter des Konzerns Deutsche Telekom AG.

Darüber hinaus hat die Telekom Security dem „Verein zur Förderung eines Deutschen Forschungsnetzes e. V.“ (nachfolgend kurz „DFN“ genannt) öffentliche Sub-CA-Zertifikate ausgestellt, mit denen der DFN wiederum als eigenständiger TSP Zertifikate für die ihm angeschlossenen Institutionen ausstellt.

Bei dem vorliegenden Dokument handelt es sich um die Zertifizierungsrichtlinie (Certificate Policy, CP) des Trust Centers der Telekom Security. Es fasst in der Struktur des [RFC3647][2] alle relevanten Anforderungen aus den in Anhang B referenzierten Dokumenten zusammen, die von den Trust Services im Geltungsbereich dieser CP umgesetzt werden müssen.

Der Geltungsbereich dieser CP umfasst alle Trust Services der Telekom Security, über die Zertifikate unterhalb der

- öffentlichen und qualifizierten Root-CAs der Telekom Security,
- internen Root-CAs der Telekom Security, die sich zu dieser CP bekennen,
- Root-CAs des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) gemäß [TR3145]

ausgestellt werden.

Des Weiteren gilt diese CP für alle Trust Services des DFN, über die Zertifikate unterhalb der von der Telekom Security ausgestellten öffentlichen Sub-CA des DFN ausgestellt werden.

Für die in diesem Dokument aufgeführten Anforderungen gilt folgende Semantik:

- Anforderungen ohne besondere Markierung gelten grundsätzlich übergreifend für alle Zertifikatstypen.
- Eingerahmte Anforderungen, die mit der Angabe eines oder mehrerer Zertifikatstypen in eckigen Klammern beginnen, gelten nur für die betroffenen Zertifikatstypen. Es werden in diesem Dokument folgende Zertifikatstypen unterschieden:
  - [TLS] kennzeichnet alle TLS-Authentisierungs-Zertifikate, die unterhalb der in den Trusted Root Programmen der Browser-Hersteller integrierten öffentlichen Roots der Telekom Security, gemäß den Vorgaben der „CA/Browser-Forum Baseline Requirements“ [BR] ausgestellt werden. Diese Kennzeichnung gilt, sofern nicht explizit anders

[1] In Anlehnung an den international etablierten Sprachgebrauch werden nachfolgend auch in der deutschen Version dieses Dokuments die englischen Fachbegriffe verwendet.

[2] Ergänzend zu den in [RFC3647#6] empfohlenen Kapiteln wurde diese CP um folgende Kapitel ergänzt
- 3.2.7: Validierung der Kontrolle über eine Domain
- 3.2.8: Validierung der Kontrolle über eine E-Mail-Adresse

angegeben, für TLS-Zertifikate die gemäß [DVCP], [OVCP], [IVCP], [EVCP], [QNCP-w] oder [QEVCP-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 [GCRP] und Apple [APRP] integrierten öffentlichen Roots der Telekom Security ausgestellt 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 [3145] 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.
- [LCP] kennzeichnet alle Zertifikate, die gemäß der in ETSI EN 319 411-1 [ETS411-1] definierten „Lightweight Certificate Policy“ ausgestellt werden.
  Hinweis: Sofern nicht explizit anders angegeben, gelten die Anforderungen von [LCP] implizit auch für [DVCP], [IVCP] und [OVCP].
- [NCP] bzw. [NCP+] kennzeichnen alle Zertifikate, die gemäß der in [ETS411-1] definierten „Normalized Certificate Policy“ bzw. der „Extended Normalized Certificate Policy“ ausgestellt werden.
  Hinweis: Sofern nicht explizit anders angegeben, gelten die Anforderungen von [NCP] implizit auch für [NCP+], [QNCP-w] und [EVCP].
- [EVCP] kennzeichnet alle Zertifikate, die gemäß der „CA/Browser Forum Extended Validation Certificate Guidelines“ [EVCG] sowie der in [ETS411-1] definierten „Extended Validation Certificate Policy“ ausgestellt werden.
  Hinweis: Sofern nicht explizit anders angegeben, gelten die Anforderungen von [EVCP] implizit auch für [QEVCP-w].
- [DVCP] kennzeichnet alle Zertifikate, die gemäß der in [ETS411-1] definierten „Domain Validation Certificate Policy“ ausgestellt werden.
- [IVCP] kennzeichnet alle Zertifikate, die gemäß der in [ETS411-1] definierten „Individual Validation Certificate Policy“ ausgestellt werden.
- [OVCP] kennzeichnet alle Zertifikate, die gemäß der in [ETS411-1] definierten „Organizational Validation Certificate Policy“ ausgestellt werden.
- [QCP] kennzeichnet übergreifend alle qualifizierten Zertifikate, die gemäß der ETSI EN 319 411-2 [ETS411-2] ausgestellt werden. Im Einzelnen sind das:
  - [QCP-n] kennzeichnet alle qualifizierten Zertifikate für natürliche Personen.
  - [QCP-l] kennzeichnet alle qualifizierten Zertifikate für juristische Personen.
  - [QCP-n-qscd] kennzeichnet alle qualifizierten Zertifikate für natürliche Personen mit Nutzung des privaten Schlüssels in einer QSCD.
  - [QCP-l-qscd] kennzeichnet alle qualifizierten Zertifikate für juristische Personen mit Nutzung des privaten Schlüssels in einer QSCD.
  - [QNCP-w] kennzeichnet alle auf [TLS] und [NCP] basierende qualifizierten Web-Server-Zertifikate.
  - [QEVCP-w] kennzeichnet alle auf [EVCP] basierende qualifizierten Web-Server-Zertifikate.

Anforderungen, welche nur einen TSP betreffen, werden analog durch eine Kennzeichnung in eckigen Klammern gekennzeichnet:

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

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

- 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 Trust Services MÜSSEN die Umsetzung der für sie relevanten Anforderungen dieser CP in ebenfalls nach [RFC3647] strukturierten Certification Practise Statements (CPS) beschreiben. Die CPS MÜSSEN dabei auf alle Aspekte dieser CP eingehen und alle Kapitel des [RFC3647] berücksichtigen. Nicht anwendbare Unterkapitel MÜSSEN mit „Nicht anwendbar“ gekennzeichnet werden, d.h. diese DÜRFEN NICHT leer bleiben oder entfallen.

Die Einhaltung der Anforderungen dieser CP in der jeweils aktuellen Version MUSS explizit in den CPS bestätigt werden.

[TLS] Die Einhaltung der jeweils aktuellen Version der [BR] und, sofern zutreffend, der [EVCG] MUSS explizit in den CPS bestätigt werden und es MÜSSEN die Links zu den Dokumenten des CA/Browser Forums (http://www.cabforum.org) aufgeführt werden.

Im Falle eines Widerspruchs zwischen dieser CP oder den CPS und den [BR] bzw. [EVCG] haben die Regelungen aus [BR] bzw. [EVCG] Vorrang.

[TLS] [SMIME] Die Einhaltung der Anforderungen aus den relevanten Trusted Root Programmen von Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP] und Apple [APRP] MUSS in den CPS explizit bestätigt werden.

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)}

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

Die Telekom Security betreibt mehrere eigene öffentliche und interne Wurzelzertifizierungsstellen (Root-CAs) und untergeordnete Zertifizierungsstellen (Sub-CAs). Darüber hinaus stellt sie auch eigene Cross-Zertifikate aus, jedoch keine Cross-Zertifikate zu Root- oder Sub-CAs anderer TSP.

Im Geltungsbereich dieses Dokuments liegen darüber hinaus die öffentlichen Sub-CAs des DFN, welche von der Telekom Security ausgestellt wurden.

Die vollständigen Hierarchien, d.h. alle relevanten Root- und/oder Sub-CA-Zertifikate im Gültigkeitsbereich eines CPS, MÜSSEN im jeweiligen CPS aufgeführt werden.

1.3.2 Registrierungsstellen (Registration Authorities, RA)

Bei den eingesetzten Registrierungsstellen DARF es sich sowohl um eigene Registrierungsstellen der TSP als auch um externe Registrierungsstellen handeln, welche in deren Auftrag agieren. Die in diesem Dokument aufgeführten Anforderungen an die Registrierungsstellen MÜSSEN, sofern anwendbar, gleichermaßen für interne als auch externe Registrierungsstellen umgesetzt werden.

Beim Einsatz externer Registrierungsstellen MÜSSEN in den CPS die Strukturen, die relevanten Prozesse sowie die Rechte und Pflichten der externen Registrierungsstellen beschrieben werden und es MÜSSEN mit diesen entsprechende vertragliche Vereinbarungen abgeschlossen werden.

[TLS] [SMIME] Die Validierung von Domain-Namen und IP-Adressen DARF NICHT an externe Registrierungsstellen übergeben werden, siehe dazu Kap. 4.2.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer der Endteilnehmerzertifikate im Geltungsbereich dieser CP DÜRFEN nur natürliche oder juristische Personen sein.

Subjekte der Endteilnehmerzertifikate im Geltungsbereich dieser CP DÜRFEN sein:

- natürliche Personen
- natürliche Personen, die in Verbindung mit einer juristischen Person identifiziert werden
- juristische Personen inkl. organisatorischer Einheiten[3], die in Verbindung mit einer juristischen Person identifiziert werden
- Geräte[4], die von oder im Namen einer natürlichen oder juristischen Person betrieben werden.

Die Zertifikatsnehmer und Subjekte im Gültigkeitsbereich eines CPS MÜSSEN im jeweiligen CPS aufgeführt werden.

[EVCP] Zertifikatsnehmer DÜRFEN ausschließlich folgende juristische Personen sein: - Private Organizations gemäß [EVCG#8.5.2] - Government Entities gemäß [EVCG#8.5.3] - Business Entities gemäß [EVCG#8.5.4] - Non-Commercial Entities gemäß [EVCG#8.5.5]

[3] organisatorische Einheiten, die in Verbindung mit einer juristischen Person identifiziert werden, werden nachfolgend unter dem Begriff „juristische Personen“ subsummiert, sofern nicht explizit anders aufgeführt

[4] der Begriff „Geräte“ subsummiert nachfolgend auch Systeme, Funktionen und IT-Prozesse, sofern nicht explizit anders aufgeführt

1.3.4 Zertifikatsnutzer

Keine Vorgabe.

1.3.5 Andere Teilnehmer

Keine Vorgabe.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Die zugelassenen Verwendungszwecke der Endteilnehmerzertifikate MÜSSEN in den CPS, den Nutzungsbedingungen und -sofern anwendbar- den PDS beschrieben werden.

1.4.2 Unzulässige Verwendung von Zertifikaten

Die unzulässigen Verwendungszwecke der Endteilnehmerzertifikate MÜSSEN in den CPS, den Nutzungsbedingungen und, sofern anwendbar, den PDS beschrieben werden.

[EVCP] Die Endteilnehmerzertifikate DÜRFEN NICHT für andere Zwecke als die TLS-Serverauthentifizierung von Web-Servern genutzt werden.

1.5 Verwaltung des Dokuments

1.5.1 Verwaltende Organisation dieses Dokuments

Das Dokument wird verwaltet von:

Deutsche Telekom Security GmbH
Trust Center & ID-Solutions
Untere Industriestraße 20
57250 Netphen, Deutschland

1.5.2 Ansprechpartner

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

Telefon: +49 (0) 1805 268 204[5]

WWW: www.telesec.de

E-Mail: FMB_Trust_Center_Rootprogram@t-systems.com

[5] anfallende Kosten bei Anrufen aus Deutschland: Festnetz 0,14 €/min, Mobilfunknetze max. 0,42 €/min

[TLS] [SMIME] Zur Meldung einer vermuteten Kompromittierung eines Schlüssels, Missbrauchs oder anderer Arten von Betrug oder unangemessenem Verhalten MÜSSEN klare Prozesse festgelegt werden. Diese MÜSSEN sowohl auf den öffentlichen Web-Seiten der TSP als auch in den CPS in Kap. 1.5.2 beschrieben bzw. veröffentlicht werden.

Anm.: Bzgl. der akzeptierten Methoden zum Nachweis einer Schlüsselkompromittierung siehe Kap. 4.9.12.

[VS-NfD] Ansprechpartner sind der Informationssicherheitsbeauftragte des Trust Centers sowie dessen Vertreter, welche wie folgt zu erreichen sind:

E-Mail: FMB-ISMS-TrustCenter@telekom.de

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

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

1.5.4 Genehmigungsverfahren dieser CP und eines CPS

Neue Versionen dieser CP MÜSSEN von der Leitung des Trust Centers freigegeben werden.

Neue Versionen eines CPS, welche auf dieser CP basieren, MÜSSEN zunächst zur Feststellung der Konformität zu dieser CP durch das Root Team geprüft und danach von der Leitung des Trust Centers freigegen werden.

1.6 Definitionen und Abkürzungen

Definitionen, Abkürzungen und Referenzen sind im Anhang dieses Dokuments aufgeführt:

- Anhang A: Abkürzungen
- Anhang B: Referenzen
- Anhang C: Definitionen

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

In den CPS MUSS beschrieben werden, wer welche Verzeichnisse mit Informationen zu den 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/

Zu jedem Trusted Service MÜSSEN mindestens

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

über geeignete Online-Services, welche rund um die Uhr erreichbar sind, veröffentlicht werden. Die CPS sowie die Root-, Cross- und Sub-CA-Zertifikate SOLLTEN, sofern nicht anders angegeben, analog zu dieser CP im o.g. PKI-Repository veröffentlicht werden.

Die relevanten Nutzungsbedingungen und CPS MÜSSEN den Zertifikaten leicht erkennbar zugordnet werden können.

Darüber hinaus DÜRFEN mit Zustimmung des Endteilnehmers die Endteilnehmerzertifikate veröffentlicht werden (siehe Kap. 4.4.2).

[TLS] Die CPS und die Audit-Bescheinigungen zu technisch nicht beschränkten Sub-CAs MÜSSEN (auch) in englischer Sprache veröffentlicht werden. Die übersetzten CPS MÜSSEN dabei die gleiche Versionsnummer haben wie die originalen CPS und DÜRFEN NICHT wesentlich von diesen abweichen. Es MUSS für jedes CPS festgelegt werden, welche Version maßgeblich in Streitfällen ist.

Alle ausgestellten Zertifikate oder alternativ alle „Pre-Zertifikate“ (siehe Kap. 4.3.1), inkl. mindestens aller Sub-CA-Zertifikate (Root-CA optional) aus dessen Kette, MÜSSEN in einer hinreichenden Anzahl von „Certificate Transparency Logs“ (CTLogs) veröffentlicht werden. Bzgl. der Anzahl der CTLogs siehe Kap. 7.1.2 (40).

[TLS] [SMIME] Die erforderlichen Informationen MÜSSEN in der „Common CA Database“ (CCADB) gemäß der CCADB-Policy (siehe https://www.ccadb.org) veröffentlicht und aktuell gehalten werden.

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

[QCP] Ergänzend zu den CPS MUSS je Trusted Service ein „PKI Disclosure Statements“ (PDS) in der Struktur gemäß des Anhang A der [ETS411-1] veröffentlicht werden.

In den PDS MUSS darauf hingewiesen werden, dass der Vertrauensanker für die Validierung eines Zertifikats im "Service Digital Identifier" des Eintrags des TSP in der EU-TL angegeben sein muss.

Zur Veröffentlichung der Sub-CA-Zertifikate in den Vertrauenslisten (nationale TSL und EU-TSL) MÜSSEN die Konformitätsbewertungsberichte (siehe Kap. 8.6) der Bundesnetzagentur übermittelt werden.

Von den qualifizierten Vertrauensdiensten DARF das EU-Vertrauenssiegel verwendet werden.

[3145] Es MUSS sichergestellt werden, dass neue Sub-CA-Zertifikate oder Informationen darüber den Endteilnehmern in authentischer Form übergeben werden. Die Fingerprints der Sub-CA-Zertifikate MÜSSEN (auch) über einen anderen Weg veröffentlicht werden als das Sub-CA-Zertifikat.

[SSL] Es MÜSSEN zu jedem öffentlichen Root-Zertifikat, unterhalb dessen TLS-Serverzertifikate ausgestellt werden, Test-Webseiten bereitgestellt werden, die mit entsprechenden TLS-Serverzertifikaten gesichert sind, welche bis zu der jeweiligen Root verkettet sind.

Es MÜSSEN jeweils Webseiten mit einem gültigen, einem abgelaufenen und einem gesperrten Zertifikat bereitgestellt werden.

Sollten unterhalb einer Root auch TLS-Serverzertifikate gemäß [EVCG] ausgestellt werden, so MÜSSEN mindestens o.g. Testwebseiten bereitgestellt werden, welche mit TLS-Serverzertifikaten gemäß [EVCG] gesichert sind.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Neue Versionen dieser CP und der auf dieser CP basierenden CPS MÜSSEN vor Inkrafttreten veröffentlicht werden.

[TLS][SMIME] Neue Root-CA-Zertifikate MÜSSEN spätestens bei Beantragung einer Root-Inklusion bei einer der in Kap. 1.1 aufgeführten Root-Programme veröffentlicht werden.

Neue Sub-CA-Zertifikate MÜSSEN vor Ihrer Inbetriebnahme, spätestens jedoch 7 Tage nach ihrer Ausstellung veröffentlicht werden.

Audit-Bescheinigungen MÜSSEN spätestens 7 Tage nach ihrer Ausstellung veröffentlicht werden.

Die Zeitpunkte bzw. Häufigkeiten der in Kap. 2.2 aufgeführten Veröffentlichungen MÜSSEN in den CPS beschrieben werden.

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

3.1.1 Namensformen

In alle Zertifikate MÜSSEN die Namen der Zertifikatsinhaber im Subject in Form eines Distinguished Names gemäß [X500] („Subject-DN“) aufgenommen werden, siehe dazu Kap. 7.1.4.

In Abhängigkeit vom Zertifikatstyp MÜSSEN darüber hinaus ggf. Anforderungen an die Aufnahme von Namensbestandteilen in die Erweiterung subjectAltName berücksichtigt werden, siehe dazu Kap. 7.1.2.

3.1.2 Aussagekraft von Namen

Zu Testzwecken ausgestellte Zertifikate MÜSSEN eindeutig als solche im Subject-DN gekennzeichnet werden.

[LCP] [NCP] [NCP+] [QCP] Der commonName in Sub-CA-Zertifikaten MUSS einen gebräuchlichen Namen des TSP (nicht unbedingt der vollständige registrierte Name) beinhalten und in einer für den Markt des TSP gebräuchlichen Sprache gewählt werden.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Keine Vorgabe.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Vorgabe.

3.1.5 Eindeutigkeit von Namen

Die Subject-DN aller von einer CA ausgestellten Zertifikate MÜSSEN eindeutig und jeweils einem Zertifikatsinhaber zugeordnet sein. Es DÜRFEN aber für einen Zertifikatsinhaber mehrere Zertifikate mit gleichem Subject-DN ausgestellt werden.

[DVCP] Ausgenommen hiervon ist der Subject-DN in Domain-validierten Zertifikaten. Hier DARF ein Subject-DN auch einem anderen Zertifikatsinhaber zugeordnet werden, wenn dieser sein rechtmäßiges Eigentumsrecht an der Domain nachgewiesen hat.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Keine Vorgabe.

3.2 Initiale Validierung der Identität

Zur initialen Validierung der Identität einer Organisation oder einer natürlichen Person MÜSSEN entweder direkte Nachweise oder Bescheinigungen von angemessenen und autorisierten Quellen verwendet werden. Nachweise DÜRFEN in Papierform oder elektronisch übermittelt werden.

Die Authentizität der bereitgestellten Nachweise MUSS soweit möglich auf Änderungen und Fälschungen hin geprüft werden.

Es MÜSSEN nur die für die Verifizierung der Identität notwendigen Nachweise verlangt werden.

In den CPS MÜSSEN die von den Antragstellern und Zertifikatsinhabern erfassten Informationen sowie deren Validierung beschrieben werden.

[SSL] [SMIME] Alle Informationen, die vom Antragsteller bereitgestellt werden und ins Zertifikat aufgenommen werden sollen, MÜSSEN über eine unabhängige Informationsquelle oder einen alternativen Kommunikationskanal verifiziert werden.

Für die Verifizierung der Authentizität des Zertifikatsantrags MUSS eine zuverlässige Methode der Kommunikation verwendet werden (Definition siehe Anhang C).

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. Es MUSS die Signatur geprüft werden.

3.2.2 Authentifizierung von Organisationen

Die Daten einer Organisation, die in ein Zertifikat aufgenommen werden sollen, DÜRFEN z.B. über die folgenden Quellen validiert werden:

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

[OVCP] Die Identität, Adresse, Firmierung oder Markenname einer Organisation, die in ein Zertifikat aufgenommen werden sollen, MÜSSEN über die zuvor aufgeführten Quellen validiert werden.

Vor Verwendung einer Datenquelle als zuverlässige Datenquelle MUSS die Quelle im Hinblick auf ihre Zuverlässigkeit, Genauigkeit und Änderungs- oder Fälschungssicherheit evaluiert werden, dabei 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 (d.h. die relative Schwierigkeit, diese zu fälschen oder zu verändern)

Von den TSP oder deren Beteiligungsgesellschaften selbst gepflegte Datenbanken DÜRFEN NICHT als zuverlässige Datenquellen angesehen werden, wenn der Hauptzweck der Datenbanken darin liegt, Informationen zur Erfüllung der Validierungsanforderungen zu sammeln.

[NCP] Die Nachweise zur Identität der juristischen Person als Zertifikatsinhaber sowie die zu prüfenden Attribute MÜSSEN gegenüber einem ordnungsgemäßen Bevollmächtigten entweder direkt durch die physische Anwesenheit einer Person oder indirekt mit Hilfe von Mitteln, die eine der physischen Anwesenheit gleichwertige Sicherheit bieten, überprüft werden.

[EVCP] Zur eindeutigen Identifizierung der autorisierten Quellen, die zur Validierung der Identitäten herangezogen werden, MÜSSEN ausreichende Informationen, wie z.B. Name, Gerichtsbarkeit und Website, online auf eine geeignete und leicht zugängliche Art und Weise veröffentlicht werden und es MUSS in den CPS in Kap. 3.2 beschrieben werden, wo diese Informationen veröffentlicht werden. Darüber hinaus MÜSSEN die zugelassenen Werte zu den nachfolgend aufgeführten Feldern veröffentlicht 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)
- jursidictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

3.2.3 Authentifizierung von natürlichen Personen

Keine Vorgabe.

[NCP] Nachweise zur Identität einer natürlichen Person als Zertifikatsinhaber (auch in Verbindung mit einer juristischen Person) 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.

[IV] [SMIME] Für die Verifizierung des Namens MUSS mindestens eine leserliche Kopie eines gültigen, amtlichen Lichtbildausweises, der das Gesicht des Antragstellers erkennbar zeigt, herangezogen werden.

Für die Verifizierung der Anschrift MUSS eine Form der Identifizierung herangezogen werden, welche die TSP als vertrauenswürdig erachten. Es DÜRFEN die amtlichen Lichtbildausweise verwendet werden, die für die Verifizierung des Namens verwendet werden oder auch Rechnungen eines Versorgungsunternehmens oder Bank- oder Kreditkartenauszüge.

[VS-NfD] Die Identität des Antragstellers MUSS mittels eines amtlichen Ausweisdokuments geprüft 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 des Antragstellers und dessen Berechtigung, im Namen des Zertifikatsinhabers zu agieren, wie folgt überprüft werden:

- Wenn der Antragsteller eine natürliche Person vertritt, die nicht mit einer juristischen Person verbunden ist, MUSS eine Bevollmächtigung der natürlichen Person, Zertifikate in ihrem Namen zu beantragen, vorliegen.
- Wenn der Antragsteller eine juristische Person oder eine natürliche Person in Verbindung mit einer juristischen Person vertritt, MUSS eine Bevollmächtigung der juristischen Person, Zertifikate in ihrem Namen oder im Namen ihrer Mitarbeiter zu beantragen, vorliegen.
- Wenn es sich bei dem Antragsteller, welcher einen anderen Zertifikatsinhaber vertritt, um eine juristische Person handelt, MUSS diese juristische Person wiederum durch eine berechtigte natürliche Person vertreten werden und dessen Vertretungsberechtigung MUSS geprüft werden.

[OVCP] Es MUSS die Authentizität der Zertifikatsanträge mittels einer zuverlässigen Kommunikationsmethode überprüft werden, dabei DARF auf die o.g. Quellen zurückgegriffen werden.

Die Authentizität eines Zertifikatsantrags DARF entweder direkt vom Vertreter der Organisation bestätigt werden oder auch durch von den TSP als verbindlich angesehene Stellen innerhalb der Organisation, wie z.B. Hauptgeschäftsstellen, Niederlassungen, Personalbüros oder IT-Abteilungen.

Darüber hinaus MUSS den Organisationen die Möglichkeit geboten werden, berechtigte Personen zur Beantragung von Zertifikaten zu benennen. Wenn eine Organisation berechtigte Personen schriftlich benannt hat, DÜRFEN Zertifikatsanträge von anderen als den benannten Personen NICHT akzeptiert werden. Auf eine schriftliche Anfrage einer Organisation MUSS eine Liste der von der Organisation benannten berechtigten Personen zur Verfügung gestellt werden.

3.2.6 Cross-Zertifikate

Keine Vorgabe.

[TLS] Es MÜSSEN alle Cross-Zertifikate veröffentlicht werden, in denen die Telekom Security als Subjekt enthalten ist und deren Ausstellung die Telekom Security veranlasst bzw. akzeptiert hat.

3.2.7 Validierung der Kontrolle über eine Domain oder IP-Adresse

Keine Vorgabe.

[TLS] Jeder vollqualifizierte Domain-Name (FQDN), der in ein Zertifikat aufgenommen werden soll, MUSS wie folgt validiert werden:

- Falls der FQDN nicht „onion“ als rechtesten Eintrag enthält, MUSS der FQDN mithilfe einer der folgenden in [BR#3.2.2.4] näher beschriebenen Methoden validiert werden:
  - E-Mail, Fax, SMS oder Post an den Domain-Kontakt gemäß [BR#3.2.2.4.2],
  - konstruierte E-Mail an den Domain-Kontakt gemäß [BR#3.2.2.4.4],
  - DNS-Veränderung gemäß [BR#3.2.2.4.7],
  - IP-Adressenprüfung gemäß [BR#3.2.2.4.8],
  - Validierung des Antragstellers als Domain-Kontakt gemäß [BR#3.2.2.4.12],
  - E-Mail an den DNS CAA E-Mail-Kontakt gemäß [BR#3.2.2.4.13],
  - E-Mail an den DNS CAA TXT-Record-E-Mail-Kontakt gemäß [BR#3.2.2.4.14],
  - Telefonanruf beim Domain-Kontakt gemäß [BR#3.2.2.4.15],
  - Telefonanruf beim DNS TXT Record-Kontakt gemäß [BR#3.2.2.4.16],
  - Telefonanruf beim DNS CAA-Kontakt gemäß [BR#3.2.2.4.17],
  - Vereinbarte Änderung der Webseite v2 gemäß [BR#3.2.2.4.18],
  - Vereinbarte Änderung der Webseite ACME gemäß [BR#3.2.2.4.19],
  - TLS unter Verwendung von ALPN gemäß [BR#3.2.2.4.20].

- Falls der FQDN „onion“ als rechtesten Eintrag enthält, MUSS der FQDN entsprechend [BR#Appendix B] bzw. [EVCG#Appendix F] validiert werden.

Nach einer erfolgreichen Validierung eines FQDN gemäß eine der oben aufgeführten Methoden aus [BR#3.2.2.4] DARF auf die Validierung weiterer FQDNs oder Wildcard Domain Names, welche mit den Domain Labels des validierten FQDN enden, verzichtet werden. Hiervon ausgenommen sind Validierungen gemäß [BR#3.2.2.4.8], [BR#3.2.2.4.18], [BR#3.2.2.4.19] und [BR#3.2.2.4.20].

Für jeden Wildcard Domain-Name, der in ein Zertifikat aufgenommen werden soll, MUSS geprüft werden, dass der FQDN-Teil vom Typ "registry-controlled" oder "public suffix" ist. Zu dieser Prüfung DARF auf eine regelmäßig aktualisierte „Public-suffix-list“ (PSL) zurückgegriffen werden. Wenn eine solche PSL zur Prüfung verwendet wird, SOLLTEN nur die „ICANN Domains“ akzeptiert werden.

[TLS] Die Validierung der Kontrolle über eine IP-Adresse MUSS gemäß einer der folgenden in [BR#3.2.2.5] näher beschriebenen Methoden durchgeführt werden:

- Vereinbarte Änderung der Webseite gemäß [BR#3.2.2.5.1],
- E-Mail, Fax, SMS oder Post an den IP-Adress-Kontakt gemäß [BR#3.2.2.5.2],
- Rückwärtssuche nach Adressen gemäß [BR#3.2.2.5.3],
- Telefonanruf beim IOP-Adress-Kontakt gemäß [BR#3.2.2.5.5],
- ACME "http-01"-Methode für IP-Adressen gemäß [BR#3.2.2.5.6],
- ACME "tls-alpn-01"-Methode für IP-Adressen gemäß [BR#3.2.2.5.7].

Um zu verhindern, dass IP-Adressen verwendet werden, welche in anderen Ländern als dem tatsächlichen Sitz des Antragstellers vergeben wurden, SOLLTE ein Verfahren zur Überprüfung von Proxy-Servern eingeführt werden. In den CPS MÜSSEN die verwendeten Methoden inkl. eines Verweises auf das relevante Kapitel der [BR] aufgeführt werden.

3.2.8 Validierung der Kontrolle über eine E-Mail-Adresse

Keine Vorgabe.

[SMIME] Zur Verifizierung der Kontrolle des Antragstellers über die im Zertifikat referenzierte E-Mail-Adresse bzw. der Autorisierung des Antragstellers, im Namen des tatsächlichen Inhabers der E-Mail-Adresse zu handeln, MÜSSEN angemessene und sichere Methoden angewendet werden. [SMIME] Nach einer erfolgreichen Validierung des Authorization Domain Names (ADN, gemäß [BR]) des Domain-Anteils von E-Mail-Adressen einer Organisation DARF auf die Validierung von Sub-Domains dieses ADN bei der Validierung weiterer E-Mail-Adressen dieser Organisation verzichtet werden.

Die angewandten Verifizierungsmethoden MÜSSEN in den CPS beschrieben werden.

3.3 Identifizierung und Authentifizierung für Zertifikatserneuerungen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Zertifikatserneuerungen

Vor routinemäßigen Zertifikatserneuerungen 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 geprüft werden.

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

[TLS] Die Verifizierung von Informationen, die für eine Zertifikatserneuerung verwendet werden, MUSS innerhalb der letzten 398 Tage vor der Erneuerung erfolgt sein, ansonsten MÜSSEN die Informationen auf Aktualität und Richtigkeit geprüft werden.

[EVCP] Um sicherzustellen, dass der Zertifikatsantrag autorisiert ist und die Informationen noch immer akkurat und gültig sind, MÜSSEN alle Aufgaben zur Authentifizierung und Verifizierung entsprechend [EVCG] durchgeführt werden.

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

Für die Ausstellung von Ersatz-Zertifikaten DARF auf bereits verifizierte Zertifikatsanträge zurückgegriffen werden, soweit das zu ersetzende Zertifikat nicht aufgrund von Betrug oder anderer rechtswidriger Handlungen gesperrt wurde und das Ablaufdatum des Ersatz-Zertifikats sowie die Angaben im Subject-DN und subjectAltName identisch bleiben.

3.3.2 Identifizierung und Authentifizierung für Zertifikatserneuerungen nach einer Sperrung

Gesperrte Zertifikate DÜRFEN NICHT erneuert werden. Nach einer Sperrung MUSS ein neues Zertifikat beantragt werden und die Validierung MUSS wie bei der initialen Beantragung erfolgen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Methoden für die Identifizierung und Authentifizierung von Sperranträgen MÜSSEN in den CPS festgelegt werden.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

Die nachfolgend aufgeführten Anforderungen MÜSSEN für alle Zertifikate umgesetzt werden, inkl. der Zertifikate, welche die TSP für sich selbst oder ihre Mitarbeiter ausstellen.

Sofern nicht explizit anders angegeben, gelten die Anforderungen für die Zertifikate aller Hierarchieebenen.

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Die Zertifikatsantragsberechtigten sowie deren möglichen Rollen MÜSSEN in den CPS beschrieben werden.

Zur Vermeidung von Interessenskonflikten DÜRFEN die TSP NICHT selbst als Antragsteller von Endteilnehmerzertifikaten fungieren. Ausnahmen bilden die Organisationen, welche Registrierungstätigkeiten durchführen und sich selbst oder Personen, die in Verbindung mit dieser Organisation identifiziert werden, Zertifikate ausstellen. Die Ausnahmen MÜSSEN in den CPS beschrieben werden.

[EVCP] Die Ausstellung von Endteilnehmerzertifikaten MUSS auf folgende Organisationsformen gemäß [EVCG] eingeschränkt werden (Definitionen siehe Anhang C):

- Business entities
- Government entities
- Private organizations
- Non-commercial entities

4.1.2 Antragsprozess und -verantwortlichkeiten

Die Antragsprozesse inkl. der zu nutzenden Schnittstellen MÜSSEN in den CPS klar beschrieben werden.

Von den Antragstellern für Endteilnehmerzertifikate MÜSSEN

- eine physische Adresse oder andere Kontaktangaben sowie
- alle in das Zertifikat in den Subject-DN oder die Erweiterung subjectAltName aufzunehmenden Attribute

eingefordert werden. Diese Daten MÜSSEN entweder vom Antragsteller selbst bei Antragstellung bereitgestellt werden oder nach Abfrage bei anderen Quellen vom Antragsteller bestätigt werden.

Vor Abschluss eines Vertragsverhältnisses MÜSSEN die Endteilnehmer über die Nutzungsbedingungen zur Verwendung der Zertifikate gemäß Kap. 9.6.3 informiert werden.

Wenn der Antragsteller eines Endteilnehmerzertifikats 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 werden 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 werden 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 eines Endteilnehmerzertifikats 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 in elektronischer Form gestellt werden. In diesem Fall MÜSSEN die Anträge aber durch eine nachvollziehbare Handlung (z. B. Ankreuzen eines Kästchens) bestätigt werden.

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

[TLS] 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), welche den öffentlichen Schlüssel und mindestens einen der gewünschten Namen enthält, einreichen.

[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 Zertifikatsanträge MÜSSEN auf Korrektheit, Vollständigkeit und Autorisierung geprüft werden.

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

Die Bearbeitung der Anträge für Endteilnehmerzertifikate oder Teile davon DÜRFEN an Externe RAs ausgelagert werden. In diesem Fall MUSS sichergestellt werden, dass der Prozess als Ganzes den Anforderungen dieser CP genügt. Dementsprechend MÜSSEN die externen RAs identifiziert und authentifiziert werden und es MUSS sichergestellt werden, dass die Informationen zwischen externer RA und TSP sicher ausgetauscht werden.

[TLS] Ausgenommen davon ist die Validierung über die Kontrolle einer Domain oder IP-Adresse gemäß Kap. 3.2.7, welche von den TSP selbst durchgeführt werden MUSS.

[SMIME] Ausgenommen davon ist die Validierung des Authorization Domain Name (gemäß [BR]) des Domain-Anteils der E-Mail-Adresse, welcher von den TSP selbst durchgeführt werden MUSS.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Subjekte der Zertifikate und, sofern davon abweichend, die Antragsteller MÜSSEN gemäß der in Kap. 3.2 beschriebenen Methoden identifiziert und authentifiziert werden, die Prozesse und Vorgaben für die Durchführung der Identifizierung und Authentifizierung inkl. der Überprüfung der vom Antragsteller zur Aufnahme in das Zertifikat angeforderten Daten MUSS in den CPS beschrieben werden.

Ist das Subjekt eines Endteilnehmerzertifikats eine natürliche Person, dann MÜSSEN überprüft werden:

- Vollständiger Name der Person (Nachname, Vornamen)
- Geburtsdatum und -ort gemäß den nationalen oder anderen geltenden Übereinkommen für die Eintragung von Geburten,
- Verweis auf ein amtliches Ausweisdokument oder andere Attribute, welche für eine eindeutige Identifikation herangezogen werden können

Ist das Subjekt eines Endteilnehmerzertifikats eine natürliche Person, die in Verbindung mit einer juristischen Person identifiziert wird, dann MÜSSEN zusätzlich überprüft werden:

- Vollständiger Name und Rechtsstand der juristischen Person
- Relevante Registrierungsinformationen der juristischen Person gemäß den nationalen oder anderen geltenden Identifizierungsverfahren
- Zugehörigkeit der natürlichen Person zur juristischen Person
- Bestätigung der juristischen und natürlichen Person, dass die Attribute des Zertifikatsinhabers auch die Organisation identifizieren

Ist das Subjekt eines Endteilnehmerzertifikats ein Gerät oder System, welches von einer natürlichen Person betrieben wird, dann MUSS zusätzlich die Kennung des Geräts (z.B. Internet-Domain-Name) überprüft werden.

Ist das Subjekt eines Endteilnehmerzertifikats eine juristische Person oder eine organisatorische Einheit, die in Verbindung mit einer juristischen Person identifiziert wird, dann MÜSSEN überprüft werden:

- Vollständiger Name der juristischen Person oder organisatorischen Einheit, die im Attribut „organization“ des Zertifikats aufgenommen werden soll,
- alle relevanten Registrierungsinformationen der juristischen Person oder der organisatorischen Einheit, inkl. einer national anerkannten Identitätsnummer oder andere Attribute, die verwendet werden können, um die organisatorische Einheit so weit wie möglich von anderen mit demselben Namen zu unterscheiden,
- Falls anwendbar, die Verbindung der juristischen Person zu der organisatorischen Einheit, die in Verbindung mit dieser juristischen Person identifiziert wird.

Ist das Subjekt eines Endteilnehmerzertifikats ein Gerät oder System, welches im Namen einer juristischen Person oder einer organisatorischen Einheit, die in Verbindung mit einer juristischen Person identifiziert wird, betrieben wird, dann MUSS zusätzlich die Kennung des Geräts oder Systems (z. B. Internet Domain Name) überprüft werden.

[TLS] Eine durchgeführte Validierung DARF für die Ausstellung mehrerer Zertifikate genutzt werden, jedoch DARF die Validierung NICHT länger als 398 Tage vor der Zertifikatsausstellung durchgeführt worden sein.

Sofern anwendbar, MÜSSEN zusätzlich erforderliche Prüfungen für „High-Risk-Zertifikatsanträge“ umgesetzt und in den CPS beschreiben werden.

[EVCP] Wenn in einem Zertifikatsantrag nicht alle erforderlichen Informationen enthalten sind, MÜSSEN die fehlenden Informationen vom Zertifikatsgenehmiger oder Vertragsunterzeichner und nicht vom Zertifikatsanforderer bestätigt werden (Definitionen der Rollen siehe Anhang C).

[3145] Bei der Validierung einer Identität MUSS geprüft werden, ob der Endteilnehmer bereits zuvor registriert wurde. Wenn das der Fall ist, so MÜSSEN alle weiteren Zertifikate dem registrierten Endteilnehmer zugeordnet werden, damit im Fall einer Suspendierung des Endteilnehmers alle Zertifikate dieses Endteilnehmers gemäß den Nutzungsbedingungen gleichzeitig suspendiert oder gesperrt werden können.

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

[VS-NfD] Die Sicherheitsfreigabe des Antragstellers MUSS in Bezug auf die Nutzung der PKI verifiziert werden.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Zertifikatsanträge DÜRFEN nur nach erfolgreicher Identifizierung und Authentifizierung gemäß Kap. 4.2.1 genehmigt werden.

Wenn zu einem Antrag ein vom Zertifikatsnehmer generierter Schlüssel vorgelegt wird, der nicht den Anforderungen aus Kap. 6.1.5 und 6.1.6 genügt, MUSS der Antrag abgelehnt werden.

[TLS] Wenn in einem Antrag ein Schlüssel vorgelegt wird,

- dessen korrespondierender privater Schlüssel nachweislich mittels einer fehlerhaften Methode erzeugt wurde,
- dessen korrespondierender privater Schlüssel über eine dem TSP bekannte oder nachgewiesene Methode kompromittiert werden kann,
- zu dem der TSP zuvor über eine Kompromittierung des korrespondierenden privaten Schlüssels informiert wurde (siehe dazu auch Kap. 4.9.1),
- auf Basis dessen dem TSP eine nachgewiesene oder bewährte Methode bekannt ist, den privaten Schlüssel leicht zu berechnen, z.B., wenn es sich um einen „Debian weak key“ handelt,
- der zuvor vom TSP generiert wurde,

MUSS der Antrag abgelehnt werden.

[QCP-l-qscd] [QCP-n-qscd] Wenn in einem Antrag ein Schlüssel vorgelegt wird, von dem nicht sichergestellt ist, dass dieser von einem Schlüsselpaar stammt, welches in einer QSCD generiert wurde, MUSS der Antrag abgelehnt werden.

[3145] Zertifikatsanträge von suspendierten Endteilnehmern MÜSSEN abgelehnt werden.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgabe.

4.3 Ausstellen von Zertifikaten

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

Bei der Ausstellung der Zertifikate MÜSSEN die Integrität und Authentizität gewährleistet werden und dementsprechende (technische, organisatorische oder personelle) Maßnahmen zum Schutz vor Fälschung der Daten vor der Ausstellung der Zertifikate getroffen werden. 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 TSP die Schlüssel der Endteilnehmer generieren, MUSS die Vertraulichkeit der Schlüssel im Generierungsprozess sichergestellt werden.

[TLS] 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 („Embedded Signed Certificate Timestamps“ (SCT)) aufgenommen werden. Bzgl. der Anzahl der SCTs sei auf Kap. 7.1.2 verwiesen.

[3145] Vor der Ausstellung von Zertifikaten SOLLTE geprüft werden, 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, MUSS

- sichergestellt werden, dass der korrekte öffentliche Schlüssel des ausgewählten Tokens ins Zertifikat übernommen wird und dass das Zertifikat auf dem Token abgelegt wird,
- sichergestellt werden, dass der personalisierte Token an den richtigen Empfänger gesendet wird,
- den Versand/die Übergabe der Token so gestaltet werden, 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 Verfahren zur Ausgabe der Token MÜSSEN in den Nutzungsbedingungen und den CPS beschrieben werden.

Wenn die TSP die Schlüssel für die Endteilnehmerzertifikate generieren, MUSS

- sichergestellt werden, dass die Schlüssel dem korrekten Empfänger übermittelt werden,
- sichergestellt werden, dass die Vertraulichkeit der Schlüssel während der Übermittlung gewährleistet ist,
- sichergestellt werden, 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 Verfahren zur Übergabe der Schlüssel MÜSSEN in den Nutzungsbedingungen und den CPS beschrieben werden.

[VS-NfD] Die Vorgaben aus [VSA] MÜSSEN zum Schutz der Schlüssel gemäß ihrer Klassifikation beachtet werden.

4.3.2 Benachrichtigung des Endteilnehmers über die Ausstellung eines Zertifikats

Sofern anwendbar, MÜSSEN die ausgestellten Endteilnehmerzertifikate den Endteilnehmern, d.h. dem Antragsteller und/oder dem Subjekt des Zertifikats, in nutzbarer Form übergeben werden oder, falls der TSP den privaten Schlüssel im Auftrag des Endteilnehmers verwaltet, die Endteilnehmer über die Ausstellung benachrichtigt werden.

Anm.: Die Endteilnehmerzertifikate müssen nicht sofort nach der Erstellung in nutzbarer Form zur Verfügung gestellt werden.

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 Endteilnehmerzertifikate MÜSSEN den Zertifikatsnehmern bereitgestellt werden.

Die Endteilnehmerzertifikate DÜRFEN Zertifikatsnutzern nur nach Zustimmung des Endteilnehmers bereitgestellt werden. Die Prozesse der Veröffentlichung MÜSSEN in den CPS beschrieben werden, siehe dazu auch Kap. 2.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP

Keine Vorgabe.

[TLS] Die Root- und Sub-CA- Zertifikate MÜSSEN in der CCADB, die Endteilnehmerzertifikate in mehreren CT-Log-Servern veröffentlicht werden, siehe Kap. 2.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Endteilnehmer

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 Nutzungszwecke der privaten Schlüssel und Zertifikate der Endteilnehmer MÜSSEN in den CPS beschreiben werden.

[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.

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 Umstände, unter denen ein Renewal erlaubt ist, MÜSSEN in den CPS festgelegt werden. Dabei MÜSSEN die Aspekte der Schwächung der Schlüssel sowie die Anforderung nach bis zum Gültigkeitsende des neuen Zertifikats ausreichenden Schlüssellängen und zulässige Algorithmen betrachtet werden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese aufgrund eines Sicherheitsvorfalls gesperrt wurden. Zertifikate DÜRFEN NICHT erneuert werden, wenn sich Angaben in den Zertifikaten geändert haben.

[3145] Die Zeiträume und Umstände, unter denen ein Renewal erlaubt ist, MÜSSEN in den CPS sowie in den Nutzungsbedingungen beschrieben werden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

4.6.2 Antragsberechtigte für ein Renewal

Keine Vorgabe.

4.6.3 Verarbeitung von Anträgen auf Renewal

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

Vor einer Erneuerung MÜSSEN die Gültigkeit des ablaufenden Zertifikats sowie der ursprünglichen vorgelegten Identifizierungsdaten und Attribute des Subjekts geprüft werden. Die Anträge MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

[3145] Für den Fall, dass die Integrität der ursprünglichen Daten nicht mehr gegeben ist, MÜSSEN in den CPS die erforderlichen Prozesse beschrieben werden

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-Key)

4.7.1 Umstände für ein Re-Key

Die Umstände, unter denen ein Re-Key erlaubt ist, MÜSSEN in den CPS beschrieben werden.

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

[3145] Die Zeiträume und Umstände, unter denen ein Re-Key erlaubt ist, MÜSSEN in den CPS sowie in den Nutzungsbedingungen beschrieben werden. Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

4.7.2 Antragsberechtigte für ein Re-Key

Keine Vorgabe.

4.7.3 Verarbeitung von Anträgen auf Re-Key

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

Vor einer Erneuerung MÜSSEN die Gültigkeit des ablaufenden Zertifikats sowie der ursprünglichen vorgelegten Identifizierungsdaten und Attribute des Subjekts geprüft werden. Die Anträge MÜSSEN vollständig, korrekt, aktuell und autorisiert sein. Wenn sich in das neue Zertifikat aufzunehmende Informationen geändert haben oder das alte Zertifikat gesperrt wurde, MÜSSEN die Registrierungsinformationen wie bei einer Erstbeantragung überprüft, aufgezeichnet und vom Endteilnehmer bestätigt werden.

[EVCP] In einem erneuerten Endteilnehmerzertifikat MÜSSEN das gleiche Ablaufdatum und der gleiche Subject-DN wie im ursprünglichen Zertifikat gesetzt werden.

[3145] Für den Fall, dass die Integrität der ursprünglichen Daten nicht mehr gegeben ist, MÜSSEN in den CPS die erforderlichen Prozesse beschrieben werden

Die Generierung neuer Schlüssel MUSS erzwungen werden.

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 Umstände, unter denen eine Änderung von Zertifikatsdaten erlaubt oder erforderlich ist, MÜSSEN in den CPS beschrieben werden.

Wenn bei einer Änderung der Zertifikatsdaten der ursprüngliche Schlüssel wiederverwendet werden soll, MÜSSEN die Aspekte der Schwächung der Schlüssel sowie die Anforderung nach bis zum Gültigkeitsende des neuen Zertifikats ausreichenden Schlüssellängen und zulässige Algorithmen betrachtet werden.

Wenn ein Verdacht oder Nachweis über die Kompromittierung des ursprünglichen Schlüssels vorliegt oder das ursprüngliche Zertifikate aufgrund eines Sicherheitsvorfalls gesperrt wurde, DARF der ursprüngliche Schlüssel NICHT wiederverwendet werden.

Die Endteilnehmer MÜSSEN verpflichtet werden, die Änderung von registrierten Daten im Gültigkeitszeitraum der auf Basis der registrierten Daten erstellten Zertifikate dem TSP zu melden. Die Endteilnehmer MÜSSEN über die Prozesse zur Änderung der Zertifikatsdaten informiert werden.

[3145] Die Zeiträume und Umstände, unter denen eine Änderung von Zertifikatsdaten erlaubt oder erforderlich ist, MÜSSEN in den CPS sowie in den Nutzungsbedingungen beschrieben werden.

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, MUSS die Akzeptanz dieser neuen Nutzungsbedingungen nachweislich vom Endteilnehmer vor der Ausstellung eines neuen Zertifikats eingeholt werden.

Vor der Änderung von Zertifikatsdaten MUSS die Gültigkeit des ablaufenden Zertifikats sowie der nicht geänderten ursprünglich vorgelegten Identifizierungsdaten und Attribute des Subjekts geprüft werden, geänderte Daten MÜSSEN gemäß Kap. 3.2 validiert und registriert werden. Alle Daten MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

[3145] Für den Fall, dass die Integrität der ursprünglichen Daten nicht mehr gegeben ist, MÜSSEN in den CPS die erforderlichen Prozesse beschrieben werden.

Die Generierung neuer Schlüssel MUSS erzwungen werden.

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

Die Zertifikatsnehmer MÜSSEN in den Nutzungsbedingungen über die Sperrgründe sowie die verfügbaren Schnittstellen zur Beantragung einer Sperrung informiert werden.

Ebenso MÜSSEN mit sperrberechtigten RAs Vereinbarungen getroffen werden, in denen die Sperrgründe sowie die verfügbaren Schnittstellen zur Beantragung einer Sperrung beschrieben sind.

[TLS] [SMIME] 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.

Bzgl. der Schnittstellen zur Meldung von Problemen sieh Kap. 1.5.2

Hinweis: Die nachfolgend aufgeführten Anforderungen gelten nicht für „Kurzzeit-Zertifikate“, wenn diese aufgrund ihrer sehr kurzen Gültigkeit grundsätzlich nicht gesperrt werden. Wenn solche Kurzzeitzertifikate ausgestellt werden, MUSS in den CPS beschrieben werden, bei welchen Zertifikaten es sich um solche Kurzzeitzertifikate handelt und wie diese behandelt werden.

4.9.1 Sperrgründe

Ergänzend zu den nachfolgend aufgeführten Sperrgründen DÜRFEN in den CPS weitere Sperrgründe festgelegt werden.

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 Betreiber der Sub-CA 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 Betreiber der Sub-CA 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 des Betreibers 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.

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.

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.

[TLS] 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,
- festgestellt wird, dass es sich bei dem privaten Schlüssel des Endteilnehmers um einen schwachen Schlüssel handelt, der leicht auf Basis des öffentlichen Schlüssels berechnet werden kann (z.B. „Debian weak key“).

[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 dem CPS der Sub-CA oder dieser CP (und damit auch der in Kap. 1.1 referenzierten Anforderungsquellen) 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 dass es eindeutige Beweise dafür gibt, dass die für die Generierung des privaten Schlüssels verwendete Methode mangelhaft war.
- das Zertifikat missbräuchlich eingesetzt wurde,
- der Endteilnehmer gegen eine oder mehrere wesentliche Vereinbarungen oder Nutzungsbedingungen verstoßen hat,
- die Informationen im Zertifikat nicht korrekt sind,
- es wesentliche Änderungen an den im Zertifikat enthalten Informationen gegeben hat.

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

- das Recht des TSP zur Ausstellung von Zertifikaten gemäß [BR] 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 von den Fristen abweichenden 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.

[TLS] [SMIME] Endteilnehmerzertifikate MÜSSEN gesperrt werden, wenn von den relevanten Root-Programmen der Applikations-Software-Hersteller hinreichende Gründe aufgeführt werden. Es gelten dabei grundsätzlich die in Kap. 4.9.1.2.1 und 4.9.1.2.2 aufgeführten Fristen. Die TSP MÜSSEN jedoch auch in der Lage sein, in begründeten Fällen Zertifikate zu einem von einem Root-Programm vorgegebenen Termin zu sperren, der von den o.g. Fristen abweicht.

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

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

[QCP-n-qscd] [QCP-l-qscd] Ein Endteilnehmerzertifikat MUSS gesperrt werden, wenn das verwendete QSCD (siehe Kap. 6.2.1) seine Zertifizierung verliert.

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 Betreibers der Sub-CA beantragt werden. Sollte einer der in Kap. 4.9.1.1 aufgeführten Sperrgründe von der Telekom Security als Betreiber der Root-CAs festgestellt werden, so DARF die Sperrung durch die Telekom Security auch ohne vorliegenden Sperrantrag durchgeführt werden. Die weiteren organisatorischen und prozessualen Vorgaben MÜSSEN im [CPS_Root] beschrieben werden.

[3145] Die Sperrung einer Sub-CA im Anwendungsbereich der TR-03145 liegt nicht im Geltungsbereich 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-CA-Betreibers erfolgen und MUSS in den CPS 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 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 in den CPS beschrieben werden.

[3145] Ein Endteilnehmerzertifikat MUSS darüber hinaus gesperrt werden, wenn der Endteilnehmer suspendiert wird.

[VS-NfD] Ein Endteilnehmerzertifikats MUSS darüber hinaus auf ein begründetes Verlangen des Sicherheitsbeauftragten gesperrt 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 nicht als berechtigter Auslöser einer Sperrung eingestuft werden.

Sowohl der Sperrantragsteller als auch der Zertifikatsnehmer MÜSSEN, sofern möglich über durchgeführte Sperrungen informiert werden.

Endgültig gesperrte Zertifikate DÜRFEN NICHT wieder entsperrt werden.

[TLS] [SMIME] Nach der Sperrung eines Sub-CA-Zertifikats MUSS der entsprechende Eintrag in der CCADB upgedatet werden. 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.

[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

Ergänzend zu den nachfolgend aufgeführten Fristen DÜRFEN in den CPS kürzere Fristen für bestimmte Sperrgründe festgelegt werden.

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. Wenn ein Sperrantrag nicht innerhalb von 24 Stunden autorisiert werden kann, muss dieser nicht umgesetzt werden.

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

Für Sperrungen, die nicht auf autorisierten Sperranträgen basieren, gelten die in Kap. 4.9.1.2.2 und 4.9.1.2.3 aufgeführten Fristen.

[TLS] Innerhalb von 24 Stunden nach Eingang einer Problemmeldung MÜSSEN die Fakten und Umstände 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
- die einschlägigen Rechtsvorschriften

4.9.6 Anforderungen an Dritte zur Prüfung von Sperrinformationen

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

Bei Kurzzeitzertifikaten, die durch die Erweiterung „Validity Assured“ (id-etsi-ext-valassured-ST-certs) gekennzeichnet sind, DÜRFEN vertrauende Dritte darauf verzichten, den Status gemäß Kap. 4.10 abzufragen.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Certification Authority Revocation Lists (CARLs) MÜSSEN innerhalb von 24 Stunden nach Sperrung eines Sub-CA-Zertifikats sowie regelmäßig mindestens alle 12 Monate aktualisiert werden.

Certificate Revocation Lists (CRLs) MÜSSEN regelmäßig mindestens alle 24 Stunden aktualisiert werden.

[3145] CRLs 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

Keine Vorgabe.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Siehe Kap. 4.10.

4.9.10 Anforderungen an Online Überprüfungsverfahren

Wenn Dritte den Status von Zertifikaten per OCSP prüfen, SOLLTEN diese RFC6960-konforme OCSP-Clientkomponenten verwenden, d.h. diese SOLLTEN 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

Keine Vorgabe.

[TLS] [SMIME] Die akzeptierten Methoden zum Nachweis einer Schlüsselkompromittierung MÜSSEN in den CPS in Kap. 4.9.12 beschrieben werden.

Anm.: Bzgl. der Meldung einer vermuteten Schlüsselkompromittierung siehe Kap. 1.5.2.

4.9.13 Umstände für eine Suspendierung

Falls eine Suspendierung angeboten wird, MÜSSEN im CPS die Umstände für eine Suspendierung festgelegt werden.

[TLS] Endteilnehmerzertifikate DÜRFEN NICHT suspendiert werden.

[3145] Ergänzend zur Sperrung oder Suspendierung von Endteilnehmerzertifikaten MÜSSEN auch Endteilnehmer suspendiert werden, wenn festgestellt wird, dass diese ihre Pflichten innerhalb der PKI nicht mehr erfüllen, z.B. bei einer Schlüsselkompromittierung oder einem Zertifikatsmissbrauch. Die Vorgaben, Abläufe und Fristen MÜSSEN in den CPS beschrieben werden.

4.9.14 Berechtigte Antragsteller für eine Suspendierung

Falls eine Suspendierung angeboten wird, MÜSSEN die berechtigten Antragsteller für eine Suspendierung im CPS festgelegt werden.

4.9.15 Ablauf einer Suspendierung

Falls eine Suspendierung angeboten wird, MÜSSEN die Abläufe einer Suspendierung im CPS festgelegt werden.

4.9.16 Begrenzung der Suspendierungsperiode

Falls eine Suspendierung angeboten wird, MÜSSEN die Zeiträume und Fristen für eine Suspendierung im CPS festgelegt werden.

4.10 Zertifikatsstatusdienste

Mindestens über die Gültigkeitsdauer aller ausgestellten Sub-CA und Endteilnehmer-Zertifikate MÜSSEN authentische und integre Zertifikatsstatusdienste in Form von Sperrlisten und/oder OCSP-Auskünften bereitgestellt werden.

Zu den Endteilnehmerzertifikaten SOLLTEN OCSP-Auskünften bereitgestellt werden.

[TLS] [SMIME] Zu Sub-CA und Endteilnehmer-Zertifikaten MÜSSEN Sperrlisten und OCSP-Auskünfte bereitgestellt werden.

[QCP] Die Zertifikatsstatusdienste MÜSSEN über die Zertifikatsgültigkeit hinaus bereitgestellt werden.

[QCP-n] [QCP-l] 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 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. Ggf. voneinander abweichende Aktualisierungsfristen MÜSSEN in den CPS aufgeführt werden und es MUSS beschreiben werden, wie daraus resultierende unterschiedliche Prüfergebnisse zu interpretieren sind.

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.

[TLS] [SMIME] 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 7 Tagen haben. Sie DÜRFEN jedoch NICHT die Gültigkeitsdauer, des ausstellenden Sub-CA-Zertifikats oder des in der OCSP-Antwort im Feld BasicOCSPResponse.certs enthaltenen Zertifikats überschreiten.

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

Die einmal auf OCSP-Anfragen erstellten OCSP-Antworten DÜRFEN vorgehalten und innerhalb ihrer Gültigkeit für weitere Anfragen wiederverwendet werden.

[TLS] [SMIME] 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.

OCSP-Anfragen zu nicht vergebenen Seriennummern SOLLTEN protokolliert 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.

[TLS] [SMIME] CARLs DÜRFEN eine Gültigkeit von 12 Monaten NICHT überschreiten, CRLs 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 in der nächsten regulären Sperrliste nach ihrem Gültigkeitsende enthalten sein.

[QCP] Wenn Sperrlisten und OCSP-Auskünfte bereitgestellt werden, SOLLTEN abgelaufene Zertifikate NICHT aus der Sperrliste entfernt werden. Wenn ausschließlich Sperrlisten angeboten werden, DÜRFEN abgelaufene Zertifikate NICHT aus der Sperrliste entfernt werden.

4.10.2 Verfügbarkeit

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

[SSL] [SMIME] 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 maximale Ausfallzeit der Systeme MUSS in den CPS aufgeführt werden.

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 sichergestellt werden, 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

In einer vom Management freigegebenen Informationssicherheitsrichtlinie MUSS der Ansatz zum Management der Informationssicherheit festgelegt werden und es MUSS ein geeignetes Informationssicherheits-Management-System (ISMS, z.B. in Anlehnung an ISO 27001) etabliert werden, 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.

Risikoanalysen, 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, identifizieren, analysieren und bewerten, MÜSSEN jährlich durchgeführt werden.

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

Zur Vermeidung von Verlust, Diebstahl, Schaden oder Kompromittierung von Anlagen, Medien und Informationen MÜSSEN physikalische Maßnahmen getroffen werden.

5.1.1 Standort und Bauweise

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

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

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

5.1.8 Externe 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

[TLS] Ergänzend zu den o.g. Rollen MUSS die Rolle des Validierungsspezialisten etabliert werden.

Die relevanten Rollen des TSP incl. einer Übersicht der zugewiesenen Tätigkeiten MÜSSEN im CPS beschrieben 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. Zur Sicherstellung des Vier-Augen-Prinzips MÜSSEN auditierbare Sicherheitsmaßnahmen umgesetzt werden.

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

5.2.3 Identifizierung und Authentifizierung für vertrauenswürdige Rollen

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

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

Vor der Übertragung einer vertrauenswürdigen Rolle MUSS 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.

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 Struktur, die die Unparteilichkeit des Betriebs gewährleistet, MUSS dokumentiert werden.

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 RA, siehe Kap. 1.3.2), MÜSSEN 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,
- Anträge für eigene Zertifikate einer Organisation, die eine externe Registrierungsstelle betreibt, sowie Zertifikate für die Mitarbeiter dieser Organisation.

Die Ausnahmen MÜSSEN in den CPS beschrieben werden.

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 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

Vor der Einstellung einer Person MUSS dessen Identität und Vertrauenswürdigkeit überprüft werden.

[EVCP] Es MUSS sichergestellt werden, 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] Es MUSS sichergestellt werden, 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).

[TLS] Alle mit der Validierung der Zertifikatsanträge betrauten Mitarbeiter MÜSSEN zu folgenden Themen geschult werden:

- 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].

Zu diesen Schulungen MÜSSEN Nachweise geführt werden und es MUSS dokumentiert werden, dass jeder mit der Validierung betraute Mitarbeiter über das erforderliche Know-How verfügt, bevor dieser die Tätigkeiten übernimmt.

Darüber hinaus MUSS von allen Validierungsspezialisten verlangt werden, dass sie eine vom TSP bereitgestellte Prüfung der in den [BR] aufgeführten Anforderungen zur Überprüfung von Informationen bestehen.

5.3.4 Nachschulungsintervalle und -anforderungen

Die Mitarbeiter SOLLTEN regelmäßig (mindestens jährlich) zu aktuellen Bedrohungen und Sicherheitspraktiken geschult werden.

Durch geeignete regelmäßige Schulungen MUSS sichergestellt werden, 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 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.

[TLS] Das an der Ausstellung von Zertifikaten beteiligte Personal von Dritten MUSS bzgl. der Einhaltung der Schulungs- und Qualifikationsanforderungen gemäß Kap. 5.3.1 und 5.3.3 überprüft werden.

[3145] Gegenüber beteiligten Dritten MÜSSEN deren Verantwortlichkeiten sowie die relevanten Praktiken klar definiert und geeignete Vorkehrungen getroffen werden, 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, der authentifizierten Endteilnehmer sowie der externen RAs mit Angabe von Datum, Uhrzeit und Identität der handelnden Person aufzeichnen:

- Alle Aktivitäten im Zusammenhang mit der Registrierung, der Bearbeitung von Anträgen auf Ausstellung, Erneuerung und Sperrung von Zertifikaten aller Hierarchiestufen,
- alle Aktivitäten im Zusammenhang mit dem Lebenszyklus von Root-, CA- und, sofern anwendbar, Endteilnehmer-Schlüsseln und -Zertifikaten Dazu zählen mindestens Schlüsselgenerierung, -Speicherung, -Backup, -Wiederherstellung, -Archivierung und -Zerstörung, Generierung und ggf. Sperrung,
- alle Aktivitäten bzgl. des Lebenszyklus der kryptografischen Module.

[TLS] Ergänzend zu obiger Auflistung MÜSSEN folgende Aktivitäten aufgezeichnet werden:

- alle Validierungen gemäß den [BR] und den CPS der TSP,
- Inbetriebnahme neuer sowie Außerbetriebnahme nicht mehr verwendeter Zertifikatstemplates

[NCP+] Ergänzend zu obiger Auflistung MÜSSEN alle Ereignisse im Zusammenhang mit der Vorbereitung bzw. Bereitstellung des Schlüsselmittels des Endteilnehmers aufgezeichnet werden.

5.4.1.2 Technische Systemereignisse

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

- alle wesentlichen Ereignisse im Zertifikats- und Schlüsselmanagement,
- die Generierung von Sperrlisten und OCSP-Antworten,
- alle sicherheitsrelevanten Ereignisse an den PKI- und Sicherheitssystemen, insbesondere Änderungen der Sicherheitsrichtlinien der Systeme, das Starten und Herunterfahren der Systeme, Systemabstürze und Hardwarefehler, Uhrzeitsynchronisationsereignisse, Firewall- und Router-Aktivitäten sowie erfolgreiche und nicht erfolgreiche PKI-Systemzugriffsversuche,
- Installation, Update und Deinstallation von Software auf den PKI-Systemen,
- alle (physikalischen) Ein- und Ausgänge zu den Sicherheitszonen

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

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. 0 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 Aufbewahrungszeiträume MÜSSEN in den CPS beschrieben werden, siehe dazu auch Kap. 5.5.2.

Bzgl. der Aufbewahrungsfrist der in Kap. 0 aufgeführten Ereignisse gibt es keine Vorgabe, die TSP SOLLTEN die Aufbewahrungsdauern in ihren CPS beschreiben.

[TLS] Die in Kap. 0 aufgeführten Ereignisse MÜSSEN für mindestens zwei Jahre nach ihrem Eintreten aufbewahrt werden.

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. In den CPS MUSS beschrieben werden, wie der Schutz dieser Aufzeichnungen sichergestellt wird.

[TLS] [SMIME] Die Aufbewahrung der Aufzeichnungen MUSS überwacht werden (z.B. in internen Audits).

[3145] Die technischen Systemereignisse gemäß Kap. 0 MÜSSEN in einem separaten manipulationssicheren System, d.h. nicht nur in dem System, in dem die Ereignisse protokolliert werden, gespeichert werden.

5.4.5 Backup-Verfahren für Audit-Protokolle

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

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 Aufzeichnungen MÜSSEN so archiviert werden, dass alle ausgestellten Zertifikate eindeutig einem registrierten Antragsteller zugeordnet werden 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

Mindestens folgende Daten MÜSSEN archiviert werden:

- 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.

[QCP] Darüber hinaus MÜSSEN ggf. weitere Informationen archiviert werden, die vom TSP ausgegeben und empfangen wurden, und als Beweismittel in Gerichtsverfahren benötigt werden könnten.

[TLS] Zu jedem ausgestellten Zertifikat MUSS die verwendete Methode zur Validierung des Domain Namens oder der IP-Adresse gemäß [BR#3.2.2.4] und [BR#3.2.2.5] inkl. der der Validierung zugrunde liegende Version der [BR] archiviert werden.

Unter Berücksichtigung der relevanten Datenschutzaspekte DÜRFEN weitere Daten archiviert werden. In den CPS sowie den Nutzungsbedingungen MUSS beschrieben werden, welche Daten archiviert werden.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die Daten zu einem Zertifikat MÜSSEN für mindestens 7 Jahre nach Ablauf der Gültigkeit des Zertifikats archiviert werden. Die Aufbewahrungszeiträume (ggf. je Zertifikatstyp) MÜSSEN in den CPS sowie den Nutzungsbedingungen beschrieben werden.

[TLS] Es MUSS überprüft werden, ob vom TSP beauftragte Dritte die Anforderungen für die Aufbewahrung von Dokumenten und die Protokollierung von Ereignissen gemäß Kap. 5.4.1 erfüllen.

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. In den CPS MUSS beschrieben werden, wie der Schutz der archivierten Informationen sichergestellt wird.

[EVCP] Die Archivierung der Informationen MUSS überwacht werden (z.B. in internen Audits).

5.5.4 Backup-Verfahren für Archive

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

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.

Die Zugriffsmöglichkeiten auf die Archivinformationen MÜSSEN festgelegt und dokumentiert werden.

5.6 Schlüsselwechsel

Vor Ablauf eines CA-Zertifikats MUSS, sofern der betroffene Dienst fortgesetzt werden soll, rechtzeitig ein neues CA-Zertifikat gemäß den aktuellen Versionen dieser CP und dem CPS beantragt werden. Dabei SOLLTE der Zeitraum zwischen der Veröffentlichung des neuen CA-Zertifikats und der Außerbetriebnahme des ablaufenden CA-Zertifikats hinreichend groß gewählt werden, 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 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen sowie zur Wiederherstellung nach Ausfällen oder Katastrophen MÜSSEN in der Notfalldokumentation beschrieben werden.

Die Notfalldokumentation MUSS folgende Aspekte beinhalten:

- Notfallvorsorge
  - Vorgaben zum Backup kritischen kryptografischen Materials an einem anderen Standort,
  - Vorgaben zum regelmäßigen Backup aller relevanten Daten, 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 Notfalldokumentation MUSS den Auditoren auf Anfrage offengelegt werden.

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

Die Verfahren zur Meldung von Vorfällen MÜSSEN festgelegt werden und es MUSS sichergestellt werden, dass diese den Mitarbeitern bekannt sind und genutzt werden.

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

[TLS] [SMIME] Verstöße gegen die Mozilla Root Store Policy MÜSSEN unverzüglich in Form eines Vorfallberichts („Bugzilla“) an Mozilla gemeldet werden und es SOLLTE die Ausgabe der betroffenen Zertifikatstypen eingestellt werden, bis die Ursache für den Verstoß behoben ist.

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 Kompromittierung, der Verdacht auf Kompromittierung und der Verlust eines privaten CA-Schlüssels MÜSSEN als Notfall in der Notfalldokumentation festgelegt werden und die daraus resultierenden Aktivitäten MÜSSEN beschrieben werden.

Im Falle einer Kompromittierung eines CA-Schlüssels MUSS das korrespondierende CA-Zertifikat gesperrt werden und alle Betroffenen (Endteilnehmer sowie alle Weiteren, mit denen die TSP Vereinbarungen getroffen haben) informiert werden. Darüber hinaus MUSS vertrauenden Dritten die Informationen verfügbar gemacht werden und angezeigt werden, dass den von der betroffenen CA ausgestellten Zertifikaten und Statusauskünften nicht mehr vertraut werden kann.

Des Weiteren SOLLTEN alle Endteilnehmerzertifikate (mit Ausnahme von Kurzzeitzertifikaten) gesperrt werden.

[QCP] Die Verfahren zur Bereitstellung der Statusinformationen zu Endteilnehmerzertifikaten im Falle der Kompromittierung eines CA-Schlüssels MÜSSEN in den CPS beschrieben werden.

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

5.7.4 Geschäftsfortführung nach einem Notfall

Siehe Kap. 5.7.1.

5.8 Einstellung des CA oder RA Betriebes

Die Vorkehrungen, die zur Beendigung eines Dienstes getroffen werden, MÜSSEN in den CPS beschrieben werden, 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 Verfahren zur Bereitstellung der Statusinformationen nach der Beendigung eines Dienstes MÜSSEN in den CPS beschrieben werden.

Ein aktueller Beendigungsplan MUSS vorgehalten werden.

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

[3145] Anstelle der Fortführung eines Dienste durch eine andere Stelle DARF ein Dienst eingestellt werden, sofern eine sichere Einstellung des Dienstes garantiert werden kann.

Vor der Einstellung eines Dienstes MÜSSEN

- alle Betroffenen informiert werden (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 bereitgestellt werden,
- die Vereinbarungen mit externen RAs beendet werden,
- eine zuverlässige Stelle verpflichtet werden, 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 zerstört oder so außer Betrieb genommen werde, dass diese nicht wiederverwendet werden können,
- die CA-Zertifikate gesperrt werden,
- ggf. ausgestellte Cross-Zertifikate gesperrt werden.

Die CA-Zertifikate MÜSSEN für einen angemessenen Zeitraum nach Beendigung noch Vom TSP selbst bereitgestellt werden oder es MUSS eine andere Stelle dazu verpflichtet werden.

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

[3145] Alle Schlüssel, Zertifikate und Kundendaten MÜSSEN gelöscht werden.

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 Trust Centers 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.0) MÜSSEN die Schlüsselzeremonie überwachen und deren korrekte Durchführung im Protokoll bestätigen.

Darüber hinaus MUSS der externe Auditor (siehe Kap. 0) 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.

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] Die Schlüsselzeremonie MUSS durch 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. 0) 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] 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. 0) 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

RA Schlüsselpaare MÜSSEN in kryptografischen Modulen gemäß Kap. 6.2.1 generiert werden.

6.1.1.4 Generierung von Endteilnehmer-Schlüsselpaaren

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

[TLS] Teilnehmer-Schlüssel, die zur Authentisierung von Servern genutzt werden können, DÜRFEN NICHT durch die Sub-CA generiert werden.

Wenn Teilnehmer-Schlüssel durch die Teilnehmer generiert werden, so MÜSSEN die Teilnehmer über die zu verwendenden zulässigen Algorithmen und Schlüssellängen informiert werden.

Wenn Teilnehmer-Schlüssel durch die Sub-CA erzeugt werden, so MÜSSEN die Schlüssel auf eine sichere Art und Weise generiert werden und bis zur Zertifikatserzeugung vorgehalten werden, 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.

[QCP-n-qscd] [QCP-l-qscd] Teilnehmer-Schlüsselpaare MÜSSEN durch ein zertifiziertes QSCD (siehe Kap. 6.2.1) erzeugt werden.

[3145] Wenn Teilnehmer-Schlüssel für kryptografischen Token als Speichermedium von der Sub-CA generiert werden,

- SOLLTEN die Schlüssel durch den Token selbst generiert werden,
- MÜSSEN außerhalb des Tokens erzeugte Schlüssel sofort nach dem Einbringen in den Token gelöscht werden, sofern keine Sicherung der Teilnehmer-Schlüssel angeboten wird.

6.1.2 Bereitstellung der privaten Schlüssel an die Endteilnehmer

Wenn Schlüssel der Endteilnehmer vom TSP generiert werden, MÜSSEN folgende Vorgaben berücksichtigt werden:

- 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).

[LCP] [NCP] Wenn Schlüssel der Endteilnehmer vom TSP generiert werden, MÜSSEN diese auf sicherem Weg dem registrierten Zertifikatsinhaber übergeben werden, es sei denn die TSP verwalten die Schlüssel im Auftrag des Endteilnehmers.

[NCP] Wenn Schlüssel der Endteilnehmer vom TSP generiert und im Auftrag des Endteilnehmers verwaltet werden und die Schlüsselverwendung in den korrespondierenden Zertifikaten mit „nonRepudiation“ festgelegt ist, MUSS sichergestellt werden, dass die Endteilnehmer die alleinige Kontrolle über die Schlüssel haben.

Für den Fall, dass ein anderer TSP als der, der die Schlüssel generiert und die Zertifikate ausgestellt hat, die Schlüssel der Endteilnehmer in deren Auftrag verwaltet und die Schlüsselverwendung in den korrespondierenden Zertifikaten mit „nonRepudiation“ festgelegt ist, MUSS der TSP, der die Schlüssel generiert und die Zertifikate ausgestellt hat, sich bestätigen lassen, dass der die Schlüssel verwaltende TSP sicherstellt, dass die Endteilnehmer die alleinige Kontrolle über die Schlüssel haben.

Die Konformität zu [ETS431-1] SOLLTE verwendet werden, um nachzuweisen, dass ein TSP, der Schlüssel im Auftrag der Endteilnehmer verwaltet, die Anforderungen zur Gewährleistung der alleinigen Kontrolle über die Schlüssel erfüllt.

[NCP+] Wenn Schlüssel der Endteilnehmer vom TSP generiert werden, MUSS sichergestellt werden, dass diese auf sicheren kryptografischen Geräten (z.B. Smartcards) auf sichere Art und Weise den registrierten Endteilnehmern übergeben werden. Für den Fall, dass ein Endteilnehmer seine Schlüssel von einem anderen TSP als dem, der die Schlüssel generiert und die Zertifikate ausgestellt hat, verwalten lässt, muss das Gerät diesem TSP auf sicherem Weg übergeben werden.

[QCP-n-qscd] [QCP-l-qscd] Wenn ein TSP QSCDs von Endteilnehmern verwaltet, MUSS die alleinige Kontrolle der Endteilnehmer über ihre QSCD sichergestellt werden.

6.1.3 Übergabe öffentlicher Schlüssel an die TSP

Keine Vorgabe.

[TLS] Die Formate und die Methoden der akzeptierten elektronischen Zertifikatsrequests SOLLTEN in den CPS oder dort referenzierten Dokumenten festgelegt werden.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

Die Root- und CA-Zertifikate MÜSSEN allgemein zugänglich in integrer und authentischer Form bereitgestellt werden. 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

Alle Schlüssel MÜSSEN gemäß den nachfolgend aufgeführten Anforderungen generiert werden. Von Antragstellern vorgelegte Schlüssel, die nicht diesen Anforderungen genügen, DÜRFEN NICHT akzeptiert werden. Sollten die verwendeten Schlüssellängen aufgrund neuer Erkenntnisse oder Vorgaben für den Verwendungszweck nicht mehr ausreichen, so MÜSSEN die Zertifikatsnehmer und vertrauende Dritte darüber informiert werden und es MUSS ein Zeitplan zur Sperrung betroffener Zertifikate sowie zur Migration auf hinreichend lange Schlüssel festgelegt werden.

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

[TLS] [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] Die Anforderungen aus [TR2102-1] MÜSSEN beachtet werden.

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Keine Vorgabe.

[TLS] Folgende Anforderungen an die Schlüssel MÜSSEN bei den selbst generierten Schlüsseln umgesetzt bzw. bei den 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: Die Schlüssel SOLLTEN entweder mit der ECC-Routine zur vollständigen Validierung öffentlicher Schlüssel oder mit der ECC-Routine zur teilweisen Validierung öffentlicher Schlüssel geprüft werden.

6.1.7 Schlüsselverwendung

Die Verwendung eines privaten Schlüssels MUSS auf die im korrespondierenden Zertifikat in den Attributen keyUsage und, sofern vorhanden, extendedKeyUsage (siehe Kap. 7.1.2) aufgeführten Verwendungszwecke beschränkt werden.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

Zum Schutz der privaten Schlüssel aller Hierarchieebenen MÜSSEN hinreichende Sicherheitsmaßnahmen getroffen bzw. den Zertifikatsnehmern vorgegeben werden.

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 in den CPS und ggf. Nutzungsbedingungen beschrieben werden.

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 140-2 Level 3 zertifiziert sind.

Eine Manipulation kryptografischer Module bei Lagerung und Transport MUSS ausgeschlossen 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 gemäß [eIDAS#Art.29-30] zertifiziert sein. Der Zertifizierungsstatus der QSCD MUSS bis zum Ablauf der Gültigkeit der Endteilnehmerzertifikate gemonitort werden und es MÜSSEN entsprechende Maßnahmen eingeleitet werden, 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 von Root- und Sub-CA-Schlüsseln 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), auf das Beisein eines externen Auditors DARF jedoch verzichtet werden. Darüber hinaus MUSS sichergestellt sein, dass der Zugriff auf die Sicherungen mindestens zwei vertrauenswürdige Mitarbeiter des TSP erfordert.

[3145] Wenn Schlüssel im Auftrag der Endteilnehmer gesichert werden, MÜSSEN

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

[VS-NfD] Wenn Schlüssel im Auftrag der Endteilnehmer gesichert werden,

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

6.2.5 Archivierung privater Schlüssel

Keine Vorgabe.

[TLS] Die privaten Schlüssel einer Sub-CA DRÜFEN NICHT ohne die Erlaubnis des TSP durch andere Parteien archiviert werden. Ebenso DÜRFEN die privaten Schlüssel eines Endteilnehmers NICHT ohne dessen Erlaubnis archiviert werden.

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), auf das Beisein eines externen Auditors DARF jedoch verzichtet werden.

[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

Wenn Schlüssel für Endteilnehmer erzeugt und diesen übergeben werden, MUSS sichergestellt werden, dass deren Aktivierung durch die Endteilnehmer auf sichere Art und Weise erfolgt. Die erforderlichen Maßnahmen und Vorgaben MÜSSEN in den CPS und ggf. den Nutzungsbedingungen beschrieben werden.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

Wenn Schlüssel für Endteilnehmer erzeugt und diesen mittels kryptografischer Module (z.B. Smartcards) übergeben werden, MUSS sichergestellt werden, dass deren Deaktivierung und ggf. Reaktivierung durch die Endteilnehmer auf sichere Art und Weise erfolgen. Die erforderlichen Maßnahmen und Vorgaben MÜSSEN in den CPS und ggf. den Nutzungsbedingungen beschrieben werden.

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 MÜSSEN berücksichtigt werden. 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

Kryptografische Module MÜSSEN vor der Beschaffung bzgl. ihrer Nutzbarkeit und der Erfüllung aller Anforderungen bewertet werden.

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.

Das Gültigkeitsende eines Zertifikats DARF das Gültigkeitsende des Zertifikats der ausstellenden 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.

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

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

[SMIME] Endteilnehmerzertifikate SOLLTEN NICHT länger als 825 Tage (d.h. zwei Jahre zzgl. einer Karenzzeit von max. drei Monaten) und DÜRFEN NICHT länger als 1095 Tage gültig sein.

[3145] Die Nutzung des privaten Schlüssels einer Sub-CA MUSS, 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.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

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

6.4.2 Schutz der Aktivierungsdaten

Wenn vom TSP Aktivierungsdaten erzeugt werden (siehe Kap. 6.4.1) MÜSSEN diese von der Erzeugung bis zur Übergabe an den Endteilnehmer so geschützt werden, dass deren Integrität und Vertraulichkeit gewahrt bleibt und sie MÜSSEN dem Endteilnehmer getrennt von den kryptografischen Modulen zeitversetzt oder über verschiedene Wege übermittelt werden.

6.4.3 Andere Aspekte der Aktivierungsdaten

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 für das Zertifikatsmanagement sowie die Status- und Verzeichnisdienste erforderlichen Systeme MÜSSEN dem Schadenspotential entsprechend geschützt werden.

Die die Accounts der für den Betrieb der kritischen Systeme erforderlichen vertrauenswürdigen Rollen (siehe Kap. 5.2.1) MÜSSEN so gemanagt werden, 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
- sie in angemessener Zeit geändert oder gelöscht werden.

Für die Accounts, welche direkt die Erstellung von Zertifikaten auslösen können, MUSS eine Multi-Faktor-Authentisierung umgesetzt werden.

Die geforderte Trennung von vertrauenswürdigen Rollen (siehe Kap. 5.2.4) MUSS von den Systemen technisch unterstützt werden.

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

[SMIME] Für alle Accounts

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

MUSS eine Multi-Faktor-Authentisierung umgesetzt werden.

[TLS] [SMIME] Die Accounts der zugriffsberechtigten Personen MÜSSEN mindestens alle drei Monate überprüft werden, nicht mehr benötigte Accounts MÜSSEN deaktiviert werden.

Bei allen Systemen, die eine Multi-Faktor-Authentisierung unterstützen, MUSS eine Multi-Faktor-Authentisierung umgesetzt werden.

Die Authentifizierungsschlüssel und Passworte der privilegierten Accounts der CA-Systeme MÜSSEN geändert werden, wenn sich die Berechtigung einer Person zum administrativen Zugriff auf die Systeme ändert oder entzogen wird.

Für vertrauenswürdige Rollen MUSS sichergestellt werden, 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, MÜSSEN, sofern technisch möglich, die nachfolgend aufgeführten Maßnahmen umgesetzt werden:

- 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, MUSS eine Multi-Faktor-Authentifizierung umgesetzt werden.
- Für Konten, auf die von außerhalb einer Sicherheitszone zugegriffen werden kann, MÜSSEN Kennwörter mit mindestens acht Zeichen gefordert werden, bei denen es sich nicht um eines der vorherigen vier Kennwörter des Benutzers handelt und es MUSS eine Kontosperre nach fünf fehlgeschlagenen Zugriffsversuchen (s.u.) umgesetzt werden.
- Bei der Entwicklung von Passwort-Richtlinien SOLLTEN die Passwort-Richtlinien in NIST 800-63B Anhang A berücksichtigt werden.
- wenn ein TSP eine Passwortrichtlinie hat, welche eine routinemäßige periodische Passwortänderungen erfordert, DARF dieser Zeitraum NICHT weniger als zwei Jahre betragen,

Personen in vertrauenswürdigen Rollen MÜSSEN verpflichtet werden, sich von ihrem Account abzumelden oder ihren Arbeitsplatz zu sperren, wenn sie nicht mehr in der Rolle tätig sind.

Die Arbeitsplätze MÜSSEN entweder so konfiguriert werden, dass diese automatisch nach einer festgelegten Zeit der Inaktivität des Nutzers gesperrt werden oder die relevanten Anwendungen MÜSSEN so konfigurieren, dass diese automatisch nach einer festgelegten Zeit der Inaktivität des Nutzers zur Abmeldung des Accounts führen.

Der Zugang zu CA-Systemen MUSS nach fünf fehlgeschlagenen Anmeldeversuchen gesperrt werden, vorausgesetzt, dass das CA-System diese Maßnahme unterstützt, die Maßnahme nicht für Denial of Service-Angriffe genutzt werden kann und die Maßnahme nicht die Sicherheit dieser Authentifizierungskontrolle schwächt,

Für den administrativen Zugriff auf kritische Systeme MUSS eine Multi-Faktor-Authentisierung oder eine Mehr-Personen-Authentifizierung sichergestellt werden,

Für alle Accounts der vertrauenswürdigen Rollen an den CA-Systemen, die von außerhalb der sicheren Umgebungen erreichbar sind, MUSS eine Multifaktor-Authentisierung sichergestellt werden.

Remote-Zugriffe auf kritische Systeme DÜRFEN 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.

Es MÜSSEN vertrauenswürdige Systeme eingesetzt werden, 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 zur Zertifikatserzeugung und ggf. -Sperrung erfassten Daten inkl. der Protokolldaten gemäß Kap. 5.4.1 MÜSSEN so gesichert werden, dass deren Integrität, Vertraulichkeit und Verfügbarkeit über den gesamten Aufbewahrungszeitraum sichergestellt ist.

Für die Produktivumgebung und die Test- bzw. Entwicklungsumgebung MÜSSEN getrennte Systeme verwendet werden.

6.5.2 Sicherheitsbewertung von Computern

Keine Vorgabe.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Steuerung der Systementwicklung

Bereits in der Entwurfs- und Anforderungsspezifikationsphase eines Systementwicklungsprojekts MUSS eine Analyse der Sicherheitsanforderungen durchgeführt werden, 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.

Es MUSS sichergestellt werden, 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.

Folgender Aktivitäten MÜSSEN überwacht werden und es MÜSSEN geeignete Alarmierungsfunktionen implementiert werden:

- 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,
- Konfigurationsänderungen, die nicht auf Basis eines autorisierten Changes durchgeführt wurden.

Bei der Überwachung SOLLTE die Sensibilität aller gesammelten oder analysierten Informationen berücksichtigt werden.

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.

[TLS] [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.

[NCP] Der Kapazitätsbedarf der Systeme MUSS überwacht werden und Prognosen für den zukünftigen Kapazitätsbedarf MÜSSEN erstellt werden, um sicherzustellen, dass angemessene Verarbeitungsleistungen und Speicherkapazitäten zur Verfügung stehen.

6.6.3 Sicherheitskontrollen während des Lebenszyklus

Für die Verwaltung aller kryptographischen Schlüssel und Geräte MÜSSEN geeignete Sicherheitskontrollen während ihres gesamten Lebenszyklus umgesetzt werden.

6.7 Netzwerk-Sicherheitskontrollen

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

[TLS] [SMIME] Es MÜSSEN Intrusion-Detection- (IDS) und Intrusion-Prevention-Systeme (IPS) implementiert werden, welche die TSP 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 Netzwerke oder Zonen MÜSSEN auf der Grundlage einer Risikobewertung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehung zwischen vertrauenswürdigen Systemen und Diensten segmentiert werden.

[VS-NfD] Bei der Netzwerktrennung MUSS [ISI LANA] als Leitfaden angewendet werden.

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. Es MÜSSEN Sicherheitsverfahren implementiert und konfiguriert werden, welche die Systeme und die Kommunikation zwischen Systemen innerhalb von Sicherheitszonen schützt.

Die Netzwerke zur Administration der Systeme MÜSSEN von den operativen Netzwerken separiert werden.

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 schützen. 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 o.g. Regeln MÜSSEN regelmäßig überprüft werden.

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.

Schwachstellenprüfungen an öffentlichen und privaten IP-Adressen, die vom TSP identifiziert wurden, MÜSSEN mindestens quartalsweise durchgeführt werden. 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 Durchführung der Schwachstellenprüfung MUSS mit Angabe der Qualifikation der prüfenden Person oder Organisation dokumentiert werden.

Bei Inbetriebnahme oder bei signifikanten Änderungen an der Infrastruktur oder den Anwendungen, mindestens aber einmal pro Jahr MÜSSEN die Systeme Penetrationstests unterzogen werden. 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 Durchführung der Penetrationstests MUSS mit Angabe der Qualifikation der prüfenden Person oder Organisation dokumentiert werden.

[TLS] [SMIME] Die o.g. Schwachstellenprüfungen MÜSSEN

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

durchgeführt werden.

Innerhalb von 48 Stunden nach der Entdeckung einer kritischen Schwachstelle

- MUSS diese Schwachstelle behoben werden oder
- wenn eine Behebung der Schwachstelle innerhalb von 48 Stunden nicht möglich ist, MUSS ein Plan zur Minderung der Schwachstelle, inkl. einer Priorisierung anhand der betroffenen Systeme, erstellt werden oder
- die faktische Grundlage für die Entscheidung des TSP, dass eine 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, MUSS dokumentiert werden.

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 Zertifikatsprofile MÜSSEN dem RFC5280 sowie den Empfehlungen der ITU-T X.509 entsprechen und in den CPS der TSP beschrieben werden.

Die Zertifikatsprofile gelten für alle Zertifikate, die ab dem Gültigkeitsbeginn dieser CP ausgestellt werden. Bereits ausgestellte Zertifikate mit Profilen gemäß älterer Anforderungen behalten ihre Gültigkeit bei, sofern nicht explizit auf deren Ungültigkeit hingewiesen wird.

[TLS] [SMIME] Die Seriennummern MÜSSEN mindestens 64 Bit groß sein und mit einem kryptographisch sicheren Zufallszahlengenerator erstellt werden.

Pre-Zertifikate gemäß RFC 6962 (“Certificate Transparency”) gelten nicht als gültige Zertifikate im Sinne des RFC 5280.

[NCP] Die Seriennummern MÜSSEN größer als Null (positiver Integerwert) sein und DÜRFEN eine maximale Länge von 160 Bit NICHT überschreiten und mit einem kryptographisch sicheren Zufallszahlengenerator erstellt werden.

7.1.1 Versionsnummer

Alle X509-Zertifikate MÜSSEN in der Version 3 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[6]. Erweiterungen, die 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.
- ***(#)*** Verweis auf die der auf die Tabelle folgenden Beschreibung der zu setzenden Parameter bzw. Inhalte.

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

Tabelle 2 - Zertifikatserweiterungen

Erweiterung gem. RFC5280 (OID)	Root-CA	Sub-CA	Endteilnehmer	OCSP-Signer[7]
AuthorityKeyIdentifier (2.5.29.35)	O	M (01)	M (01)	M (01)
SubjectKeyIdentifier (2.5.29.14)	M (02)	M (02)	S	S
KeyUsage (2.5.29.15)	M K (03)	M K (03)	M K [TLS] O (04)(05)	M K
CertificatePolicies (2.5.29.32)	O [TLS] SN (06)	O [TLS] M (06)(07)(08)(09)(10)	M (06)(11)(13)(14)	N
subjectAltName (2.5.29.17)	O (15)	O (15)	O [TLS] [SMIME] M (15)(16)(17)(18)	N
BasicConstraints (2.5.29.19)	M K (19)	M K (19)	O (K) (20)	O (K) (20)
NameConstraints (2.5.29.30)	N	O [TLS] [SMIME] (M) K (21)	N	N
ExtendedKeyUsage (2.5.29.37)	N	SN [TLS] [SMIME] M (22)(23)(24)(25)(26)	O [TLS] [SMIME] M (22)(26)(27)(28)	M (22)(29)
cRLDistributionPoints (2.5.29.31)	N	(M) [TLS] [SMIME] M (30)(31)	(M) [TLS] [SMIME] M (30)(32)(33)	O[8] [TLS] N
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	N	(M) [TLS] [SMIME] M (34)(35)	(M) [TLS] [SMIME] M (34)(36)	O[8] [TLS] SN
qcStatements (1.3.6.1.5.5.7.1.3)	N	N	N [QCP] M (37)(38)	N
validity model 1.3.6.1.4.1.8301.3.5	N	N [QCP] O	N [QCP] M	N
IssuerAlternativeName (2.5.29.18)	SN	SN	O	N
SubjectDirectoryAttributes (2.5.29.9)	SN	SN	O	N
id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)	N	N	N	O[8] [TLS] M
cabfOrganizationIdentifier (2.23.140.3.1)	N	N	N [EVCP] (M) (39)	N
signedCertificateTimestampList (1.3.6.1.4.1.11129.2.4.2)	N	N	N [TLS] M (40)	O
id-etsi-ext-valassured-ST-certs (0.4.0.194121.2.1)	N	N	(M) (41)	N

[7] Die hier aufgeführten Anforderungen gelten für alle OCSP-Signer der öffentlichen Root- oder Sub-CAs, sollten aber mangels sonstiger Anforderungen an OCSP-Signer und im Sinne der Vereinheitlichung grundsätzlich für alle OCSP-Signer angewendet werden.
[8] Siehe dazu Kap. 7.3

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

AuthorityKeyIdentifier

(01) In Sub-CA-, Endteilnehmer- und OCSP-Signer-Zertifikaten MUSS der „keyIdentifier“ gemäß [RFC5280#4.2.1.1] gesetzt werden.

SubjectKeyIdentifier

(02) In Root- und Sub-CA-Zertifikaten MUSS der SubjectKeyIdentifier gesetzt werden und MUSS dem AuthorityKeyIdentifier in den von diesen (Root-) CAs ausgestellten Zertifikaten entsprechen.

KeyUsage

(03) 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. Andere Bits DÜRFEN NICHT gesetzt sein.

(04) In Endteilnehmer-Zertifikaten DÜRFEN die Bits für keyCertSign und cRLSign NICHT gesetzt sein, die übrigen Bits MÜSSEN ihrem Anwendungszweck entsprechend gemäß [RFC5280#4.2.1.3] gesetzt werden. Wenn die Erweiterung „ExtendedKeyUsage“ gesetzt ist, MÜSSEN die Bits der KeyUsage konsistent zu den Parametern der ExtendedKeyUsage gemäß [RFC5280#4.2.1.12] gesetzt werden.

(05) [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

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

(07) [TLS] [TSEC] In Sub-CA-Zertifikaten DARF eine OID enthalten sein, welche die Einhaltung der Baseline-Requirements 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) [TLS] [DFN] 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.

(09) [SMIME] In Sub-CA-Zertifikaten SOLLTE die OID für „anyPolicy“ (2.5.29.32.0) NICHT gesetzt werden.

(10) TLS] [SMIME] Die in Sub-CA- und Endteilnehmer-Zertifikaten gesetzten OIDs MÜSSEN zueinander korrespondieren, d.h. es DÜRFEN von einer Sub-CA NICHT Endteilnehmer-Zertifikate mit OIDs ausgestellt werden, welche in dem Sub-CA-Zertifikat selbst nicht enthalten sind („Policy-Chaining“).

(11) [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

Die OID für „anyPolicy“ (2.5.29.32.0) DARF NICHT gesetzt werden.

(12) [TLS] 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

Sofern es sich um qualifizierte Website-Zertifikate handelt, SOLLTE zusätzlich eine der folgenden OIDs enthalten sein:
- [QEVCP-w] 0.4.0.194112.1.4 (vormals QCP-w)
- [QNCP-w] 0.4.0.194112.1.5

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

Des Weiteren DARF der Qualifier „cPSuri“ mit einem Verweis (http URL) zum CPS oder anderen online verfügbaren Informationen des TSP gesetzt werden. Der Qualifier „user-Notice“ DARF NICHT gesetzt werden.

(13) [EVCP] In Endteilnehmerzertifikaten MUSS der Qualifier „cPSuri“ mit einem Verweis (http URL) zum CPS gesetzt werden.

(14) [3145] In Endteilnehmerzertifikaten DARF der Qualifier „userNotice“ NICHT gesetzt werden.

subjectAltName

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

(16) [SSL] In Root- und Sub-CA-Zertifikaten DARF die Erweiterung „subjectAltName“ NICHT gesetzt werden.
In Endteilnehmerzertifikaten MUSS mindestens ein Eintrag in die Erweiterung „subjectAltName“ aufgenommen werden. Zulässige Angaben sind FQDNs oder Wildcard Domain Names (als „dNSName“) oder IP-Adressen (IPv4 oder IPv6-Adressen als „iPAddress“).
Die FQDNs sowie die FQDN-Anteile von Wildcard Domain Names MÜSSEN ausschließlich aus „P-Labels“ oder „Non-Reserved LDH-Labels“ bestehen.
Reservierte IP-Adressen oder interne Namen DÜRFEN NICHT eingetragen werden.

(17) [EVCP] Die in Endteilnehmerzertifikaten aufgenommenen FQDNs MÜSSEN dem Endteilnehmer gehören oder von ihm kontrolliert werden und mit dessen Dienst verknüpft sein. Wildcard Domain Names DÜRFEN NICHT aufgenommen werden.

(18) [SMIME] In Endteilnehmerzertifikaten MUSS mindestens eine E-Mail-Adresse als rFC822Name in die Erweiterung „subjectAltName“ aufgenommen werden.

BasicConstraints

(19) 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.

(20) In Endteilnehmer- und OCSP-Signer-Zertifikaten MUSS das „cA“-Flag auf „false“ gesetzt sein. Das Feld „pathLenConstraints“ DARF NICHT gesetzt werden.

NameConstraints

(21) [TLS] [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

(22) Wenn die Erweiterung „ExtendedKeyUsage“ gesetzt ist, MÜSSEN die Bits der KeyUsage konsistent zu den Parametern der ExtendedKeyUsage gemäß [RFC5280#4.2.1.12] gesetzt werden.

(23) [TLS] In Sub-CA-Zertifikaten[9] 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.

(24) [SMIME] In Sub-CA-Zertifikaten[9] 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.

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

[9] Diese Anforderung gilt für alle Sub-CA Zertifikate, die nach dem 01.01.2019 ausgestellt werden und gilt nicht für Cross-Zertifikate.

(26) [TLS] [SMIME] Die in Sub-CA- und Endteilnehmer-Zertifikaten gesetzten OIDs MÜSSEN zueinander korrespondieren, d.h. es DÜRFEN von einer Sub-CA NICHT Endteilnehmer-Zertifikate mit OIDs ausgestellt werden, welche in dem Sub-CA-Zertifikat selbst nicht enthalten sind („EKU-Chaining“). Hiervon ausgenommen sind OCSP-Signer-Zertifikate, welche auch von Sub-CAs ausgestellt werden DÜRFEN, welche selbst nicht die OID 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning) enthalten.

(27) [TLS] 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

(28) [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.

(29) In OCSP-Signer-Zertifikaten MUSS die OID 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning) eingetragen werden. Weitere OIDs DÜRFEN NICHT eingetragen werden.

cRLDistributionPoints

(30) In allen Zertifikaten, deren Aussteller Sperrlisten anbietet, MUSS die Erweiterung cRLDistributionPoints mit mindestens einer http-URL, welche auf den Sperrlistenservice des TSP verweist, im Feld distributionPoints gesetzt werden.

(31) [TLS] [SMIME] In Sub-CA-Zertifikaten MUSS die Erweiterung cRLDistributionPoints mit mindestens einer http-URL, welche auf den Sperrlistenservice des TSP verweist, im Feld distributionPoints gesetzt werden.

(32) [TLS][SMIME] In Endteilnehmerzertifikaten MUSS die Erweiterung cRLDistributionPoints mit mindestens einer http-URL, welche auf den Sperrlistenservice des TSP verweist, im Feld distributionPoints gesetzt werden.

(33) [3145] [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten MUSS die Erweiterung cRLDistributionPoints gesetzt werden, wenn die ausstellende Sub-CA CRLs unterstützt. Wenn sie gesetzt wird, MUSS sie mindestens eine öffentlich erreichbare http-oder ldap-URL im Feld distributionPoints enthalten.

authorityInfoAccess

(34) In allen Zertifikaten, welche per OCSP prüfbar sind. 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))

(35) [TLS] In Sub-CA- und Endteilnehmer-Zertifikaten MUSS die Erweiterung authorityInfoAccess gesetzt werden und 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)).

(36) [LCP] [NCP] [NCP+] [QCP] [SMIME] In Endteilnehmer-Zertifikaten MUSS die Erweiterung authorityInfoAccess gesetzt werden und MUSS mindestens eine http- oder https-URL zum Download des ausstellenden Sub-CA-Zertifikats (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)) enthalten.

qcStatements

(37) [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 [ETS4125] berücksichtigt werden.

(38) [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

(39) [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 [EVCG] verwiesen.

signedCertificateTimestampList

(40) [SSL] In Endteilnehmerzertifikaten MÜSSEN mindestens folgende SCT enthalten sein:
- mindestens ein SCT eines beliebigen CT-Log-Servers, der zum Zeitpunkt der Überprüfung den Status „qualified“, „usable“ oder „readOnly“ hatte,
- mindestens ein SCT eines von Google betriebenen CT-Log-Servers, der zum Zeitpunkt der Überprüfung den Status „qualified“, „usable“, „readOnly“ oder „retired“ hatte,
- mindestens ein SCT eines nicht von Google betriebenen CT-Log-Servers, der zum Zeitpunkt der Überprüfung den Status „qualified“, „usable“, „readOnly“ oder „retired“ hatte.

id-etsi-ext-valassured-ST-certs

(41) In Endteilnehmerzertifikaten, die Kurzzeitzertifikate sind, MUSS die Erweiterung id-etsi-ext-valassured-ST-certs wie folgt gesetzt werden:
- in Kurzzeitzertifikaten, welche nicht gesperrt werden können, MUSS die Erweiterung id-etsi-ext-valassured-ST-certs gesetzt werden,
- in Kurzzeitzertifikaten, welche gesperrt werden können, SOLLTE die Erweiterung id-etsi-ext-valassured-ST-certs NICHT gesetzt werden.
- In Endteilnehmerzertifikaten, die keine Kurzzeitzertifikate sind, DARF die Erweiterung id-etsi-ext-valassured-ST-certs NICHT gesetzt werden.

7.1.3 Algorithmen-OID

Die für die Signatur der Zertifikate aller Hierarchieebenen verwendeten Algorithmen MÜSSEN den Anforderungen aus [SOGIS] genügen.

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:304106092a864886f70d01010a3034a00f300d06096086480165030402010500a2030201200a11c301a06092a864886f70d010108300d06096086480165030402010500a203020120
  - MGF-1 with SHA-384, and a salt length of 48 bytes, Hex-codierter Wert des AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d06096086480165030402020500a2030201300a11c301a06092a864886f70d010108300d06096086480165030402020500a203020130
  - MGF-1 with SHA-512, and a salt length of 64 bytes, Hex-codierter Wert des AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d06096086480165030402030500a2030201400a11c301a06092a864886f70d010108300d06096086480165030402030500a203020140

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.
- Falls ein Zertifikat für eine natürliche Person in Verbindung mit einer juristischen Person ausgestellt wird, dann MÜSSEN die Zertifikatsattribute, welche die Organisation identifizieren, die juristische Person widerspiegeln und das Subject im Zertifikat SOLL die natürliche Person sein.

Die folgende Tabelle gibt einen Überblick über obligatorische und optionale Zertifikatserweiterungen für Root-CA-, Sub-CA-, Endteilnehmer- und OCSP-Signer-Zertifikate[10]. Namensattribute, die dort nicht aufgeführt sind, DÜRFEN NICHT verwendet werden.

[10] CRL-Signer-Zertifikate werden nicht aufgeführt, da die CRLs von den CAs direkt ausgestellt 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.
- ***(#)*** Verweis auf die der auf die Tabelle folgenden Beschreibung der zu setzenden Inhalte.

Tabelle 3 - Namensformen

Subject-DN Attribut (OID)	**Root-CA**	**Sub-CA**	**Endteilnehmer**	**OCSP-Signer** [11]
commonName (2.5.4.3)	M (01)	M (01)	M [TLS] O (02)	M
serialNumber (2.5.4.5)	N	N	(M) (03)	N
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)	N
localityName (2.5.4.7)	N	N	(M) (10)	N
stateOrProvinceName (2.5.4.8)	N	N	(M) (11)	N
postalCode (2.5.4.17)	N	N	(M) (12)	N
businessCategory (2.5.4.15)	N	N	(M) (13)	N
organizationalUnitName (2.5.4.11)	N	N	O (14)	N
organizationIdentifier (2.5.4.97)	N [QCP] O	(S) (15)	(M) (16) (17)	N
jurisdictionOfIncorporation-LocalityName (1.3.6.1.4.1.311.60.2.1.1)	N	N	(M) (18)	N
jurisdictionOfIncorporation-StateOrProvinceN. (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 [TLS] [EVCP] (M) (24)	M
Sonstige Attribute	N	N	O [EVCP] N	N

[11] Die hier aufgeführten Anforderungen gelten für alle OCSP-Signer der öffentlichen Root- oder Sub-CAs, sollten aber mangels sonstiger Anforderungen an OCSP-Signer und im Sinne der Vereinheitlichung grundsätzlich für alle OCSP-Signer angewendet werden.

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

commonName

(01) [TLS] 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) [TLS] [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 einen Eintrag enthalten, der auch im subjectAltName enthalten ist. Bzgl. der Codierung des commonName gilt:

- IPv4-Adressen MÜSSEN gemäß RFC3986 codiert sein,
- IPv6-Adressen MÜSSEN gemäß RFC5952#4 codiert sein,
- FQDN und Wildcard Domain Names MÜSSEN eine Zeichen-für-Zeichen-Kopie des entsprechenden dNSName-Eintrags aus dem subjectAltName (siehe Kap. 7.1.2) sein.

(02) [EVCP] In Endteilnehmerzertifikaten DARF das Attribut commonName gesetzt werden. Wenn es gesetzt wird, MUSS es genau einen Domain Name 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. Wildcard-Zertifikate DÜRFEN NICHT ausgestellt werden, mit Ausnahme von „onion“-Zertifikaten[12].

serialNumber

(03) [LCP] [NCP] [NCP+] [QCP] In Endteilnehmerzertifikaten MUSS das Attribut serialNumber gesetzt werden, wenn die Attribute countryName, commonName sowie givenName und surname oder pseudonym nicht ausreichen, um die Eindeutigkeit des Namens zu gewährleisten. Das Attribut serialNumber hat keine definierte Semantik, die über die Sicherstellung der Eindeutigkeit des Subject-DNs hinausgeht.

[12] Siehe Appendix F der CABF EV Guidelines

(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.

givenName

(04) [IV] In Endteilnehmerzertifikaten DARF das Attribut givenName gesetzt werden. Wenn das Attribut givenName gesetzt wird, MUSS es zusammen mit dem Attribut surname den Namen des Zertifikatsinhabers enthalten.

(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.

surname

(06) [IV] In Endteilnehmerzertifikaten DARF das Attribut surname gesetzt werden. Wenn das Attribut surname gesetzt wird, MUSS es zusammen mit dem Attribut givenName den Namen des Zertifikatsinhabers enthalten.

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

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

postalCode

(12) [TLS] In Endteilnehmerzertifikaten DARF das Attribut postalCode gesetzt werden, wenn die Attribute surname und givenName oder organizationName gesetzt sind. Es DARF NICHT gesetzt werden, wenn die Attribute surname und givenName oder organizationName 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[13] der folgenden Werte gesetzt werden:

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

organizationalUnitName

(14) [SSL] In Endteilnehmerzertifikaten DARF das Attribut organizationalUnitName bei Zertifikaten gesetzt werden, die vor dem 1.09.2022 ausgestellt werden und die Attribute organizationName, givenName, surname, localityName und countryName enthalten.

(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.

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[14],
- einen Bindestrich („-“),
- Referenz, die gemäß dem identifizierten Registrierungsschema zugewiesen wurde.

(15) [TLS] 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[14],
- einen Bindestrich („-“),
- Referenz, die gemäß dem identifizierten Registrierungsschema zugewiesen wurde.

[13] Siehe CABF EV Guidelines #8.5
[14] ISO 3166 country codes,bei NTR ggf. auch zwei Zeichen für country sowie zwei Zeichen für state or province, getrennt durch ein “+”

(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[14],
- 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.

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[14].

organizationName

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

(22) [TLS] 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

Bzgl. der Kodierung des countryName für Länder, die nicht durch einen zweistelligen Countrycode repräsentiert werden, sei auf die ISO 3166-1 verwiesen.(24) [TLS] [EVCP] In Endteilnehmerzertifikaten MUSS das Attribut countryName gesetzt werden, wenn die Attribute surname und givenName oder organizationName gesetzt sind, ansonsten DARF es gesetzt werden.

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

7.1.5 Namensbeschränkungen

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

[TLS] [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 reason-Code 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:

- Es wird dem OCSP-Signer für die Lebensdauer des OCSP-Signer-Zertifikats vertraut. 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.
- ES wird eine Prüfmöglichkeit des OCSP-Signer-Zertifikats in den Erweiterungen cRLDistributionPoints und/oder authorityInfoAccess festgelegt.
- Es wird keine Methode zu Prüfung des Status des OCSP-Signers definiert und somit dem Prüfenden die Entscheidung überlassen, ob und wie er den Status des OCSP-Signer-Zertifikats prüft.

[TLS] [SMIME] 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.

[TLS] [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.

[TLS] Im gesamten Zeitraum, in dem Endteilnehmerzertifikate ausgestellt werden, MÜSSEN durch geeignete Selbstüberprüfungen die Einhaltung der Vorgaben dieser CP und der anwendbaren CPS sowie ihre Servicequalität kontrolliert werden. Diese Selbstüberprüfungen MÜSSEN mindestens vierteljährlich erfolgen und MÜSSEN stichprobenartig eine zufällige Auswahl von mindestens drei Prozent der Endteilnehmerzertifikate[15] umfassen, die seit der letzten Selbstüberprüfung ausgestellt wurden.

[EVCP] Selbstüberprüfungen MÜSSEN laufend durchgeführt werden.

8.1.2 Prüfungen durch externe Auditoren

Keine Vorgabe.

[TLS] [SMIME] Die TSP MÜSSEN in einer ununterbrochenen Folge von Audit-Perioden gemäß eines in Kap. 0 gelisteten 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 bzgl. der Bereitschaft zur Ausgabe von Zertifikaten in Übereinstimmung mit dem entsprechenden Auditschema geprüft werden („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.

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.

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

[EVCP] Die o.g. Anforderungen zu [TLS] [SMIME] gelten analog für [EVCP]. 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.

[TLS] Analog zur Selbstüberprüfung gemäß Kap. 8.1.1 MÜSSEN mindestens vierteljährlich Zertifikate geprüft werden, 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 MUSS ein Validierungsspezialist des TSP eingesetzt werden.

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

[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.

[TLS] [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. 0 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 MUSS die Prüfstelle gemäß ISO 17065 unter Anwendung der in ETSI EN 319 403 festgelegten Anforderungen durch die DAkkS (Deutsche Akkreditierungsstelle) 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.

[TLS] [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 EN 319 411-2 ab Version 2.2.2

[TLS] 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 oder
- NCP+.

Die Prüfungen MÜSSEN alle Roots und nicht beschränkte Sub-CAs sowie Cross-Zertifikate umfassen. In der Prüfdokumentation MÜSSEN alle geprüften PKI-Hierarchien dokumentiert werden.

[EVCP] 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.

[TLS] [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.

[TLS] [SMIME] Die Links zu den von den externen Prüfern erstellten und veröffentlichten Audit-Bescheinigungen aller technisch nicht beschränkten Root- und Sub-CAs MÜSSEN in der „Common CA Database“ (CCADB) veröffentlicht werden.

Diese Bescheinigungen SOLLTEN innerhalb von drei Monaten nach Ende der Prüfung veröffentlicht werden. Im Falle einer Verzögerung von mehr als drei Monaten MUSS ein von dem externen Prüfer unterzeichnetes Erläuterungsschreiben vorgelegt werden.

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

[EVCP] Die TSP MÜSSEN in Bezug auf ihre Leistungen und Verpflichtungen gemäß dieser CP über folgende Haftpflichtversicherung(en) verfügen:

- 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

Vertrauliche Geschäftsinformationen MÜSSEN ihrer Klassifizierung entsprechend angemessen geschützt werden.

9.4 Schutz von personenbezogenen Daten

9.4.1 Datenschutzkonzept

Die Vorgaben des Bundesdatenschutzgesetzes [BDSG] MÜSSEN beachtet werden, es DÜRFEN NICHT Daten erhoben werden, die zur Erbringung der Dienstleistung nicht relevant oder angemessen sind.

In den Datenschutzkonzepten MUSS beschrieben werden, wie die Vorgaben des [BDSG] bzgl. der im Registrierungsprozess erhobenen Daten umgesetzt werden. Zum Schutz der personenbezogenen Daten MÜSSEN 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 ergriffen werden.

9.4.2 Als privat zu behandelnde Informationen

Die die als privat zu behandelnden Informationen MÜSSEN in den CPS beschrieben werden.

9.4.3 Nicht als privat geltende Informationen

Die nicht als privat geltenden Informationen MÜSSEN in den CPS beschreiben.

9.4.4 Verantwortung für den Schutz privater Informationen

Die Verantwortung für den Schutz privater Informationen MUSS in den CPS beschrieben werden.

9.4.5 Benachrichtigung und Zustimmung zur Verwendung privater Informationen

Die Methoden zur Benachrichtigung der Betroffenen sowie die Einholung der Zustimmung zur Verwendung privater Informationen MÜSSEN in den CPS beschrieben werden.

9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

Die Bedingungen zur Offenlegung personenbezogener Daten im Rahmen von Gerichts- oder Verwaltungsverfahren MÜSSEN in den CPS beschrieben werden.

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, z.B. Anbieter von Vertrauensdienstkomponenten oder externen Registrierungsstellen, auslagern. Dazu MÜSSEN die Aufgaben der Dritten und die damit verbundenen Verfahrensweisen, Verantwortlichkeiten und Haftungsbedingungen festlegt werden und die Dritten MÜSSEN vertraglich verpflichtet werden, alle geforderten Maßnahmen umsetzen. Wenn von einem Anbieter bereitgestellte Vertrauensdienstkomponente verwendet werden, MUSS sichergestellt werden,

- dass die Verwendung der Schnittstelle der Komponente den vom Anbieter der Vertrauensdienstkomponente festgelegten Anforderungen entspricht,
- dass die von der Vertrauensdienstkomponente geforderte Sicherheit und Funktionalität den entsprechenden Anforderungen dieser CP und dem relevanten CPS entsprechen.

[3145] Wenn Dritte im Rahmen des Identifizierungs- und Registrierungsverfahrens Dienstleistungen für einen TSP erbringen, MÜSSEN diese das Sicherheitsniveau "hoch" und die Zuverlässigkeit sowie die Vertrauenswürdigkeit des eingesetzten Personals gewährleisten. Hierzu MUSS mit dem Dritten eine unterzeichnete Vereinbarung abgeschlossen werden, 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.

Dritten MUSS die Möglichkeit geboten werden, alle angebotenen Zertifikatstypen zu überprüfen und zu testen.

[TLS] Telekom Security als Betreiber der Root CAs ist verantwortlich für

- die Leistungen und Gewährleistungen der TSP,
- die Einhaltung dieser CP durch die TSP,
- alle Verbindlichkeiten und Freistellungsverpflichtungen der TSP gemäß [BR].

Für jedes ausgestellte Zertifikat MUSS sowohl den Endteilnehmern, den Anbietern der Anwendungssoftware, mit denen Telekom Security eine Vereinbarung zur Aufnahme der Root-Zertifikate in die Trusted Rootstores getroffen hat, als auch allen vertrauenden Dritten garantiert werden, dass

- der Endteilnehmer das Recht hat, die im Zertifikat (im Subject-DN und/oder subjectAltName) aufgeführten Domain Names 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 zur Einhaltung der vorgenannten Zertifikatsgarantien erforderlichen Prozesse und Maßnahmen MÜSSEN in den CPS beschrieben werden.

Zu allen Endteilnehmern SOLLTEN geeignete Kommunikationskanäle existieren, um diese im Bedarfsfall über Änderungen informieren zu können.

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

[EVCP] Für jedes ausgestellte EV-Zertifikat MUSS gewährleistet werden, dass

- über eine Gründungs- oder Registrierungsagentur in der Gründungs- oder Registrierungsgerichtsbarkeit des Endteilnehmers geprüft wurde, 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,
- alle zumutbaren Schritte unternommen wurden, um zu überprüfen, ob
  - der Endteilnehmer zum Zeitpunkt der Ausstellung des Zertifikats das Recht hat, alle im Zertifikat aufgeführten Domain Names zu verwenden,
  - der Endteilnehmer die Ausstellung des Zertifikats genehmigt hat,
  - alle anderen Informationen im Zertifikat zum Zeitpunkt der Ausstellung des Zertifikats korrekt waren,
- mit dem Endteilnehmer, sofern dieser nicht mit dem TSP verbunden ist, eine rechtsgültige und durchsetzbare Vereinbarung getroffen wurde, die alle Anforderungen aus [EVCG] berücksichtigt.

[QCP] Wenn private Schlüssel der Endteilnehmer während der Gültigkeitsdauer der korrespondierenden Zertifikate vom TSP verwaltet werden, SOLLTE dies in den CPS beschrieben werden. Darüber hinaus DARF diese Information auch im Zertifikat des Endteilnehmers aufgeführt werden.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Siehe Kap. 5.3.7, 6.5.1 und 9.6.1.

9.6.3 Zusicherungen und Gewährleistungen der Endteilnehmer

Die Nutzungsbedingungen für die Endteilnehmerzertifikate MÜSSEN festgelegt werden und es MUSS von den Endteilnehmern vor der Ausstellung der Zertifikate deren Akzeptanz bestätigt werden. 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 eines 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) [TLS] eine Verpflichtung, alle angemessenen Maßnahmen zu ergreifen, um die Vertraulichkeit und Kontrolle über die privaten Schlüssel und Aktivierungsdaten zu gewährleisten,
o) [TLS] eine Verpflichtung, den Inhalt des Zertifikats auf Richtigkeit zu überprüfen,
p) [TLS] eine Verpflichtung, das Zertifikat nur auf Servern zu installieren, auf die unter den im Zertifikatsattribut subjectAltName aufgeführten Namen zugegriffen werden kann,
q) [TLS] eine Verpflichtung, das Zertifikat ausschließlich in Übereinstimmung mit allen geltenden Gesetzen und in Übereinstimmung mit der abgeschlossenen Vereinbarung und den Nutzungsbedingungen zu nutzen,
r) [TLS] eine Verpflichtung, innerhalb eines bestimmten Zeitraums auf die Anweisungen des TSP bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauch zu reagieren,
s) [TLS] 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 0,
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

In den Nutzungsbedingungen (siehe dazu auch Kap. 9.6.3) und/oder den PDS MÜSSEN folgende Empfehlungen für vertrauende Dritte aufgenommen werden.

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 Haftung der TSP DARF im Einklang mit geltendem Recht beschränkt werden. Die Haftungsbeschränkungen MÜSSEN in den CPS sowie den Nutzungsbedingungen beschrieben werden, siehe dazu auch Kap. 9.6.3 Abs. ii).

[TLS] Für den Fall, dass die TSP Aufgaben an Dritte auslagern, DARF die Haftung vertraglich mit dem Dritten im Innenverhältnis entsprechend der Aufgaben aufgeteilt werden, im Außenverhältnis MUSS die Gesamtverantwortung entsprechend dieser CP und ihrer CPS jedoch beim TSP verbleiben.

[EVCP] Die Haftung der TSP DARF 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 beschränkt werden.

[QCP] 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.

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

9.12.1 Verfahren für Änderungen

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 Team unterzogen werden. Das Root-Team MUSS daher regelmäßig in angemessenen Abständen die zugrunde liegenden Anforderungen der in Anhang B referenzierten Dokumente auf neue Versionen überprüfen und die Aktivitäten in relevanten Foren verfolgen.

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.

Neue Versionen dieser CP MÜSSEN gemäß Kap. 1.5.4 genehmigt werden und eine neue aufsteigende Versionsnummer erhalten.

Analog MÜSSEN die CPS aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, mindestens aber einmal pro Jahr einem Review durch die Trusted Services unterzogen werden. Bzgl. der Änderungshistorie, Genehmigungsverfahren und Versionierung gilt das oben gesagte.

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Neue Versionen dieser CP MÜSSEN gemäß den Vorgaben aus Kap. 2.2 veröffentlicht werden. Spätestens mit der Veröffentlichung einer neuen Version MÜSSEN alle betroffenen Trusted Services informiert werden.

Neue Versionen eines CPS MÜSSEN gemäß den Vorgaben aus Kap. 2.2 veröffentlicht werden. Wenn Änderungen an einem CPS vorgenommen wurden, die sich auf die Akzeptanz des Dienstes durch die Zertifikatsnehmer oder die Zertifikatsnutzer auswirken könnten, so MUSS die Änderungen rechtzeitig den Zertifikatsnehmern, den Zertifikatsnutzern und, sofern anwendbar, Bewertungsstellen und Aufsichts- oder andere Regulierungsbehörden bekannt gegeben werden, siehe dazu auch Kap. 9.6.1 und 9.6.3. Bei Bekanntgabe der Änderungen DARF bzgl. der Details auf geänderte Dokumente im Repository verweisen werden.

9.12.3 Umstände, unter denen der OID geändert werden muss

Wenn sich an dieser CP oder an einer CPS Änderungen ergeben, welche sich auf die Anwendbarkeit des jeweiligen Dokuments auswirken, so SOLLTE das Dokument eine neue OID bekommen.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Die Richtlinien und Verfahren zur Beilegung von Beschwerden und Streitigkeiten, die von den Endteilnehmern oder vertrauenden Dritten zu den bereitgestellten Diensten eingehen, MÜSSEN festgelegt und in den CPS sowie den Nutzungsbedingungen (Siehe Kap. 9.6.3 Abs. kk)) beschrieben werden.

9.14 Geltendes Recht

In den CPS MUSS das deutsche Recht als geltendes Recht festgelegt werden.

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.

[TLS] Im Falle eines Konflikts zwischen [BR] und einem Gesetz DARF eine widersprüchliche Anforderung so weit modifiziert werden, 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 in Kap. 9.16.3 des betroffenen CPS ein detaillierter Verweis auf das Gesetz, das eine Änderung dieser Anforderungen gemäß diesem Abschnitt erfordert, sowie die durchgeführte spezifische Änderung dieser Anforderungen aufgenommen werden. Vor der Ausstellung eines Zertifikats gemäß der geänderten Anforderung MUSS das CA/Browser Forum über die relevanten Passagen des geänderten Kapitels informiert werden (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

ANHANG

Anhang A: Abkürzungen

Hinweis: Aufgrund der internationalen Standardisierung verbergen sich hinter den Abkürzungen meist englische Fachbegriffe, auf deren Übersetzung in die deutsche Sprache an dieser Stelle verzichtet wird.

Tabelle 4 - Abkürzungen

Abkürzung	Bedeutung
AATL	Adobe Approved Trust List
ADN	Authorization Domain Name
ARL	Authority Revocation List (siehe CARL)
ASN.1	Abstract Syntax Notation One
BR	Baseline Requirements
CA	Certification Authority
CAA	Certification Authority Authorization
CAB Forum	CA/Browser Forum
CARL	Certification Authority Revocation List
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DAkkS	Deutsche Akkreditierungsstelle (German Accreditation Body)
DBA	Doing Business As
DNS	Domain Name System
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification, Authentication and trust Services
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
gTLD	Generic Top-Level Domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers

IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunications Union
IVCP	Individual Validation Certificate Policy
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
MGF	Mask Generation Function
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
QCP	Qualified Certificate Policy
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person
QEVCP-w	Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG (formerly QCP-w)
QNCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person based on the BRG
QSCD	Qualified electronic Signature/Seal Creation Device [eIDAS#AnnexII]
QTSP	Qualified TSP
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman (public-key cryptosystem, described by Ron Rivest, Adi Shamir and Leonard Adleman)
RSASSA	RSA Signature Scheme with Appendix
RSASSA-PSS	improved Probabilistic RSA Signature Scheme
SCT	Signed Certificate Timestamp
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SOG-IS	Senior Officials Group Information Systems Security
SSL	Secure Socket Layer
SÜG	Sicherheitsüberprüfungsgesetz
TLS	Transport Layer Security

TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VDG	Vertrauensdienstegesetz
VDV	Vertrauensdiensteverordnung
VSA	Verschlusssachenanweisung
VS-NfD	Verschlussache - Nur für den Dienstgebrauch

Anhang B: Referenzen

Tabelle 5 - Referenzen

[ADTL]	Adobe Approved Trust-List Tech. Requirements
[APRP]	Apple Root Certificate Programm
[APCT]	Apple's Certificate Transparency policy
[BR]	CAB-Forum Baseline Requirements
[CCADB]	CCADB Policy
[CPS_Root]	Telekom Security CPS Root
[eIDAS]	eIDAS (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates)
[ETS401]	ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETS411-1]	ETSI EN 319-411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETS411-2]	ETSI EN 319-411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETS412-1]	ETSI EN 319-412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETS412-2]	ETSI EN 319-412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETS412-3]	ETSI EN 319-412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETS412-4]	ETSI EN 319-412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[ETS412-5]	ETSI EN 319-412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETS312]	ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETS431-1]	ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
[ETS461]	ETSI TS 119 461: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
[RFC5753]	RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)

[RFC3279]	RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC3647]	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC5280]	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC6960]	RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[RFC6962]	RFC 6962 Certificate Transparency
[RFC4055]	RFC 4055 Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC5756]	RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters
[RFC4491]	RFC 4491 Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[RFC5480]	RFC 5480 Elliptic Curve Cryptography Subject Public Key Information, March 2009
[RFC5758]	RFC 5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, January 2010
[RFC8692]	RFC 8692 Internet X.509 Public Key Infrastructure: Additional Algorithm Identifiers for RSASSA-PSS and ECDSA Using SHAKEs, December 2019
[RFC8813]	RFC 8813 Clarifications for Elliptic Curve Cryptography Subject Public Key Information
[RFC5019]	RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
[RFC8823]	RFC 8823 Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates
[EVCG]	CAB-Forum Extended Validation Certificate Guidelines
[GCTP]	google chrome Certicate Transparency Policy
[GCRP]	Chromium Root Certificate Policy
[GGS]	Google G-Suite SMIME Zertifikatsprofil
[GCTL]	google Certificate Transparency Log Policy
[MSRP]	Microsoft Trusted Root Program inkl. - Security Incident Response Requirements - Audit Requirements -Testing Instruction - New CA application
[MOZRP]	Mozilla Root Store Policy
[MOZCA]	Mozilla CA/Application Process
[NSG]	CAB-Forum Network Security Guidelines
[SÜG]	Sicherheitsüberprüfungsgesetz
[TR3145]	Technische Richtlinie TR-03145-1, Secure CA operation, Part 1, Bundesamt für die Sicherheit in der Informationstechnik
[TR3145VS]	Technische Richtlinie TR-03145-VS-NfD, Secure CA operation, VS-NfD, Bundesamt für die Sicherheit in der Informationstechnik
[VDG]	Vertrauensdienstegesetz
[VDV]	Vertrauensdiensteverordnung
[VSA]	Verschlusssachenanweisung des Bundes
[X500]	ITU-T X.500 Serie / ISO/IEC 9594 Serie Information technology - Open systems interconnection - The Directory

Anhang C: Definitionen

Hinweis: Es wird an dieser Stelle darauf verzichtet, bekannte Definitionen international etablierter Begriffe im PKI-Umfeld erneut aufzuführen, diesbezüglich sei auf die Definitionen der in Anhang B aufgeführten ETSI-Spezifikationen und RFCs verwiesen. Nachfolgend werden zum einen Begriffe definiert, die spezifisch für bestimmte Zertifikatstypen verwendet werden und zum anderen werden einige in diesem Dokument verwendete Begriffe klargestellt, deren Verwendung sich ggf. zwischen der deutschen und der englischen Sprache unterscheidet.

Tabelle 6 - Definitionen

Begriff	Bedeutung
Antragsteller	Natürliche oder juristische Person, die für sich selbst oder einen anderen *Zertifikatsnehmer* ein Zertifikat beantragt.
Ausstellendes System	System zum Signieren von Zertifikaten oder Zertifikatsstatusinformationen
Business Entity	[EVCP] Alle Zertifikatsnehmer von EV-Zertifikaten, die nicht in die Kategorien ▪ *Private Organization*, ▪ *Government Entity* oder ▪ *Non-Commercial Entity* fallen, z.B. offene Handelsgesellschaften, Vereinigungen ohne eigene Rechtspersönlichkeit, Einzelunternehmen, etc.
Certification Authority Authorization (CAA)	[TLS] DNS-Ressourceneintrag, der es dem Inhaber eines DNS-Domänen Namens ermöglicht, die TSP anzugeben, die berechtigt sind, Zertifikate für diese Domäne auszustellen
Endteilnehmer	Siehe *Zertifikatsnehmer*
Fortgeschrittene elektronische Signatur	Elektronische Signatur nach [eIDAS#Art.26]
Fortgeschrittenes elektronisches Siegel	Elektronisches Siegel nach [eIDAS#Art.36]
Geprüfte Kommunikationsmethode	[EVCP] Die Verwendung einer Telefonnummer, einer Faxnummer, einer E-Mail-Adresse oder einer Postanschrift, die von einem TSP als zuverlässiger Weg der Kommunikation mit dem Antragsteller gemäß [EVCG# 11.5] bestätigt wurde
Government Entity	[EVCP] Eine von einer Regierung betriebene juristische Person, Behörde, Abteilung oder andere damit verbundene Organisationseinheiten
High-Risk-Zertifikatsanträge	[TLS] Zertifikatsanträge welche die TSP anhand interner Kriterien für eine zusätzliche Prüfung kennzeichnen. Dazu können gehören: ▪ Namen, bei denen ein höheres Risiko für Phishing oder andere betrügerische Nutzung besteht, ▪ Namen, die in zuvor abgelehnten Zertifikatsanträgen oder widerrufenen Zertifikaten enthalten sind, ▪ Namen, die auf der Miller Smiles Phishing-Liste oder der Google Safe Browsing-Liste aufgeführt sind, oder ▪ Namen, die ein TSP anhand ihrer eigenen Kriterien zur Risikominderung identifiziert

Hochsicherheitszone	Ein spezifischer physischer Standort der Sicherheitszone des TSP oder eines beauftragten Dritten, an dem sich die privaten Schlüssel oder die kryptografische Hardware befindet
Kurzzeitzertifikat	Zertifikat, dessen Gültigkeitsdauer kürzer ist als die im CPS angegebene maximale Bearbeitungszeit für einen Sperrantrag
Leaf Zertifikat	[TLS] Ein TLS-Zertifikat, dass zuvor als *Pre-Zertifikat* veröffentlicht wurde
Non-Reserved LDH-Label	[TLS] Komponente eines Domain Namens, die kein '-' an der dritten und vierten Position hat
Non-commercial entity	[EVCP] Eine internationale Organisation, die im Rahmen einer Charta, eines Abkommens, einer Konvention oder einem gleichwertigen Instrument geschaffen wurde, das von oder im Namen von mehr als einer Regierung eines Landes unterzeichnet wurde
P-Label	[TLS] Komponente eines Domain Namens, die ein '-' an der dritten und vierten Position hat („XN-Label“) und auf die ab der fünften Position eine gültige Ausgabe des Punycode-Algorithmus gemäß [RFC3492# 6.3] folgt
Pre-Zertifikat	[TLS] Zertifikat gemäß [RFC6962] zur öffentlichen Protokollierung eines noch auszustellenden TLS-Zertifikats. Das Pre-Zertifikat wird aus dem noch auszustellenden Zertifikat zzgl. der speziellen kritischen Erweiterung „Certificate Transparency precertificate poison extension“ (OID 1.3.6.1.4.1.11129.2.4.3) erzeugt. Pre-Zertifikate gelten nicht als Zertifikat gemäß [RFC5280] und können von Standard-X.509v3-Clients nicht validiert werden. Das später aus dem Pre-Zertifikat erzeugte (echte) TLS-Zertifikat wird als *Leaf-Zertifikat* bezeichnet.
Private Organization	[EVCP] Eine nichtstaatliche juristische Person, deren Existenz durch eine Anmeldung bei (oder einen Akt) der Gründungsbehörde oder einer gleichwertigen Stelle in ihrem Gründungsland begründet wurde
Pseudonym	Fiktive Identität, die eine Person zu einem bestimmten Zweck annimmt und die sich von ihrer ursprünglichen oder wahren Identität unterscheidet. HINWEIS: Eine pseudonyme Identität kann, im Gegensatz zu einer anonymen Identität, mit der wahren Identität der Person verknüpft werden. Die wahre Identität ist dem TSP bekannt.
Sichere Zone	Logischer oder physischer Bereich, der durch Maßnahmen geschützt ist, welche die Vertraulichkeit, Integrität und Verfügbarkeit der vom TSP genutzten Systeme angemessen schützen.
Sicherheitsunterstützungssystem	System, das zur Bereitstellung von Sicherheitsfunktionen verwendet wird, zu denen z.B. Authentifizierung, Kontrolle der Netzwerkgrenzen, Audit-Protokollierung, Schwachstellen-Scans oder Intrusion Detection gehören können
Subjekt eines Zertifikats	Entität, die in einem Zertifikat als Inhaber des privaten Schlüssels identifiziert wird, der mit dem im Zertifikat angegebenen öffentlichen Schlüssel verbunden ist. Subjekte können natürliche oder juristische Personen oder auch mit diesen in Verbindung stehende organisatorische Einheiten oder auch Prozesse, Funktionen oder Geräte sein, die in deren Namen betrieben werden. Das Subjekt eines Zertifikats kann auch gleichzeitig, muss aber nicht, der *Zertifikatsnehmer* und/oder der *Antragsteller* sein
Technisch beschränkte CA	[TLS] Eine Sub-CA, bei der eine Kombination aus Werten in den Erweiterungen extendedKeyUsage und nameConstraints verwendet wird, um den Bereich zu begrenzen, in dem diese Sub-

	CA Endteilnehmer- oder weitere Sub-CA-Zertifikate ausstellen darf
Token	Hardware-Modul, das kryptografische Schlüssel auf sichere Weise erzeugt und/oder handhabt
Validierungsspezialist	[TLS] Mitarbeiter eines TSP oder einer RA, der die in [BR] genannten Aufgaben der Informationsüberprüfung wahrnimmt
Verschlussache - Nur für den Dienstgebrauch	[3145] Klassifizierung von zu schützenden staatlichen Informationen
Vertragsunterzeichner	[EVCP] Eine natürliche Person, die ausdrücklich befugt ist, den Zertifikatsnehmer zu vertreten und in dessen Namen Zertifikatsanträge zu unterzeichnen.
Wildcard Zertifikat	[TLS] Ein Zertifikat mit einem *Wildcard Domain Namen*
Wildcard Domain Name	[TLS] Ein Domain Name, bestehend aus einem einzelnen Sternchen, gefolgt von einem einzelnen Punkt ("*."), gefolgt von einem voll qualifizierten Domänennamen
Zertifikatsanforderer	[EVCP] Eine natürliche Person, die ausdrücklich befugt ist, den *Zertifikatsnehmer* zu vertreten, um einen Zertifikatsantrag im Namen des Zertifikatsnehmers auszufüllen und einzureichen
Zertifikatsgenehmiger	[EVCP] Eine natürliche Person, die ausdrücklich befugt ist, den *Zertifikatsnehmer* zu vertreten, um ▪ selbst als *Zertifikatsanforderer* zu handeln, ▪ andere Mitarbeiter des *Zertifikatsnehmers* oder Dritte zu ermächtigen, als *Zertifikatsanforderer* zu handeln, ▪ von anderen *Zertifikatsanforderern* eingereichte Zertifikatsanträge zu genehmigen.
Zertifikatsmanagement-System	Ein System, das von einem TSP oder einem beauftragten Dritten verwendet wird, um die Ausstellung von Zertifikaten oder Zertifikatsstatusinformationen zu verarbeiten, zu genehmigen oder zu speichern, einschließlich Datenbank, Datenbankserver und Speicher
Zertifikatsnehmer (*Endteilnehmer*)	Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die durch Nutzungsbedingungen oder einen Vertrag mit einem TSP rechtlich gebunden ist. Ein Zertifikatsnehmer kann auch gleichzeitig, muss aber nicht das *Subjekt eines Zertifikats* und/oder der *Antragsteller* sein
Zertifikatsnutzer	Natürliche oder juristische Personen, die im Vertrauen auf die Zertifikate handeln, d.h. z.B. mittels der Zertifikate elektronische Signaturen verifizieren, Personen oder Geräte authentifizieren oder Daten verschlüsseln. In diesem Dokument werden die Begriffe „Zertifikatsnutzer“ und "vertrauende Dritte" austauschbar verwendet.
Zuverlässige Methode der Kommunikation	[TLS] [SMIME] Eine Kommunikationsmethode, die anhand einer anderen Quelle als dem Vertreter des Antragstellers überprüft wurde (z. B. Anschrift, Telefonnummer oder E-Mail-Adresse)