Deutsche Telekom Security GmbH

Certification Practice Statement V-PKI-CAs

Version: 04.00

Gültig ab: 13.01.2025

Status: Final

Letzter Review: 09.01.2025

ÄNDERUNGSHISTORIE

Version	Stand	Bearbeiter	Änderungen / Kommentar
01.00	21.10.2022	Telekom Security	Initialversion zur TR-03145-Umsetzung der V-PKI-CAs
02.00	21.10.2023	Telekom Security	Jährliche Revision
03.00	21.10.2024	Telekom Security	Jährliche Revision
04.00	09.01.2025	Telekom Security	Anpassung in Kap. 1.4.1 (Anwendungsbereiche - nicht eingestuft/VS-NfD)

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 Überblick

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

Hierzu zählen auch die in die „Verwaltungs-PKI“ (V-PKI) des Bundes integrierten „Deutschland Online Infrastruktur-Certification Authority“ (DOI-CA) und „Informationsverbund Berlin Bonn-Certification Authority“ (IVBB-CA), welche die Telekom Security im Auftrag des „Netze des Bundes – Verbindungsnetz“ (NdB-VN) bzw. „Netze des Bundes“ (NdB) betreibt.

Bei dem vorliegenden Dokument handelt es sich um das Certification Practice Statement (CPS) des Trust Centers der Telekom Security zu der DOI- und IVBB-CA (nachfolgend V-PKI-CAs genannt). Es beschreibt in der Struktur des [RFC3647] die Einhaltung und die Umsetzung der Anforderungen aus:

- der Telekom Security Certificate Policy [TSCP] mit der OID 1.3.6.1.4.1.7879.13.42,
- der Certificate Policy der Wurzelzertifizierungsstelle (Root-CA) der PKI-1-Verwaltung [VPKICP] mit der OID 1.3.6.1.4.1.7924.1.1 sowie
- der Technischen Richtlinie TR-03145-1 [TR3145] vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

in der jeweils zum Zeitpunkt der Erstellung einer neuen Version dieses Dokuments gültigen Version.

Im Falle eines Widerspruchs zwischen dieser CPS und den oben referenzierten Quellen haben die Regelungen aus den referenzierten Quellen Vorrang.

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument trägt den Namen „Telekom Security CPS V-PKI-CAs“ und wird durch die OID 1.3.6.1.4.1.7879.13.44 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) Telekom Security CPS V-PKI-CAs (44)}

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CAs)

Die Zertifizierungshierarchie der V-PKI-CAs ist zweistufig aufgebaut:

- Die „PCA-1-Verwaltung“ stellt als Root-CA die Sub-CA-Zertifikate der V-PKI-CAs aus.
- Die V-PKI-CAs stellen die Zertifikate der Endteilnehmer (nachfolgend Zertifikatsnehmer genannt)[1] aus.

Da die PCA-1-Verwaltung durch das BSI betrieben wird, liegen die Root-CA-Zertifikate nicht im Geltungsbereich dieser CPS, sondern der [VPKICP].

Im Geltungsbereich dieser CPS liegen alle von der Telekom Security betriebenen V-PKI-CAs, die unter https://x500.bund.de im Bereich „Service-Zertifikate“ unter „aktive Zertifikate“ veröffentlicht sind, d.h. alle

- DOI CA *<nn> sowie*
- CA IVBB Deutsche Telekom AG *<nn>*.

Es gibt keine Cross-Zertifizierung von/zu den o.g. V-PKI-CAs.

1.3.2 Registrierungsstellen (Registration Authorities, RAs)

Die Registrierung der Zertifikatsnehmer kann sowohl durch die interne RA des Trust Centers als auch durch externe RAs erfolgen.

Da die V-PKI-CAs von verschiedenen Bundes-, Landes- und Kommunalverwaltungen sowie übergreifenden Verwaltungsanwendungen genutzt werden, sind sie in zweistufig gegliederte Zuständigkeitsbereiche („Master- und Sub-Domänen“) unterteilt, innerhalb derer die Registrierungsprozesse für die Zertifikatsnehmer dieses Bereichs ablaufen. D.h. eine Registrierungsstelle für eine bestimmte Domäne kann auch nur Zertifikatsnehmer dieser Domäne registrieren und deren Anträge auf Ausstellung oder Sperrung genehmigen oder ablehnen.

Eine Liste der Registrierungsstellen wird auf Anfrage (Kontakt siehe Kap. 1.5.2) bereitgestellt.

[1] Der Begriff „Endteilnehmer-Zertifikate“ wird weiterhin zur Abgrenzung gegenüber CA-Zertifikaten verwendet.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind alle natürlichen Personen oder Organisationen, welche Zertifikate der V-PKI-CAs beziehen. Grundsätzlich sollten diese aus den öffentlichen Institutionen des Bundes, der Bundesländer und der kommunalen Behörden stammen. Unternehmen und Personen, die in einer engen Beziehung mit einer der o.g. Institutionen stehen, können für die Kommunikation mit den oben genannten Teilnehmern ebenfalls Zertifikate der V-PKI-CAs erhalten[2].

Subjekte der Zertifikate sind:

- natürliche Personen (auch pseudonymisiert)
- Organisationen
- Gruppen bzw. Funktionen,
- IT-Prozesse

Antragsteller sind entweder die natürlichen Personen, welche Zertifikate für sich selbst oder im Auftrag einer Organisation beantragen oder die „Schlüsselverantwortlichen“, welche Zertifikate für Gruppen, Funktionen und IT-Prozesse beantragen.

Bei Gruppen-/Funktionszertifikaten gibt es darüber hinaus noch folgende (optionale) Rollen:

- Als ***Schlüsselinhaber*** werden alle natürlichen Personen bezeichnet, welche zusätzlich zum Schlüsselverantwortlichen Zugriff auf die privaten Schlüssel von Gruppen/Funktionen haben. Die Anzahl der Schlüsselinhaber darf die maximale Anzahl von 30 Personen nicht überschreiten.
- Als ***Sperrberechtigte*** werden alle natürlichen Personen bezeichnet, welche zusätzlich zum Schlüsselverantwortlichen Zugriff auf das Sperrkennwort eines Gruppen-/Funktionszertifikats haben und somit eine Sperrung des Zertifikats veranlassen können.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind Personen, Systeme oder IT-Prozesse, welche den Zertifikaten der V-PKI-CAs vertrauen („vertrauende Dritte“).

1.3.5 Andere Teilnehmer

Keine Bestimmungen.

[2] weitere Regelungen siehe [VPKICP]

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

CA-Zertifikate werden ausschließlich zur Signatur von OCSP-Signer- und Endteilnehmer-Zertifikaten sowie Sperrlisten verwendet.

Endteilnehmer-Zertifikate dürfen für folgende Anwendungen genutzt werden:

- Einfache und fortgeschrittene elektronische Signatur, unter Beachtung folgender Voraussetzungen:
  - Eine fortgeschrittene Signatur ist nur mit einem Zertifikat möglich, das als keyUsage ausschließlich „nonRepudiation“ verwendet.
  - Eine fortgeschrittene Signatur kann nur durch eine natürliche Person erzeugt werden, d.h. eine Erzeugung von fortgeschrittenen Signaturen ist nicht mit Gruppen- oder Funktionszertifikaten möglich.
  - Der Schlüssel zur Erzeugung der Signatur muss in der alleinigen Kontrolle des Teilnehmers sein.
- Authentisierung.
- Verschlüsselung von Daten bis zur Vertrauensstufe des jeweiligen Zertifikats. Für VS-NfD müssen folgende PolicyOIDs gesetzt sein:
  - 0.4.0.127.0.7.3.6.1.1.3.4 (IVBB-CA)
  - 0.4.0.127.0.7.3.6.1.1.5.4 (DOI-CA)

Die Anwendung muss den in den Zertifikaten eingetragenen Schlüsselverwendungen in den Attributen „keyUsage“ und „extendedKeyUsage“ genügen

1.4.2 Unzulässige Verwendung von Zertifikaten

Die Zertifikate dürfen nicht für andere als in Kap. 1.4.1 angegebenen Zwecke verwendet werden.

1.5 Verwaltung des Dokuments

1.5.1 Verwaltende Organisation dieses Dokuments

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

1.5.2 Ansprechpartner

Ansprechpartner für dieses CPS ist das Trust Center der Telekom Security:

- E-Mail: trust_center_notary@telekom.de,
- Internet: https://www.telesec.de/de/service/kontakt/anfragemitteilung.

1.5.3 Instanz für die Feststellung der Konformität dieser CPS

Zuständig für die Feststellung der Konformität dieser CPS zu [TSCP] und [VPKICP] ist das Compliance-Management des Trust Centers, welches wie folgt erreichbar ist:

- E-Mail: trustcenter-roots@telekom.de.

Darüber hinaus wird die Konformität dieser CPS zu [TR3145] im Rahmen der regelmäßigen Audits durch externe Auditoren (siehe Kap. 8) geprüft.

1.5.4 Genehmigungsverfahren dieses CPS

Jede Version dieses CPS wird nach Feststellung der Konformität gemäß Kap. 1.5.3 von der Leitung des Trust Centers freigegeben.

1.6 Definitionen und Abkürzungen

Siehe [TSCP].

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

Telekom Security betreibt ein Repository mit Informationen und Dokumenten (siehe Kap. 2.2) sowie Zertifikatsstatusdienste für beide V-PKI-CAs in Form von Sperrlisten und OCSP-Auskünften (siehe Kap. 4.9 bzw. 4.10).

Die Verzeichnisdienste zur Veröffentlichung der Zertifikate und Sperrlisten der beiden V-PKI-CAs unterscheiden sich wie folgt:

- **DOI-CA**: Als Verzeichnisdienst zur Veröffentlichung wird der „zentrale Verzeichnisdienst der Verwaltungen“ verwendet, welcher von der Telekom Security im Auftrag der „Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben“ (BDBOS) betrieben wird. Dieser Verzeichnisdienst beinhaltet ein internes Verzeichnis („Verzeichnisdienst der Verwaltungen“, VDV) im NdB-VN auf das alle an das Verbindungsnetz angeschlossenen Verwaltungen Zugriff haben, sowie ein externes Verzeichnis („Veröffentlichungsdienst“, VöD), welches im Internet zur Verfügung gestellt wird. Die Zertifikate und Sperrlisten werden wie folgt in den Verzeichnissen veröffentlicht:
  - CA-Zertifikate und Sperrlisten werden sowohl im VDV als auch im VöD veröffentlicht. Darüber hinaus werden CA-Zertifikate und Sperrlisten auch im X.500-Verzeichnis des NdB veröffentlicht.
  - Endteilnehmer-Zertifikate werden, mit Ausnahme der Zertifikate für IT-Prozesse und RA-Mitarbeiter grundsätzlich im VDV veröffentlicht. Bei Antragstellung kann für jedes Zertifikat festgelegt werden, ob es darüber hinaus im VöD veröffentlicht wird.
- **IVBB-CA**: Als Verzeichnisdienst zur Veröffentlichung wird das X.500-Verzeichnis des NdB verwendet. Dieser Verzeichnisdienst beinhaltet ein internes Verzeichnis im NdB, auf das alle am NdB angeschlossenen Verwaltungen Zugriff haben, sowie ein externes Verzeichnis, welches im Internet zur Verfügung gestellt wird. Die Zertifikate und Sperrlisten werden wie folgt in den Verzeichnissen veröffentlicht:
  - CA-Zertifikate und Sperrlisten werden sowohl im internen als auch im externen X.500-Verzeichnis des NdB veröffentlicht.
  - Teilnehmer-Zertifikate werden von der CA ausschließlich im internen X.500-Verzeichnis des NdB veröffentlicht.

Anmerkung: Sofern ein Teilnehmer die externe Veröffentlichung seines X.500-Verzeichniseintrags wünscht, wird der Eintrag inkl. der Zertifikate in das externe X.500-Verzeichnis des NdB übertragen. Dies geschieht jedoch unabhängig von der Zertifikatsbeantragung bzw. -ausstellung über interne Mechanismen des X.500 und liegt damit nicht im Geltungsbereich dieser CPS.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Telekom Security veröffentlicht im PKI-Repository des Trust Centers (https://www.telesec.de/de/service/downloads/pki-repository/) folgende Informationen und Dokumente (aktuelle als auch abgelöste Versionen):

- Telekom Security CP [TSCP],
- Certification Practice Statements (CPS, beinhaltet dieses Dokument),
- alle im Geltungsbereich der CPS befindlichen CAs,
- Nutzungsbedingungen und
- Selbsterklärung der Telekom Security zur Teilnahme an der V-PKI.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Neue Versionen der [TSCP] und dieser CPS werden mindestens jährlich sowie zusätzlich bei Bedarf im o.g. Repository vor Inkrafttreten veröffentlicht.

Neue Versionen der Nutzungsbedingungen werden vor Inkrafttreten im o.g. Repository veröffentlicht.

Neue CA-Zertifikate im Geltungsbereich dieses CPS werden vor Inbetriebnahme im Repository veröffentlicht.

2.4 Zugang zu den Verzeichnissen

Die in Kap. 2.1 aufgeführten Verzeichnisse sind aus den dort aufgeführten Netzen ohne Zugriffsbeschränkungen für lesenden Zugriff per LDAPv3 erreichbar.

Die in Kap. 2.2 aufgeführten Informationen sind öffentlich für den lesenden Zugriff ohne Zugriffsbeschränkung erreichbar.

Die Verfügbarkeit und Integrität der bereitgestellten Informationen werden durch entsprechende technische Maßnahmen sichergestellt.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

3.1.1 Namensformen

Es werden in allen Zertifikaten die Namen der Subjekte in Form eines „Distinguished Names“ gemäß [X500] („Subject-DN“) aufgenommen.

Darüber hinaus enthalten die Endteilnehmer-Zertifikate immer einen subjectAltName.

Siehe Kap. 7.1.4 für Details.

3.1.2 Aussagekraft von Namen

Pseudonymisierte Personen-Zertifikate werden durch das Suffix „:PN“ im „commonName“ gekennzeichnet.

Zertifikate für Gruppen bzw. Funktionen werden durch das Präfix „FKT:“[3] im „commonName“ gekennzeichnet.

Zertifikate für externe Mitarbeiter von Organisationen werden durch das Suffix „Ext.“ im „commonName“ gekennzeichnet.

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

Die in Gruppen- oder Funktionszertifikaten verwendeten Namen müssen aussagekräftig sein, d.h. die Gruppe oder Funktion muss eindeutig erkennbar sein. Die Entscheidung über die Aussagekraft trifft die RA, welche ggf. den beantragten Namen in Abstimmung mit dem Antragsteller abändern oder den Antrag ablehnen kann.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Eine Verwechslung mit existierenden Namen natürlicher Personen oder Organisationen muss ausgeschlossen werden.

Die wahre Identität einer pseudonymisierten Identität ist der zuständigen RA sowie der Telekom Security als CA bekannt.

[3] bisher wurde hierfür der Präfix „GRP:“ verwendet, zukünftig sollte auf „FKT:“ geschwenkt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

Ein Subject-DN ist in der Zuordnung zu den Zertifikatsnehmern aufgrund der einem Zertifikatsnehmer zugeordneten „serialNumber“ eindeutig, wird also nicht an unterschiedliche Zertifikatsnehmer vergeben. Ein Zertifikatsnehmer kann jedoch mehrere Zertifikate mit gleichem Subject-DN haben.

CA-übergreifend wird die Eindeutigkeit des Subject-DN innerhalb der V-PKI durch die Reservierung der Namensräume für das Attribut „organization“ und ggf. „organizationalUnit“ durch die einzelnen CA-Betreiber bei der Root-CA sichergestellt.

Eine Liste der von Telekom Security reservierten Namensräume wird auf Anfrage bereitgestellt (Kontakte siehe Kap. 1.5.2).

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Keine Bestimmungen.

3.2 Initiale Validierung der Identität

Zur initialen Validierung der Identität einer natürlichen Person oder einer Organisation werden ausschließlich direkte Nachweise (z.B. amtliche Ausweise) oder Bescheinigungen von autorisierten Quellen (z.B. Bestätigung mittels Dienstsiegel, Handelsregisterauszug) verwendet.

Bescheinigungen können dabei in Papierform oder elektronisch mit fortgeschrittener oder qualifizierter Signatur eingereicht werden.

Es werden nur solche Nachweise angefordert, welche für die Identifizierung notwendig sind.

Die Authentizität bereitgestellter Nachweise wird, soweit möglich, auf Änderungen und Fälschungen hin geprüft.

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Bei Generierung der Schlüssel durch den Zertifikatsnehmer erfolgt der Besitznachweis mittels eines mit dem privaten Schlüssel signierten PKCS#10-Requests.

3.2.2 Authentifizierung der Identität von Organisationen

Es werden die nachfolgenden Methoden zur Validierung einer Organisationsidentität verwendet:

- die Existenz und Identität einer staatlichen Organisation (als Zertifikatsnehmer oder Domäneninhaber oder Registrierungsstelle) werden mittels einer mit einem Dienstsiegel versehenen Bescheinigung der Organisation selbst oder einer ihr übergeordneten Organisation verifiziert,
- die Existenz und Identität einer privaten Organisation werden über staatlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert („Qualified Government Information Source“, QGIS, z.B. Handelsregister). Ergänzend dazu wird der Antragsteller gemäß einer in Kap. 3.2.3 aufgeführten Methode persönlich identifiziert. Falls es sich bei dem Antragsteller nicht um einen direkt Vertretungsberechtigten der Organisation handelt, wird darüber hinaus dessen Bevollmächtigung gemäß Kap. 3.2.5 geprüft.

3.2.3 Authentifizierung der Identität natürlicher Personen

Die Identität einer natürlichen Person als Antragsteller oder Vertreter einer Organisation wird mittels einer der folgenden Methoden geprüft:

- Persönliche Identifizierung unter Vorlage eines amtlichen Ausweises durch:
  - einen Mitarbeiter der zuständigen Registrierungsstelle oder
  - einen Mitarbeiter in einer siegelführenden Stelle einer Behörde oder
  - einen Mitarbeiter oder berechtigten Vertreter der Zertifizierungsstelle,
- PostIdent-Verfahren,
- sonstige nach [eIDAS#24] zugelassene Identifizierungsverfahren.

3.2.4 Nicht überprüfte Informationen

Es werden ausschließlich geprüfte Informationen in ein Zertifikat aufgenommen.

3.2.5 Validierung der Bevollmächtigung

Zum Nachweis einer Vertretungsberechtigung werden ausschließlich rechtsgültig unterschriebene Vollmachten akzeptiert.

3.2.6 Kriterien für Interoperabilität

Keine Bestimmungen.

3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerungen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Zertifikatserneuerungen

Eine erneute Identifizierung im Rahmen von Zertifikatserneuerungen erfolgt spätestens 10 Jahre nach einer erfolgreichen Identifizierung gemäß Kap. 3.2.

Die Authentifizierung des Antragstellers erfolgt über die Referenznummer und das Sperrkennwort des zu erneuernden Zertifikats.

3.3.2 Identifizierung und Authentifizierung für Zertifikatserneuerungen nach einer Sperrung

Eine Erneuerung gesperrter Zertifikate wird nicht angeboten.

3.4 Identifizierung und Authentifizierung bei Sperranträgen

Die Identifizierung und Authentifizierung eines Zertifikatsnehmers bei einem Sperrantrag erfolgt

- über die Referenznummer und das Sperrkennwort des zu sperrenden Zertifikats oder
- durch eine persönliche Identifizierung des Zertifikatsnehmers oder des Schlüsselverantwortlichen unter Vorlage eines amtlichen Ausweises durch
  - einen Mitarbeiter der zuständigen Registrierungsstelle oder
  - einen Mitarbeiter oder berechtigten Vertreter der Zertifizierungsstelle.

Die Identifizierung und Authentifizierung einer RA im Rahmen einer Sperrung eines Endteilnehmer-Zertifikats erfolgt durch die zertifikatsbasierte Anmeldung des RA-Mitarbeiters am Web-RA-Frontend der V-PKI-CAs.

Die Identifizierung und Authentifizierung einer Organisation, die einen schriftlichen Antrag zur Sperrung eines Zertifikats eines Mitarbeiters einreicht, erfolgt durch ein auf dem Sperrantrag aufgebrachtes Dienstsiegel.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Zertifikate können von

- den Antragstellern selbst oder
- von der zuständigen RA im Auftrag des Antragstellers

beantragt werden.

Die Antragsteller müssen nachweisen, dass sie zur Beantragung berechtigt sind. Im Falle von Zertifikaten für natürliche Personen erfolgt diese Prüfung implizit durch die zuständige RA mittels Prüfung der Organisationszugehörigkeit. Im Falle von Zertifikaten für Gruppen, Funktionen, IT-Prozesse oder Organisationen muss die Berechtigung des Antragstellers durch einen berechtigten Vertreter der Organisation bestätigt werden.

4.1.2 Antragsprozess und -verantwortlichkeiten

Zur Beantragung von Zertifikaten gibt es zwei Varianten:

- Im Fall der ***dezentralen Beantragung*** beantragen die Antragsteller selbst die Zertifikate über die Benutzer-Webseiten der V-PKI-CAs. Der Antragsprozess sieht in diesem Fall folgende Schritte vor:
  - Der Antragsteller meldet sich an der Benutzer-Webseite der V-PKI-CAs mit der Zugangskennung seiner Domäne zur Zuordnung des Zuständigkeitsbereiches an.
  - Der Antragsteller gibt alle erforderlichen Daten ein, trifft eine Festlegung bzgl. der Veröffentlichung des Zertifikats und bestätigt die Akzeptanz der Nutzungsbedingungen und die Zustimmung zur Verarbeitung der Daten.
  - Nach Absenden des Web-Antrags bekommt der Antragsteller den Zertifikatsantrag als vorausgefülltes PDF zum Download angeboten.
  - Der Antragsteller druckt den Zertifikatsantrag aus und unterschreibt diesen zur späteren Verwendung im Rahmen der persönlichen Identifizierung (siehe Kap. 4.2.1).

- Im Fall der ***zentralen Beantragung*** beantragen die zuständigen RAs die Zertifikate im Auftrag der Antragsteller über die RA-Webseiten der V-PKI-CAs. Der Antragsprozess sieht in diesem Fall folgende Schritte vor:
  - Der Antragsteller erstellt einen schriftlichen Zertifikatsantrag mit allen erforderlichen Daten, inkl. einer Festlegung bzgl. der Veröffentlichung des Zertifikats sowie der Bestätigung der Akzeptanz der Nutzungsbedingungen und der Zustimmung zur Verarbeitung der Daten.
  - Der Antragsteller unterschreibt den Antrag zur späteren Verwendung im Rahmen der persönlichen Identifizierung (siehe Kap. 4.2.1).
  - Die zuständige RA beantragt, nach erfolgreicher Identifizierung des Antragstellers (siehe Kap. 4.2.1), das Zertifikat im Auftrag des Antragstellers über die RA-Webseiten der V-PKI-CAs.

4.2 Bearbeitung der Zertifikatsanträge

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identität des Antragstellers wird gemäß Kap. 3.2.3 geprüft, es stehen folgende Varianten zur Verfügung:

- Persönliche Identifizierung vor Ort durch die zuständige RA:
  In diesem Fall erfolgt die Identifizierung des Antragstellers im Rahmen der Antragsprüfung durch die zuständige RA.
- Vorgelagerte Identifizierung durch eine andere der in Kap. 3.2.3 aufgeführten Methoden:
  In diesem Fall erfolgt unabhängig von der Antragsprüfung (bis zu 3 Jahre vorher) die Identifizierung des Antragstellers. Der Antragsteller lässt anschließend die Bestätigung der Identifizierung zusammen mit dem Zertifikatsantrag der zuständigen RA zukommen.

Im Rahmen der Identitätsprüfung des Antragstellers wird neben dem Namen des Antragstellers ein eindeutiges Identifikationsmerkmal, z.B. die Nummer des amtlichen Ausweises, zur späteren eindeutigen Nachvollziehbarkeit in den Registrierungsunterlagen vermerkt.

Nach der Identifizierung des Antragstellers erfolgt die Prüfung des Zertifikatsantrags durch die zuständige RA auf Vollständigkeit, Korrektheit und Echtheit, es werden alle Angaben validiert.

Die Identität einer Organisation wird wie folgt geprüft:

- Die Identität einer Organisation, welche als eigenständige Domäne eine eigene RA betreibt, wird unabhängig von den Zertifikatsanträgen vorab bei der Einrichtung der Domäne und der RA gemäß Kap. 3.2.2 geprüft. In diesem Zuge wird auch die Identität der RA-Mitarbeiter gemäß einer der in Kap. 3.2.3 aufgeführten Methoden geprüft.
- Die Identität einer Organisation als Zertifikatsnehmer, welche keine eigene Domäne und keine eigene RA betreibt, wird im Rahmen der Antragsprüfung durch die RA gemäß Kap. 3.2.2 geprüft.

Mit der Identifizierung und Authentifizierung verbundene manuelle Tätigkeiten werden ausschließlich von vertrauenswürdigen Personal durchgeführt.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Zertifikatsanträge werden abgelehnt, wenn sie unvollständig oder fehlerhaft sind. Falls Schlüssel durch die Zertifikatsnehmer erzeugt werden, werden Anträge darüber hinaus abgelehnt, wenn

- der Schlüssel als kompromittiert gilt oder die Qualitätskriterien gemäß Kap. 6.1.5 und Kap. 6.1.6 nicht erfüllt,
- die Prüfung der Signatur des vorgelegten PKCS#10-Requests fehlschlägt und somit kein Nachweis über den Besitz des privaten Schlüssels erbracht werden kann.

Wenn alle Validierungsschritte gemäß Kap. 4.2.1 erfolgreich durchgeführt wurden und keiner der in diesem Kapitel genannten Prüfschritte zu einer Ablehnung führt, wird die Zertifikatsausstellung genehmigt.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Bestimmungen.

4.3 Ausstellung von Zertifikaten

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

Telekom Security stellt durch technische, organisatorische und personelle Maßnahmen sicher, dass bei der Ausstellung der Zertifikate die Integrität und Authentizität der in das Zertifikat zu schreibenden Daten gewährleistet werden.

Die korrekte Zuordnung der Schlüssel sowie die Wahrung der Vertraulichkeit der privaten Schlüssel werden in Abhängigkeit des Schlüsselmediums wie folgt sichergestellt:

- Im Fall von Software-Zertifikaten werden die Schlüssel unmittelbar vor der Zertifikatserzeugung durch die CA selbst erzeugt, die generierten Schlüssel und Zertifikate werden in Form verschlüsselter PKCS#12-Container sicher übergeben (siehe Kap. 6.1.2).
- Im Fall der Nutzung von Smartcards werden die öffentlichen Schlüssel unmittelbar vor der Zertifikatserzeugung aus der zu verwendenden Smartcard ausgelesen, nach Erzeugung der Zertifikate werden diese unmittelbar in die Smartcard geschrieben. Die privaten Schlüssel sind ausschließlich in den Smartcards gespeichert und können nicht ausgelesen werden.
- Im Fall von Zertifikaten für IT-Prozesse werden die Schlüssel entweder analog zu Software-Zertifikaten (s.o.) oder durch den Zertifikatsnehmer selbst erzeugt und nur die öffentlichen Schlüssel inkl. der relevanten Daten für die Zertifikate in Form von PKCS#10-Requests übergeben.

4.3.2 Benachrichtigung des Antragstellers über die Ausstellung eines Zertifikats

Nach der Ausstellung eines Zertifikats wird der Zertifikatsnehmer über die Ausstellung des Zertifikats und die ggf. erforderlichen nächsten Schritte (z.B. Download oder Freischaltung der Zertifikate, Aktivierung der Smartcard) per E-Mail informiert.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Keine Bestimmungen.

4.4.2 Veröffentlichung der Zertifikate durch das Trust Center

Siehe Kap. 2.1.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch das Trust Center

Keine Bestimmungen.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Zertifikatsnehmer werden über die Nutzungsbedingungen verpflichtet,

- Zertifikate ausschließlich gemäß der vorgesehenen Verwendungszwecke zu nutzen,
- Zertifikate bei Vorliegen eines Sperrgrundes unverzüglich sperren zu lassen,
- private Schlüssel nach Ablauf der Gültigkeit oder der Sperrung des Zertifikates nicht mehr zu nutzen, außer zur Entschlüsselung und
- die privaten Schlüssel über ihren gesamten Lebenszyklus zu schützen.

Bei Zertifikaten für Gruppen, Funktionen oder IT-Prozesse sind darüber hinaus die Schlüsselverantwortlichen verpflichtet:

- Schlüssel nur an autorisierte Schlüsselnutzer weiterzugeben, wobei eine maximale Anzahl von 30 Kopien nicht überschritten werden darf,
- die weiteren Schlüsselnutzer über die Nutzungsbedingungen zu informieren und sich deren Akzeptanz bestätigen zu lassen,
- die weiteren Schlüsselnutzer zum sorgsamen Umgang mit dem privaten Schlüssel zu verpflichten,
- sofern erforderlich, weiteren sperrberechtigten Personen das Sperrkennwort mitzuteilen und diese, sofern nicht bereits geschehen, ebenfalls über die Nutzungsbedingungen zu informieren und sich deren Akzeptanz bestätigen zu lassen,
- nach dem Ausscheiden einer Person aus dem Kreis der Schlüsselnutzer durch geeignete Maßnahmen sicherzustellen, dass ein Missbrauch des privaten Schlüssels durch den ausgeschiedenen Schlüsselnutzer hinreichend sicher verhindert wird. Falls dies nicht möglich ist, muss das Zertifikat gesperrt werden und ein neues Zertifikat mit neuem Schlüssel beantragt werden.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats

Zertifikatsnutzer haben die Verantwortung, vor Nutzung eines Zertifikats den gesamten Kontext und die gesamte Vertrauenskette inklusive der bereitgestellten Sperr- und Statusinformationen zu prüfen. Eine fehlende Prüfung von Zertifikatsinformationen oder das Ignorieren eines Prüfergebnisses geschieht auf eigene Verantwortung.

4.6 Zertifikatserneuerung unter Beibehaltung der Schlüssel (Renewal)

4.6.1 Umstände für ein Renewal

Ein Renewal von Zertifikaten ist nur bei Nutzung von Smartcards erlaubt, dabei gelten folgende Randbedingungen:

- Die Algorithmen und Schlüssellängen müssen weiterhin als zulässig für die gesamte Gültigkeitsdauer des neuen Zertifikats angesehen werden.
- Die maximale Nutzungsdauer der Schlüssel von 10 Jahren darf nicht überschritten werden.
- Zertifikate werden nur in einer festgelegten Frist zum Ende ihrer Laufzeit (ca. 6 Wochen) erneuert.
- Gesperrte und abgelaufene Zertifikate werden nicht erneuert.
- Der Name und die Organisationszugehörigkeit des Zertifikatsnehmers haben sich nicht geändert.
- Der Zertifikatsnehmer behält die Kontrolle über seine Smartcard, d.h. sofern eine Nachpersonalisierung der vorhandenen Smartcard beim Zertifikatsnehmer nicht möglich ist, muss der Zertifikatsnehmer persönlich zur Nachpersonalisierung der Smartcard bei der zuständigen RA vorstellig werden.

4.6.2 Antragsberechtigte für ein Renewal

Siehe Kap. 4.1.1.

4.6.3 Verarbeitung von Anträgen auf Renewal

Die Beantragung erfolgt grundsätzlich analog zur initialen Beantragung inkl. der Akzeptanz der aktuellen Nutzungsbedingungen. Es werden jedoch die Zertifikatsdaten nicht erneut abgefragt, sondern aus dem zu erneuernden Zertifikat übernommen.

Anträge auf Renewal werden wie initiale Anträge bearbeitet, siehe Kap. 4.2.

4.6.4 Benachrichtigung des Endteilnehmers über die Zertifikats-Neuausstellung

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 Zertifikatsausstellung durch die TSP

Siehe Kap. 4.4.3.

4.7 Zertifikatserneuerung mit neuen Schlüsseln (Re-Keying)

4.7.1 Umstände für ein Re-Keying

Für eine Zertifikatserneuerung mit neuen Schlüsseln gelten folgende Randbedingungen:

- Zertifikate werden nur in einer festgelegten Frist zum Ende ihrer Laufzeit (ca. 6 Wochen) erneuert.
- Gesperrte und abgelaufene Zertifikate werden nicht erneuert.
- Der Name und die Organisationszugehörigkeit des Zertifikatsnehmers haben sich nicht geändert.

4.7.2 Antragsberechtigte für ein Re-Keying

Siehe Kap. 4.1.1.

4.7.3 Verarbeitung von Anträgen auf Re-Keying

Die Beantragung erfolgt grundsätzlich analog zur initialen Beantragung inkl. der Akzeptanz der aktuellen Nutzungsbedingungen. Es werden jedoch die Zertifikatsdaten nicht erneut abgefragt, sondern aus dem zu erneuernden Zertifikat übernommen.

Anträge auf Re-Keying werden wie initiale Anträge bearbeitet, siehe Kap. 4.2.

4.7.4 Benachrichtigung des Endteilnehmers über die Zertifikats-Neuausstellung

Siehe Kap. 4.3.2.

4.7.5 Verhalten, das die Annahme eines Re-Key-Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.7.6 Veröffentlichung von Re-Key-Zertifikaten durch die TSP

Siehe Kap. 4.4.2.

4.7.7 Information Dritter über die Zertifikatsausstellung durch den TSP

Siehe Kap. 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Änderung von Zertifikatsdaten

Änderungen des Namens oder der Domänenzugehörigkeit des Zertifikatsnehmers erfordern eine Sperrung des alten Zertifikats und eine Neu-Beantragung gemäß Kap. 4.1 ff inkl. einer erneuten Identifizierung gemäß Kap. 3.2.

4.8.2 Antragsberechtigte für eine Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.3 Verarbeitung von Anträgen auf eine Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.4 Benachrichtigung des Endteilnehmers über die Zertifikats-Neuausstellung

Nicht anwendbar.

4.8.5 Verhalten, das die Annahme eines geänderten Zertifikats bestätigt

Nicht anwendbar.

4.8.6 Veröffentlichung geänderter Zertifikate durch die TSP

Nicht anwendbar.

4.8.7 Information Dritter über die Zertifikatsausstellung durch den TSP

Nicht anwendbar.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Sperrgründe

Zertifikate werden gesperrt, wenn:

- ein autorisierter Sperrantrag, auch ohne Angabe von Gründen, vom Zertifikatsnehmer oder, sofern anwendbar, der zuständigen RA vorliegt,
- die Angaben im Zertifikat zum Namen und zur Domäne nicht (mehr) korrekt sind,
- keine Autorisierung des Zertifikats (mehr) vorliegt,
- eine Schlüsselschwäche oder -Kompromittierung nachgewiesen wird, dazu zählt auch, wenn:
  - der private Schlüssel einer unautorisierten Person übergeben wurde,
  - der private Schlüssel nicht mehr den Anforderungen gemäß Kap. 6.1.5 und 6.1.6 genügt,
- ein Verstoß gegen die CP, CPS oder die Nutzungsbedingungen nachgewiesen wird, dazu zählt auch, wenn:
  - das Zertifikat nicht in Übereinstimmung mit der zum Zeitpunkt der Ausstellung gültigen Version dieser CPS ausgestellt wurde,
  - das Zertifikat missbräuchlich eingesetzt wurde,
  - der Zertifikatsnehmer gegen Vereinbarungen oder Nutzungsbedingungen verstoßen hat.

Zertifikate für Gruppen werden darüber hinaus gesperrt, wenn nach dem Ausscheiden einer Person aus dem Kreis der Schlüsselnutzer ein Missbrauch des privaten Schlüssels durch den ausgeschiedenen Schlüsselnutzer nicht hinreichend sicher verhindert werden kann (siehe Kap. 4.5.1).

Darüber hinaus werden alle betroffenen Zertifikate gesperrt, wenn

- Telekom Security den Betrieb des Trust Centers einstellt und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen hat,
- Telekom Security die Berechtigung verliert, Zertifikate der V-PKI auszustellen und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen hat,
- der private Schlüssel einer CA kompromittiert wurde oder
- ein Root- oder CA-Zertifikat gesperrt wird.

4.9.2 Berechtigte Sperrantragsteller

Die Sperrung eines Zertifikats kann grundsätzlich durch den Zertifikatsnehmer, den Schlüsselverantwortlichen oder die benannten Sperrberechtigten (nur bei Gruppen-/Funktionszertifikaten), die zuständige RA oder die Organisation beantragt werden.

4.9.3 Verfahren zur Beantragung von Sperrungen

Zur Sperrung eines Zertifikats gibt es verschiedene Möglichkeiten:

- Der Zertifikatsnehmer sperrt sein Zertifikat selbst über die Benutzer-Webseiten der V-PKI-CAs. Die Sperrung erfolgt in diesem Fall automatisch sofort nach Bestätigung des Sperrwunsches
- Der Zertifikatsnehmer wendet sich bei einem Sperrwunsch an die zuständige RA, welche die Sperrung über die RA-Webseiten veranlasst.
- Der Zertifikatsnehmer beantragt telefonisch eine Sperrung bei der Sperr-Hotline der Zertifizierungsstelle (7x24 Stunden erreichbar).
- Die Organisation des Zertifikatsnehmers beantragt schriftlich die Sperrung eines Zertifikats.

Der Zertifikatsnehmer wird über die Sperrung des Zertifikats informiert.

Gesperrte Zertifikate werden nicht wieder entsperrt.

4.9.4 Fristen zur Beantragung einer Sperrung

Zertifikatsnehmer werden über die Nutzungsbedingungen dazu verpflichtet, unverzüglich einen Sperrantrag zu stellen, sobald ein Sperrgrund gemäß Kap. 4.9.1 festgestellt wird.

4.9.5 Fristen zur Verarbeitung von Sperranträgen

Endteilnehmer-Zertifikate werden grundsätzlich so schnell wie möglich, jedoch spätestens innerhalb von 24 Stunden nach Eingang eines autorisierten Sperrantrags gesperrt. Diese Frist beinhaltet die Umsetzung des Sperrstatus in den Zertifikatsstatusdiensten.

Ausgenommen davon sind Sperrungen, die für einen späteren Zeitpunkt beantragt werden. In diesem Fall ist das im Sperrantrag aufgeführte Wunschdatum zur Sperrung des Zertifikats maßgeblich.

4.9.6 Anforderungen an Zertifikatsnutzer zur Prüfung von Sperrinformationen

Zertifikatsnutzer sind dazu angehalten, den Status von Zertifikaten mithilfe der angebotenen Zertifikatsstatusdienste gemäß Kap. 4.10 abzufragen, bevor sie einem Zertifikat vertrauen.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Sperrlisten („Certificate Revocation Lists“ (CRLs)), werden mindestens einmal täglich sowie kurzfristig nach der Sperrung eines Zertifikats aktualisiert.

4.9.8 Maximale Latenzzeit von Sperrlisten

Neu erstellte CRLs werden unmittelbar nach der Generierung in den Verzeichnissen veröffentlicht.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Es werden Online-Statusinformationen zu allen Zertifikaten per OCSP bereitgestellt. Die URL des jeweils relevanten OCSP-Responders ist in der Zertifikatserweiterung „Authority Information Access“ eines jeden Zertifikats enthalten.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

Zertifikatsnutzer sind dazu angehalten, bei der Prüfung eines Zertifikatsstatus per OCSP die Vorgaben zur Verarbeitung von OCSP-Antworten gemäß [RFC6960] zu berücksichtigen (siehe [TSCP]).

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Zu jedem von der DOI-CA ausgestellten Zertifikat kann der Status über den öffentlichen Bereich der Benutzer-Webseiten unter https://doi.telesec.de/doi/public/ unter Angabe der Zertifikatsseriennummer oder der Referenznummer abgefragt werden.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Die Zertifikatsnehmer müssen bei einer Schlüsselkompromittierung eine Sperrung gemäß Kap. 4.9.3 mit der Angabe „Schlüssel kompromittiert“ als Sperrgrund beantragen.

4.9.13 Umstände für eine Suspendierung

Eine Suspendierung von Zertifikaten (temporäre Sperrung) erfolgt ausschließlich als Transportschutz von personalisierten Smartcards im Null-PIN-Status (siehe Kap. 4.3.1). In diesem Fall erfolgt die Suspendierung automatisch durch die CA unmittelbar nach Ausstellung des Zertifikats. Ebenso erfolgt die Aufhebung der Suspendierung automatisch durch die CA unmittelbar nach Freischaltung des Zertifikats durch den Zertifikatsnehmer.

Darüber hinaus ist keine Suspendierung von Zertifikaten möglich.

4.9.14 Berechtigte Antragsteller für eine Suspendierung

Nicht anwendbar.

4.9.15 Ablauf einer Suspendierung

Siehe Kap. 4.9.13.

4.9.16 Begrenzung der Suspendierungsperiode

Siehe Kap. 4.9.13.

4.10 Zertifikatsstatusdienste

Über die gesamte Gültigkeitsdauer aller ausgestellten Zertifikate werden sowohl von den CAs signierte Sperrlisten als auch von delegierten OCSP-Respondern signierte OCSP-Auskünfte bereitgestellt, deren Authentizität und Integrität durch technische sowie organisatorische Maßnahmen sichergestellt wird.

4.10.1 Betriebliche Vorgaben

Alle Zertifikatsstatusdienste werden i.d.R. mehrmals täglich, spätestens jedoch alle 24 Stunden zeitsynchronisiert.

Unter Berücksichtigung der unterschiedlichen Aktualisierungsfristen beider Methoden sind die bereitgestellten Statusinformationen von Sperrlisten und OCSP-Auskünften nach spätestens 24 Stunden konsistent.

4.10.1.1 Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

Die OCSP-Responder werden konform zum [RFC6960] betrieben. Anfragen zu Zertifikaten mit unbekannten Zertifikatseriennummern werden mit dem Status „unknown“ beantwortet.

OCSP-Antworten erhalten einen Wert im nextUpdate-Feld, der 5 Tage nach dem thisUpdate-Wert liegt, werden jedoch für maximal 2 Stunden für weitere Anfragen wiederverwendet, sofern es zu keinen Statusänderungen in einer geringeren Frist kommt.

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

Gesperrte Zertifikate verbleiben auch nach ihrem Gültigkeitsende in der Sperrliste.

4.10.2 Verfügbarkeit

Die Zertifikatsstatusdienste stehen 7x24h zur Verfügung. Es sind Maßnahmen getroffen worden, die im Falle einer Störung die kurzfristige Wiederherstellung der Verfügbarkeit der Zertifikatsstatusdienste gewährleisten. Darüber hinaus werden größtmögliche Bemühungen unternommen, Störungen so schnell wie möglich zu beheben.

4.10.3 Optionale Merkmale

Keine Bestimmungen.

4.11 Beendigung der Teilnahme

Mit der Beendigung der Teilnahme eines Zertifikatsnehmers ist die Sperrung von dessen Zertifikaten verbunden, es gelten die in Kap. 4.9.1 ff beschriebenen Bestimmungen.

4.12 Schlüsselhinterlegung und Wiederherstellung

Eine Schlüsselhinterlegung wird nicht angeboten.

4.12.1 Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und-Praktiken

Nicht anwendbar.

4.12.2 Richtlinien und Praktiken für die Kapselung und Wiederherstellung von Sitzungsschlüsseln

Nicht anwendbar.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE REGELUNGEN

Das Trust Center der Deutschen Telekom Security GmbH liegt im Geltungsbereich einer vom Management freigegebenen Sicherheitsleitlinie und einem dazu gehörigen „Information Security Management System“ (ISMS), welches nach ISO 27001 zertifiziert ist.

Das ISMS selbst sowie weitere Sicherheitsrichtlinien, Sicherheitskonzepte und andere Dokumente stellen die Einhaltung der in [TSCP#5] genannten Anforderungen sicher. Insbesondere umfasst das Risikomanagement eine Risikoanalyse unter Einbeziehung von Eintrittswahrscheinlichkeiten und Schadensausmaßen sowie einer angemessenen Risikobehandlung inkl. einer abschließenden (Rest-)Risikoakzeptanz. Die Prozesse des Risikomanagements werden mindestens jährlich sowie anlassbezogen durchgeführt.

5.1 Physikalische Maßnahmen

Anlagen, Medien und Informationen des Trust Centers werden entsprechend ihrer Kritikalität durch physikalische Maßnahmen vor Verlust, Diebstahl, Schaden oder Kompromittierung geschützt. Diese Maßnahmen sind in internen Sicherheitskonzepten und weiteren Dokumenten festgehalten.

5.1.1 Standort und Bauweise

Die Infrastruktur des Trust Centers befindet sich in zwei georedundanten Rechenzentren (ein sogenanntes Twin-Core Rechenzentrum) innerhalb Deutschlands. Bei der Wahl der Standorte wurden, basierend auf einer entsprechenden Risikoanalyse, die umgebungsbezogenen Gegebenheiten wie die Anfälligkeit für Naturkatastrophen und andere Gefahrenquellen berücksichtigt. Die Bauweise und Infrastruktur des Gebäudes ist für den sicheren Betrieb kritischer Systeme ausgelegt und erfüllt die Anforderungen an eine Hochsicherheitszone.

Die für den Betrieb des Trust Centers relevanten Bereiche sind durch zusätzliche Einhausungen von anderen Bereichen getrennt und nach „Trusted Site Infrastructure TSI V3.2 Dual Site“ auditiert und zertifiziert.

5.1.2 Physikalischer Zutritt

Die Rechenzentren verfügen über umfängliche physische Sicherheitsmaßnahmen, die unter anderem Sicherheitspersonal, gesicherte Eingänge, Einbruchmeldeanlagen und Multi-Level-Zugangssysteme umfassen. Insbesondere sind die Räumlichkeiten des Trust Centers ausschließlich für berechtigte Personen in vertrauenswürdigen Rollen zugänglich und Besucher nur in Begleitung einer solchen Person gestattet.

Die Zutrittsrechte werden regelmäßig sowie bei Bedarf überprüft und ggf. angepasst.

5.1.3 Stromversorgung und Klimatisierung

Die Rechenzentren sind mit redundanten Stromversorgungen und Klimaanlagen ausgestattet. Die Systeme werden vor Spannungsschwankungen geschützt und sind durch unterbrechungsfreie Stromversorgungen (Kurz- und Langzeitüberbrückungen) mit Kreuz-Verkabelung abgesichert.

5.1.4 Wassereinwirkung

Die Rechenzentren befinden sich außerhalb des Gefahrenbereichs von Hochwasser oder anderen Gefahrenquellen. Darüber hinaus sind die Räumlichkeiten selbst durch weitere Maßnahmen vor Wassereinbruch bzw. Wasserschäden geschützt.

5.1.5 Brandvorsorge und Brandschutz

Die Rechenzentren sind dem kritischen Schutzbedarf entsprechend mit baulichen Maßnahmen und gemäß geltender Brandschutzbestimmungen vor Brandschäden geschützt.

5.1.6 Aufbewahrung von Medien

Medien werden ausschließlich in den Betriebsräumen des Trust Centers, vor Feuer- und Wassereinwirkung sowie unberechtigtem Zugriff geschützt, aufbewahrt.

5.1.7 Abfallentsorgung

Vertrauliche Dokumente und Datenträger werden ausschließlich über zertifizierte Entsorgungsunternehmen sicher entsorgt. Alle Datenträger werden darüber hinaus vor ihrer Entsorgung mit zertifizierten Verfahren gelöscht. Datenträger werden nicht für andere Zwecke wiederverwendet.

5.1.8 Off-Site-Sicherung

Sicherungen werden georedundant vorgehalten.

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Das Trust Center ist auf Basis der folgenden vertrauenswürdigen Rollen organisiert:

- Leiter Trust Center: trägt die gesamte Verantwortung für alle Trust Services des Trust Centers.
- Informations-Sicherheitsbeauftragter: plant und überwacht die Implementierung von Sicherheitsmaßnahmen, leitet das ISMS.
- Administrator: konfiguriert und wartet die IT-Infrastruktur (Netzwerke, Datenbanken, Server, Applikationen etc.).
- Solution-Manager: verantwortet einen Trust Service.
- Interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten Zertifikate, Prozesse, Dokumentationen und begutachtet die Konformität von Schlüssel- bzw. Root-Zeremonien.
- Root-/Compliance-Team: koordiniert die Umsetzung von Anforderungen, überwacht Anforderungsquellen , berät bei Vorfällen und Änderungen, verantwortet [TSCP], bearbeitet Anträge für CA-Ausstellungen.
- RA-Mitarbeiter: validiert Zertifikatsanträge, veranlasst die Ausstellung oder Sperrung von Zertifikaten.

Bei den externen RAs sind folgende vertrauenswürdigen Rollen etabliert:

- Leiter Registrierungsstelle: verantwortet die Umsetzung und Einhaltung der Anforderungen gemäß der mit der Zertifizierungsstelle abgeschlossenen RA-Vereinbarung, benennt die Master- und/oder Sub-RA-Mitarbeiter.
- Master-RA-Mitarbeiter: verwaltet die Sub-Domänen und Sub-RA-Mitarbeiter, richtet die Zugänge der Sub-RA-Mitarbeiter ein.
- Sub-RA-Mitarbeiter: identifiziert und registriert Zertifikatsnehmer, prüft und genehmigt oder lehnt Anträge auf Ausstellung und Sperrung von Zertifikaten ab.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Für alle in Kap. 5.2.1 aufgeführten Rollen des Trust Centers ist mindestens ein Vertreter benannt.

Es sind technische und organisatorische Maßnahmen vorhanden, wodurch sicherheitsrelevante oder -kritische Tätigkeiten nur durch Personen in vertrauenswürdigen Rollen und nur im Vier-Augen-Prinzip durchgeführt werden. Die Anzahl der Mitarbeiter, die solche sicherheitsrelevanten oder -kritischen Tätigkeiten ausüben, ist unter Berücksichtigung von Vertreterregelungen und arbeitstechnischen Umständen auf ein Minimum beschränkt.

Die sicherheitsrelevanten und -kritischen Tätigkeiten, für die ein Vier-Augen-Prinzip (oder mehr) benötigt werden, sind:

- Generierung, Sicherung und Wiederherstellung von CA-Schlüsseln,
- Bewertung von Sicherheitsvorfällen.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Für die Identifizierung und Authentifizierung geeigneter Personen für die in Kap. 5.2.1 benannten Rollen des Trust Centers gelten die nachfolgend aufgeführten Bestimmungen.

Die davon anwendbaren Bestimmungen gelten analog für die externen RAs, Details sind in den mit den externen RAs abgeschlossenen RA-Vereinbarungen geregelt.

Die Identifizierung geeigneter Personen zur Besetzung von Rollen, die Übertragung der Rollen (Authentifizierung) sowie deren Entzug erfolgen nach einem dokumentierten Prozess, welcher u.a. die Klärung des Bedarfs bzw. Ausschluss von Interessenskonflikten, die Bereitschaft der Person zur Übernahme der Tätigkeiten, die Freigabe durch die Führungskraft und die Dokumentation von Nachweisen hierfür beinhalten.

Vor der Übertragung einer vertrauenswürdigen Rolle (oder schon bei der Einstellung als Mitarbeiter) wird die entsprechende Person unter Vorlage eines amtlichen Ausweises persönlich identifiziert und es werden von dieser Person sowie der Leitung des Trust Centers die Akzeptanz zur Übertragung der Rolle, der damit verbundenen Verantwortung und den daraus resultierenden Pflichten zur Gewährleistung der Sicherheit eingeholt.

Rollen werden nur an Personen übertragen, wenn dadurch keine Interessenskonflikte (siehe dazu auch Kap. 5.2.4) entstehen und die Unabhängigkeit gewahrt wird, d.h. dass:

- die Bereiche des Trust Centers, 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 sind,
- alle Mitarbeiter, die mit der Generierung und Sperrung von Zertifikaten betraut sind, in der Ausübung ihrer Tätigkeit frei von finanziellem oder anderem Druck sind, der das Vertrauen in die vom Trust Center erbrachten Dienstleistungen beeinträchtigen könnte. Dies gilt sowohl für alle Mitarbeiter in vertrauenswürdigen Rollen als auch für die leitenden Angestellten und Führungskräfte.

Diese Struktur, die die Unparteilichkeit des Betriebs gewährleistet, ist unter anderem im ISMS-Handbuch des Trust Centers dokumentiert.

Die Rolleninhaber werden offiziell von der Leitung des Trust Centers in die vertrauenswürdige Rolle berufen.

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

Die Vergabe der erforderlichen Berechtigungen erfolgt nach dem „Least Privilege“-Prinzip, d.h. alle Berechtigungen sind auf das erforderliche Minimum beschränkt.

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

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Folgende Rollen werden voneinander getrennt, sodass ein Mitarbeiter nur die unter einem Auflistungspunkt geführten Rollen gleichzeitig besetzen darf:

- Management/Leiter Trust Center,
- IT-Sicherheitsbeauftragter/Compliance-Team/Interner Auditor,
- RA-Mitarbeiter/Validierungsspezialist,
- Administrator.

Die genannten Rollen können ausschließlich Antragsteller für Zertifikate sein, wenn diese Zertifikate im Namen der eigenen Organisation beantragt werden.

5.3 Personelle Maßnahmen

5.3.1 Qualifikationen, Erfahrung und Berechtigungen

Die Leitung des Trust Centers (Management) ist beständig und hat langjährige Erfahrung in Bezug auf den technischen und auch organisatorischen Betrieb der angebotenen Dienste des Trust Centers. Darüber hinaus ist sie durch Ausbildung, Erfahrung und Schulung versiert in den Bereichen Informationssicherheit (inkl. Risikomanagement, Sicherheitsverfahren für Personal etc.) und PKI-Technologien.

Die Mitarbeiter des Trust Centers erfüllen die Anforderung an hinreichendes Expertenwissen zur korrekten Ausübung ihrer Tätigkeiten aufgrund von Ausbildung, spezifischer Schulungen, langjähriger Erfahrung oder einer Kombination aus diesen. Darüber hinaus werden alle Mitarbeiter der Telekom Security und die des Trust Centers im Besonderen regelmäßig zu allgemeinen Sicherheits- und Datenschutzbestimmungen, aktuellen Gefahren sowie den konkreten Vorgaben des ISMS informiert (bspw. vom ISMS oder konzernweiten Informationsveranstaltungen).

Die RA-Mitarbeiter der externen Registrierungsstellen werden vor Aufnahme ihrer Tätigkeit geschult, so dass sie über hinreichendes Wissen zur korrekten Ausübung ihrer Tätigkeiten verfügen. Die Schulung der Leiter der Registrierungsstellen und der Master-RA-Mitarbeiter erfolgt durch qualifizierte Mitarbeiter des Trust Centers oder vom Trust Center beauftragte qualifizierte Dritte. Die Schulung der Sub-RA-Mitarbeiter erfolgt entweder analog oder durch die Leiter der Registrierungsstellen oder die Master-RA-Mitarbeiter als Multiplikatoren.

5.3.2 Verfahren zur Hintergrundprüfung

Alle Mitarbeiter des Trust Centers in vertrauenswürdigen Rollen weisen ihre Vertrauenswürdigkeit durch regelmäßige Vorlage eines amtlichen Führungszeugnisses nach. Vor der Erstbeschäftigung werden zudem relevante Abschlüsse und Referenzen überprüft, um die Eignung für die Tätigkeit festzustellen. Mitarbeiter, welche mit kritischen oder sicherheitsrelevanten Prozessen betraut werden, müssen erfolgreich eine Sicherheitsüberprüfung absolviert haben.

Diese Anforderungen gelten, sofern anwendbar, analog für Mitarbeiter externer RAs, Details sind in den RA-Vereinbarungen geregelt.

5.3.3 Schulungsanforderungen

Siehe Kap. 5.3.1.

5.3.4 Nachschulungsintervalle und -anforderungen

Die Mitarbeiter des Trust Centers werden regelmäßig (mindestens jährlich) hinsichtlich der Informationssicherheit sowie Datenschutz und zusätzlich anlassbezogen zu aktuellen Bedrohungen und Sicherheitspraktiken sensibilisiert.

Darüber hinaus wird Personal in vertrauenswürdigen Rollen regelmäßig fachlich geschult bzw. fortgebildet, um das erforderliche Know-How aufrechtzuerhalten.

Die RA-Mitarbeiter der externen Registrierungsstellen erhalten regelmäßig sowie bei Bedarf, z.B. bei Änderungen, eine Auffrischungsschulung, analog zur initialen Schulung entweder durch Mitarbeiter oder Beauftragte des Trust Centers oder durch geschulte Mitarbeiter der Registrierungsstellen als Multiplikatoren.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Keine Bestimmungen.

5.3.6 Sanktionen bei unbefugten Handlungen

Mitarbeiter des Trust Centers sowie der externen RAs sind rechenschaftspflichtig für ihr Handeln.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Nicht anwendbar.

5.3.8 Dem Personal zur Verfügung gestellte Dokumentation

Allen Rolleninhabern stehen Rollenbeschreibungen zur Verfügung, die neben den sich aus der Rolle ergebenden Verantwortungen und Pflichten mindestens die erforderlichen

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

enthalten.

Die Informationssicherheitsrichtlinien sowie die darin festgelegten Sicherheitsrollen und -zuständigkeiten werden in entsprechenden Konzerndokumenten beschrieben und stehen allen Mitarbeitern über das Intranet zur Verfügung.

Allen RA-Mitarbeitern der externen RAs werden neben den Schulungsunterlagen verständliche Handbücher zur Verfügung gestellt.

5.4 Protokollierungsverfahren

5.4.1 Zu protokollierende Ereignisse

Die folgenden Ereignisse werden kontinuierlich inkl. einer Beschreibung des Ereignisses, des präzisen Zeitpunkts und, sofern anwendbar, der Identität des Auslösers protokolliert:

- alle wesentlichen Ereignisse der Zertifikats- und Schlüsselmanagementsysteme sowie Statusdienste, dazu zählen:
  - Schlüsselerzeugung, -sicherung, -speicherung, -wiederherstellung, -archivierung und -vernichtung,
  - Zertifikatsbeantragung inkl. Erneuerung,
  - Validierungen, Genehmigungen und Ablehnungen,
  - Ausstellung der Zertifikate,
  - Beantragung von Sperrungen,
  - Sperrung von Zertifikaten,
  - Generierung von Sperrlisten,
  - Signatur von OCSP-Antworten,
- alle sicherheitsrelevanten Ereignisse an den PKI- und Sicherheitssystemen, dazu zählen
  - Änderungen der Sicherheitsrichtlinien der Systeme,
  - 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,
- Physikalische Ein- und Austritte in bzw. aus den Sicherheitszonen

Die Zeit der protokollierenden Systeme wird mehrfach pro Tag mit einer zentralen und vertrauenswürdigen Quelle synchronisiert.

5.4.2 Häufigkeit der Log-Verarbeitung

Logdaten werden wie folgt ausgewertet:

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

5.4.3 Aufbewahrungszeitraum für Logdaten

Alle in Kap. 5.4.1 erfassten Logdaten werden über einen angemessenen Zeitraum aufbewahrt.

5.4.4 Schutz der Audit-Protokolle

Es sind technische und organisatorische Maßnahmen etabliert, welche die Vertraulichkeit und Integrität der Logdaten sicherstellen. Die Aufbewahrung der Logdaten wird zudem in internen Audits überwacht.

Logdaten werden im Bedarfsfall, z.B. in Gerichtsverfahren oder auf Anfrage interner und externer Auditoren, bereitgestellt.

5.4.5 Backup-Verfahren für Audit-Protokolle

Logdaten werden im Rahmen der regelmäßigen System-Backups mitgesichert.

5.4.6 Audit-Sammelsystem

Alle sicherheitsrelevanten Ereignisse an PKI- und Sicherheitssystemen werden unverzüglich über sichere Kommunikationskanäle an einen separaten und manipulationsgeschützten Log-Server gesendet.

5.4.7 Benachrichtigung der Ereignis-auslösenden Person

Keine Bestimmungen.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Bestimmungen.

5.5 Aufbewahrung von Aufzeichnungen

5.5.1 Aufzubewahrende Aufzeichnungen

Zu jedem Zertifikat wird die Antrags-/Zertifikatshistorie mit Angabe von Datum, Uhrzeit und, sofern anwendbar, der Identität der handelnden Person elektronisch in der CA aufgezeichnet. Dazu zählen die folgenden Aktivitäten der Zertifikatsnehmer sowie der internen und ggf. externen RAs:

- alle Aktivitäten im Zusammenhang mit der Beantragung, Registrierung, Validierung und Genehmigung oder Ablehnung von Anträgen auf Ausstellung, Erneuerung und Sperrung von Zertifikaten aller Hierarchiestufen,
- alle Aktivitäten im Zusammenhang mit dem Lebenszyklus von Schlüsseln und Zertifikaten aller Hierarchiestufen. Dazu zählen mindestens, sofern anwendbar,
  - die Generierung, Speicherung, Backup, Wiederherstellung, Archivierung und Zerstörung von Schlüsseln sowie
  - die Ausstellung, Akzeptanz, Veröffentlichung und Sperrung von Zertifikaten.

Des Weiteren werden zu jedem Zertifikat die im Rahmen der Beantragung einer Ausstellung, Erneuerung oder Sperrung vom Antragsteller vorgelegten oder dem Antragsteller übermittelten relevanten Informationen und Dokumente aufgezeichnet bzw. aufbewahrt („Registrierungsinformationen“). Hierzu zählen mindestens die Antragsformulare inkl. der Informationen zur Identität und ggf. weiterer Attribute des Zertifikatsnehmers bzw. Schlüsselverantwortlichen und der Akzeptanz der zum Zeitpunkt der Antragstellung geltenden Nutzungsbedingungen.

Die Antragsformulare verbleiben für die gesamte Dauer der Aufbewahrung bei der zuständigen RA, entweder in Papierform oder elektronisch. Die Anforderungen zur Aufbewahrung sowie ggf. Übergabe bei Einstellung des RA-Betriebs sind in den mit den externen RAs abgeschlossenen RA-Vereinbarungen festgelegt.

Darüber hinaus werden folgende Informationen und Dokumente aufgezeichnet bzw. aufbewahrt:

- alle veröffentlichten CP, CPS und Nutzungsbedingungen,
- Zertifizierungsunterlagen und Auditberichte,
- relevante Dokumentationen bzgl. der Sicherheit der Systeme aus dem
  - Changemanagement,
  - Schwachstellenmanagement,
  - Rollenmanagement,
  - Lifecycle-Management der kryptografischen Module,
- ggf. weitere Informationen, die zur Gewährleistung der Kontinuität der Dienste erforderlich sind oder als Beweismittel in Gerichtsverfahren benötigt werden.

5.5.2 Aufbewahrungszeitraum für Aufzeichnungen

Von den in Kap. 5.5.1 aufgeführten Aufzeichnungen werden die Antrags-/Zertifikatshistorie, Antragsformulare, CP, CPS und Nutzungsbedingungen sowie die Zertifikate selbst für 10 Jahre nach Ablauf der Zertifikatsgültigkeit aufbewahrt.

Alle weiteren Aufzeichnungen werden für 2 Jahre aufbewahrt.

5.5.3 Schutz der Aufzeichnungen

Es sind technische und organisatorische Maßnahmen etabliert, welche die Verfügbarkeit, Vertraulichkeit und Integrität der Aufzeichnungen über die Aufbewahrungsdauer sicherstellen.

5.5.4 Backup-Verfahren für Aufzeichnungen

Die elektronischen Ablagen zur Aufbewahrung elektronisch signierter Anträge und ggf. digitalisierter Protokolle sind mehrfach redundant aufgebaut und werden regelmäßig gesichert.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Siehe Kap. 6.8.

5.5.6 Archivsystem (intern oder extern)

Zur Archivierung elektronisch erfasster Daten (z.B. Zertifikatshistorie) kommen ausschließlich interne Archivsysteme zum Einsatz. Papierunterlagen (z.B. Antragsformulare) werden bei den zuständigen RAs archiviert, diese können sowohl intern als auch extern angesiedelt sein.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Aufzeichnungen

Die in Kap. 5.5.1 aufgeführten Aufzeichnungen werden im Bedarfsfall geprüft und ggf. als Beweismittel herausgegeben oder auf Anfrage interner oder externer Auditoren zur Verfügung gestellt.

5.6 Schlüsselwechsel

Vor Ablauf eines Sub-CA-Zertifikats wird rechtzeitig ein neues CA-Zertifikat bei der Root-CA beantragt. Dabei wird der Zeitraum zwischen der Beantragung und Veröffentlichung des neuen CA-Zertifikats und der Außerbetriebnahme des alten CA-Zertifikats hinreichend groß gewählt, so dass für Zertifikatsnehmer keine Unterbrechung in deren Betrieb entsteht.

Das neue Sub-CA-Zertifikat wird erst zur geplanten Inbetriebnahme aktiviert.

5.7 Kompromittierung und Notfall-Wiederherstellung

5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

Die Notfalldokumentation des Trust Centers berücksichtigt die Anforderungen der [TSCP].

Die Mitarbeiter des Trust Centers verfügen über mehrere Möglichkeiten (technische Schnittstelle, direkter Kontakt zum ISMS, Mitarbeiter-Portal) zur Meldung von (Informationssicherheits-)Vorfällen und sind dazu verpflichtet, Vorfälle zu melden. Meldungen bzw. Alarmen wird durch qualifiziertes Personal entsprechend der Kritikalität in angemessener Zeit nachgegangen.

Sicherheitsvorfälle mit signifikanten Auswirkungen auf den bereitgestellten Vertrauensdienst oder auf personenbezogene Daten werden innerhalb von 24 Stunden an die zuständigen Behörden gemeldet, je nach Art und Kontext des Vorfalls.

Natürliche oder juristische Personen, welche die Vertrauensdienste der Telekom Security in Anspruch nehmen und potenziell von einem Sicherheitsvorfall negativ betroffen sind, werden umgehend über den Sicherheitsvorfall informiert.

5.7.2 Wiederherstellung bei Beschädigung von Computern, Software oder Daten

Es werden regelmäßige Datensicherungen aller relevanten Systeme durchgeführt, um diese bei Bedarf wiederherstellen zu können. Die Datensicherungen werden georedundant vorgehalten und unterliegen den gleichen Sicherheitsmaßnahmen wie kritische Systeme.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

Die Kompromittierung, der Verdacht auf Kompromittierung oder der Verlust eines privaten CA-Schlüssels wird als Notfallszenario behandelt und entsprechend der in der Notfalldokumentation definierten Prozesse bearbeitet. Die betroffenen Schlüssel werden bis zur endgültigen Klärung nicht mehr benutzt.

Im Falle einer Kompromittierung eines CA-Schlüssels wird die Sperrung des CA-Zertifikats beantragt und alle betroffenen Zertifikatsnehmer, die RAs sowie weitere Instanzen, mit denen entsprechende Vereinbarungen abgeschlossen wurden, informiert.

5.7.4 Geschäftsfortführung nach einem Notfall

Im Falle eines Notfalls wird der Betrieb innerhalb der in der Notfalldokumentation festgelegten Frist wiederhergestellt, nachdem alle Ursachen durch geeignete Abhilfemaßnahmen beseitigt wurden.

5.8 Einstellung des CA- oder RA-Betriebs

Telekom Security wird vor Einstellung des Betriebs evaluieren, ob die Bereitstellung des Trust Services für bestehende Kunden an einen anderen Trust Service Provider übertragen werden kann. Vor der Übertragung werden entsprechende Vereinbarungen mit dem übernehmenden Trust Service Provider abgeschlossen.

Sollte eine Übergabe nicht möglich sein, wird eine sichere Beendigung gemäß eines fortlaufend aktualisierten Beendigungsplans gewährleistet.

Vor der Beendigung oder Übertragung einer CA werden

- alle Betroffenen informiert (Zertifikatsnehmer, RAs, Root-CA, weitere Betroffene mit denen Telekom Security Verträge hat),
- Zertifikatsnutzern die Information über die Beendigung oder Übertragung bereitgestellt,
- die Vereinbarungen mit Unterauftragnehmern, z.B. externen RAs, beendet.

Vor der Beendigung einer CA

- wird eine zuverlässige Stelle verpflichtet alle Informationen die erforderlich sind um den Betrieb der CA nachzuweisen, für einen angemessenen, ggf. mit den Endteilnehmern und Anderen vereinbarten Zeitraum aufzubewahren. Dazu zählen mindestens:
  - Registrierungsinformationen,
  - Zertifikatsstatusinformationen,
  - Ereignisprotokollarchive,
  - CA-Zertifikate,
- werden die privaten CA-Schlüssel zerstört und
- alle von der CA ausgestellten, noch gültigen und nicht gesperrten Zertifikate gesperrt.

Nach der Beendigung oder Übertragung einer CA und Übergabe der Informationen an eine andere Stelle werden alle Schlüssel, Zertifikate und Kundendaten gelöscht.

Die Vorkehrungen, die zur Beendigung oder Übertragung einer CA getroffen werden, werden in einem aktuellen Beendigungsplan festgelegt.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

6.1.1.1 Generierung von CA-Schlüsselpaaren

Schlüsselpaare für CAs werden mit HSMs gemäß Kap. 6.2.1 in der sicheren Umgebung des Trust Centers im Rahmen einer Schlüssel-Zeremonie generiert.

Die Generierung erfolgt durch mindestens zwei vertrauenswürdige Mitarbeiter des Trust Centers und setzt die Freigabe des Managements voraus.

Die an der Zeremonie beteiligten vertrauenswürdigen Rollen und deren Aufgaben vor, während und nach der Schlüsselzeremonie sind in einer Arbeitsanweisung beschrieben. Die einzelnen Schritte der Schlüsselzeremonie folgen einem festgelegten Protokoll und werden in diesem dokumentiert.

Zum Nachweis der Authentizität und der Integrität wird der Hashwert des generierten Zertifikatsrequests im Generierungsprotokoll aufgenommen und bei der Zertifikatsbeantragung übergeben.

6.1.1.2 Generierung von OCSP-Signer-Schlüsselpaaren

Schlüsselpaare für OCSP-Signer werden in HSMs gemäß Kap. 6.2.1 in der sicheren Umgebung des Trust Centers generiert.

6.1.1.3 Generierung von Endteilnehmer-Schlüsselpaaren

Die Erzeugung der Endteilnehmer-Schlüssel ist abhängig von dem verwendeten Schlüsselmedium:

- Die Schlüssel von Software-Zertifikaten werden durch die Zertifizierungsstelle unter Nutzung eines zertifizierten Hardware-Kryptomoduls erzeugt.
- Die Schlüssel von Zertifikaten für IT-Prozesse werden entweder wie Software-Zertifikate (s.o.) oder durch den Zertifikatsnehmer selbst erzeugt.
- Die Schlüssel von Smartcard-Zertifikaten werden durch sichere Schlüsselgeneratoren innerhalb der Smartcards erzeugt.

6.1.2 Bereitstellung der privaten Schlüssel an die Zertifikatsnehmer

Die Übergabe der privaten Schlüssel ist abhängig von dem verwendeten Schlüsselmedium:

- Im Fall von Software-Zertifikaten werden die Schlüssel in Form von PKCS#12-Containern den Antragstellern oder bevollmächtigten RAs über die Web-Frontends zum Download angeboten. Zur sicheren Übergabe werden folgende Maßnahmen getroffen:
  - Die PKCS#12-Container werden durch ein hinreichend langes und komplexes Passwort geschützt.
  - Der Download eines PKCS#12-Containers durch einen RA-Mitarbeiter im Auftrag des Zertifikatsnehmers ist nur nach erfolgreicher zertifikatsbasierter Authentifizierung des RA-Mitarbeiters am RA-Web-Frontend möglich.
  - Der Download eines PKCS#12-Containers durch den Zertifikatsnehmer über das Benutzer-Web-Frontend ist nur mittels eines antragsindividuellen, hinreichend langen und komplexem Download-Passworts möglich, welches nur dem Zertifikatsnehmer selbst bekannt ist.
  - Nach Bestätigung des erfolgreichen Downloads eines PKCS#12-Containers wird der private Schlüssel in der CA gelöscht, so dass kein weiterer Download mehr möglich ist.
  - Nach drei erfolglosen Download-Versuchen werden die Schlüssel gelöscht und das Zertifikat gesperrt.
- Im Fall der Nutzung von Smartcards als Schlüsselmedium wird sichergestellt, dass die Smartcards dem korrekten Empfänger zugestellt werden und die Schlüssel bzw. Zertifikate nur durch die korrekten Empfänger genutzt werden können.

6.1.3 Übergabe öffentlicher Schlüssel an die Zertifizierungsstelle

Öffentliche Schlüssel werden der Zertifizierungsstelle nur in dem Fall übergeben, wenn die Schlüssel durch die Zertifikatsnehmer selbst erzeugt werden, d.h. nur bei Zertifikaten für IT-Prozesse. In diesem Fall werden die öffentlichen Schlüssel mittels PKCS#10-Requests über die Web-Frontends übergeben.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

Alle CA-Zertifikate werden wie in Kap. 2.2 beschrieben durch die Telekom Security in den entsprechenden Verzeichnissen veröffentlicht. Darüber hinaus werden sie von der Root-CA unter https://x500.bund.de/ veröffentlicht.

6.1.5 Schlüssellängen

Alle im Umfeld der V-PKI-CAs verwendeten Schlüssel und Kryptoalgorithmen entsprechen den Empfehlungen der [TR2102-1] sowie [SOGIS].

Es werden zurzeit ausschließlich folgende Schlüssel für Endteilnehmer-Zertifikate unterstützt:

- RSA-Schlüssel mit einer Schlüssellänge von mindestens 3072 Bit.
- EC-Schlüssel der nachfolgend aufgeführten Kurven:
  - mit einer Schlüssellänge von 256 Bit:
    - brainpoolP256r1,
    - secp256r1,
  - mit einer Schlüssellänge von 384 Bit:
    - secp384r1.

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Keine Bestimmungen.

6.1.7 Schlüsselverwendung

Alle Zertifikate erhalten eine zu den erlaubten Anwendungen (siehe Kap. 1.4.1) korrespondierende Schlüsselverwendung, welche in den Erweiterungen keyUsage und extendedKeyUsage festgelegt ist.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

Es werden derzeit ausschließlich HSMs verwendet, welche nach FIPS 140-2 Level 3 zertifiziert sind und auch in dem entsprechenden FIPS-Modus betrieben werden. Zum Schutz der HSMs während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet, die während der FIPS- Zertifizierungen geprüft wurden.

Bei den eingesetzten Smartcards handelt es sich um Smartcards, welche nach CC EAL 4+ zertifiziert sind.

6.2.2 Mehrpersonenkontrolle über private Schlüssel (n von m)

Generierung, Sicherung, Wiederherstellung und Löschung privater CA-Schlüssel sind nur im Vier-Augen-Prinzip möglich, siehe dazu Kap. 6.1.1, 6.2.4, 6.2.8 und 6.2.10. Beim Import und Export der Schlüssel in die bzw. aus den Backup-HSMs kommen Authentisierungstoken zum Einsatz, über die ein Mehr-Personen-Prinzip erzwungen wird.

Zur Nutzung privater Endteilnehmer-Schlüssel ist keine Mehrpersonenkontrolle vorgesehen.

6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung von privaten Schlüsseln außerhalb des Trust Centers der Telekom Security findet nicht statt.

6.2.4 Sicherung privater Schlüssel

Die privaten CA-Schlüssel werden im Vier-Augen-Prinzip ausschließlich auf Backup-HSM gesichert, welche unter einem vergleichbaren Sicherheitsniveau wie die in Betrieb befindlichen HSMs aufbewahrt werden.

Private Endteilnehmer-Schlüssel werden grundsätzlich nicht durch die Zertifizierungsstelle gesichert.

6.2.5 Archivierung privater Schlüssel

Eine Archivierung von privaten Schlüsseln findet nicht statt.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Eine Übertragung privater CA-Schlüssel findet ausschließlich zu Zwecken der Sicherung in bzw. Rücksicherung von Backup-HSMs statt (siehe Kap. 6.2.4). Die Arbeitsschritte werden im Rahmen einer Schlüssel-Zeremonie und mindestens im Vier-Augen-Prinzip durchgeführt. Die Schlüssel werden ausschließlich mit den Bordmitteln der HSMs verschlüsselt übertragen und liegen außerhalb des Kryptomoduls niemals im Klartext vor.

Eine Übertragung privater Schlüssel in bzw. aus Smartcards ist nicht möglich.

6.2.7 Speicherung privater Schlüssel in kryptografischen Modulen

Die in den kryptografischen Modulen gespeicherten Schlüssel sind mit den Bordmitteln der kryptografischen Module gesichert abgelegt.

6.2.8 Methoden zur Aktivierung privater Schlüssel

Eine Aktivierung privater CA-Schlüssel wird durch Personen in vertrauenswürdigen Rollen mithilfe der vom HSM bereitgestellten Funktionen durchgeführt.

Smartcards müssen zur initialen Aktivierung aus dem Null-PIN-Zustand in den Betriebszustand mittels Setzens einer mindestens sechsstelligen PIN versetzt werden. Im Betriebszustand muss für jede Nutzung des privaten Schlüssels die PIN eingegeben werden.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

Eine Deaktivierung privater CA-Schlüssel wird durch Personen in vertrauenswürdigen Rollen mithilfe der vom HSM bereitgestellten Funktionen durchgeführt.

6.2.10 Methoden zur Zerstörung privater Schlüssel

Die Zerstörung von CA-Schlüsseln erfolgt wie die Generierung in einer Schlüssel-Zeremonie (siehe Kap. 6.1.1) und berücksichtigt alle Kopien der Schlüssel. Die Schlüssel werden mit den Bordmitteln der HSMs zerstört.

Wenn HSMs mit CA-Schlüsseln am Ende ihrer Nutzungsdauer oder aufgrund eines Defekts außer Betrieb genommen werden, so werden alle privaten Schlüssel, die in diesen Modulen gespeichert sind, wie oben beschrieben zerstört. Die Zerstörung betrifft nicht die Kopien der privaten Schlüssel, sofern die Schlüssel in anderen bzw. neuen kryptografischen Modulen noch weiter genutzt werden sollen.

Die Zerstörung privater Endteilnehmer-Schlüssel obliegt den Endteilnehmern gemäß der akzeptierten Nutzungsbedingungen.

6.2.11 Bewertung kryptografischer Module

Siehe Kap. 6.2.1.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel (d.h. Zertifikate) werden gemäß Kap. 5.5.1 ff archiviert.

6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Endteilnehmer-Zertifikate werden mit folgenden Gültigkeitsdauern ausgestellt:

- Smartcard-Zertifikate: maximal 5 Jahre
- Server-/Gateway-Zertifikate: maximal 1 Jahr
- alle anderen Zertifikate: maximal 3 Jahre

Dabei gilt, dass das Gültigkeitsende eines Zertifikats niemals das Gültigkeitsende des ausstellenden CA-Zertifikats überschreitet (Schalenmodell).

Die Zertifikate werden grundsätzlich nur im Zeitraum ihrer Gültigkeit genutzt. Ausgenommen davon sind Signaturzertifikate, die auch nach Ablauf ihrer Gültigkeit zur Prüfung von älteren Signaturen verwendet werden dürfen[4].

Die privaten Schlüssel werden grundsätzlich nur im Zeitraum der Gültigkeit des korrespondierenden Zertifikates genutzt. Ausgenommen davon sind ggf. Schlüssel zur Entschlüsselung, um die Entschlüsselung verschlüsselter Daten auch nach Ablauf des zur Verschlüsselung verwendeten Zertifikats zu ermöglichen[5].

Bei Nutzung von Smartcards ist ein Renewal der Endteilnehmer-Zertifikate möglich. In diesem Fall kann sich die Nutzungsdauer der Schlüssel somit auf die zweifache Laufzeit, d.h. maximal 10 Jahre, belaufen.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Die Aktivierungsdaten der HSMs werden bei Inbetriebnahme der HSMs im Vier-Augen-Prinzip im Rahmen eines geregelten Change-Prozesses mit den Bordmitteln der HSMs generiert und installiert.

[4] Teilnehmer sind jedoch angehalten, langfristig prüfbare Dokumente/Daten rechtzeitig zu übersignieren.
[5] Teilnehmer sind jedoch angehalten, langfristig verschlüsselt abgelegte Daten rechtzeitig umzuschlüsseln.

Die PINs und PUKs für Endteilnehmer-Schlüssel auf Smartcards können wie folgt generiert und installiert werden:

1. Erzeugung durch einen sicheren Zufallszahlengenerator der CA:
   In diesem Fall werden bereits bei Antragstellung die PINs und PUKs erzeugt, dem Endteilnehmer sicher übergeben und bis zur Installation sicher in der CA vorgehalten. Die Installation der PINs und PUKs erfolgt im Rahmen der Personalisierung der Smartcards vor der Übergabe an den Endteilnehmer.
2. Erzeugung durch den Endteilnehmer selbst:
   In diesem Fall werden die Smartcards ohne Aktivierungsdaten personalisiert und den Endteilnehmern im Null-PIN-Status übergeben. Die Endteilnehmer müssen nach Erhalt und Prüfung der Unversehrtheit der Karte zur Aktivierung selbst PINs und PUKs setzen.

Die Passwörter der im PKCS#12-Format übergebenen Schlüssel von Softwarezertifikaten werden immer durch einen sicheren Zufallszahlengenerator der CA erzeugt.

6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten der HSMs sind nur Personen in vertrauenswürdigen Rollen bekannt, der Kreis der wissenden Personen ist dabei auf das unbedingt erforderliche Maß eingeschränkt.

Im Fall der Generierung von Aktivierungsdaten für Schlüssel der Endteilnehmer durch die CA werden diese bereits bei Antragstellung generiert und unmittelbar dem Antragsteller als PIN- bzw. Passwort-Brief in Form einer PDF-Datei über eine HTTPS-gesicherte Verbindung übergeben.

Im Fall der Generierung der Aktivierungsdaten durch die Endteilnehmer selbst sowie nach Erhalt der Aktivierungsdaten von der CA obliegt der Schutz der Aktivierungsdaten dem Endteilnehmer selbst gemäß den Nutzungsbedingungen.

6.4.3 Andere Aspekte der Aktivierungsdaten

Gemäß Kap. 6.4.1 können Smartcards der Endteilnehmer im Null-PIN-Status, d.h. ohne installierte Aktivierungsdaten, personalisiert und übergeben werden. In diesem Fall werden zum Schutz vor unbefugter Nutzung die Zertifikate direkt nach Ausstellung suspendiert. Erst nach Prüfung der Unversehrtheit der Smartcard (d.h. die Smartcards befindet ich weiterhin im Null-PIN-Status) wird die Suspendierung der Zertifikate durch den Endteilnehmer mittels eines antragsindividuellen, hinreichend langen und komplexen Freischalte-Passworts, welches nur dem Antragsteller bekannt ist, aufgehoben.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Telekom Security setzt ausschließlich vertrauenswürdige Systeme ein, welche die technische Sicherheit und Zuverlässigkeit der von den Systemen unterstützten Prozesse gewährleisten. Alle Systeme für das Zertifikatsmanagement sowie die Status- und Verzeichnisdienste werden im Risikomanagement des Trust Centers berücksichtigt und entsprechend ihrer Kritikalität bzw. dem Schadenspotenzial geschützt und dimensioniert.

Alle Systeme werden nach konzernweiten Vorgaben gehärtet, d.h. nicht benötigte Accounts, Dienste, Protokolle und Ports werden deaktiviert. Zudem werden die Systeme mit einem Integritätsschutz versehen, der vor Viren, sonstigem Schadcode und dem Einspielen unerlaubter Software schützt. Die Auslastung und verfügbare Ressourcen werden überwacht, um einen ununterbrochenen Betrieb zu gewährleisten. Diese und weitere Sicherheitsmaßnahmen sind in einem Sicherheitskonzept beschrieben.

Alle Systeme werden regelmäßig über einen Zeitserver mit exakten Zeitinformationen synchronisiert.

Die Administrationssysteme zur Umsetzung der Sicherheitsrichtlinien werden ausschließlich für diesen und keine anderen Zwecke verwendet.

Die geforderte Trennung von vertrauenswürdigen Rollen (siehe Kap. 5.2.4) wird von allen notwendigen Systemen technisch unterstützt. Insbesondere werden die Accounts der für den Betrieb der kritischen Systeme erforderlichen vertrauenswürdigen Rollen (siehe Kap. 5.2.1) so verwaltet, 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. Dies beinhaltet die Verwendung von personalisierten Accounts. Alle Accounts werden regelmäßig, mindestens aber alle drei Monate, überprüft und bei Bedarf in angemessener Zeit geändert oder gelöscht.

Accounts, welche direkt die Erstellung von Zertifikaten auslösen können, werden mit Multi-Faktor-Authentifizierung geschützt.

Die zur Zertifikatserzeugung und ggf. -sperrung erfassten Daten inkl. der Protokolldaten gemäß Kap. 5.5.1 werden so gesichert, dass deren Integrität, Vertraulichkeit und Verfügbarkeit über den gesamten Aufbewahrungszeitraum sichergestellt sind.

6.5.2 Sicherheitsbewertung von Computern

Keine Bestimmungen.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Steuerung der Systementwicklung

Telekom Security setzt Software renommierter Hersteller ein, welche die für die Entwicklung von IT-Sicherheitssystemen üblichen Sicherheitsmaßnahmen beachten und langjährige Erfahrung in diesem Umfeld aufweisen.

Die Release-Planung und Dokumentation erfolgt gemäß den Vorgaben des Releasemanagements. Neue Versionen der Software (geplante Updates) oder Fehlerbeseitigungen (kurzfristige Bugfixes) werden erst nach ausgiebiger Prüfung im Testsystem ins Wirksystem überführt. Nach Überführung ins Wirksystem erfolgen dort weitere Tests, um die Funktionsfähigkeit und Fehlerfreiheit zu überprüfen. Die Entwicklungs-, Test- und Produktivumgebungen werden auf unterschiedlicher Hardware in unterschiedlichen Netzsegmenten betrieben und sind daher gänzlich voneinander getrennt.

6.6.2 Maßnahmen des Sicherheitsmanagements

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

Alle Änderungen, die sich auf das festgelegte Sicherheitsniveau auswirken, werden zuvor vom Management und ggf. vom ISMS freigegeben.

Die Integrität der Systeme wird kontinuierlich auf Änderungen überwacht. Bei Änderungen, die nicht auf Basis eines autorisierten Change durchgeführt wurden, wird den daraus resultierenden Alarmmeldungen durch qualifiziertes Personal nachgegangen.

Systeme loggen, soweit möglich, alle in Kap. 5.4.1 genannten sicherheitsrelevanten Ereignisse.

Das Patchmanagement ist so geregelt, 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.

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

6.6.3 Sicherheitskontrollen während des Lebenszyklus

Keine Bestimmungen.

6.7 Netzwerk-Sicherheitskontrollen

Netze und Systeme werden mithilfe mehrstufiger Firewalls, IDS und IPS, Segmentierung sowie weiteren Schutzmaßnahmen vor unautorisierten Zugriffen und Angriffen geschützt. Die Segmentierung des Netzwerks basiert auf einer Risikobetrachtung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehungen zwischen vertrauenswürdigen Systemen und Diensten. Verbindungen sind so eingeschränkt, dass nur die zum Betrieb erforderlichen Verbindungen möglich sind, nicht benötigte Verbindungen werden explizit verboten oder deaktiviert. Die Netzwerke zur Administration der Systeme sind von den operativen Netzwerken separiert.

Alle für den CA-Betrieb kritischen Systeme sind in sicheren oder hochsicheren Zonen untergebracht. Innerhalb einer Zone gelten für alle Systeme die gleichen Mindestsicherheitsanforderungen.

Die Kommunikation ist grundsätzlich auf mehreren Schichten verschlüsselt und wird für alle vertrauenswürdigen Systeme über vertrauenswürdige Kanäle realisiert, die eine sichere Identifizierung ihrer Endpunkte gewährleisten.

Alle externen Netzanbindungen sind redundant aufgebaut.

Mindestens einmal je Quartal sowie, i.d.R. innerhalb einer Woche nach signifikanten System- oder Netzwerkänderungen erfolgt eine Schwachstellenprüfung an öffentlichen und privaten IP-Adressen.

Mindestens einmal pro Jahr sowie bei Inbetriebnahme oder signifikanten Änderungen an der Infrastruktur bzw. Anwendungen werden Penetrationstests durchgeführt.

Die zuvor genannten Schwachstellenscans und Penetrationstests werden von Personen oder Organisationen durchgeführt, die über die für eine zuverlässige Prüfung und Dokumentation erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung wird zusammen mit den Ergebnissen dokumentiert.

Nach Bekanntwerden einer kritischen Schwachstelle wird diese i.d.R., sofern es keine guten Gründe gibt, die Schwachstelle nicht zu beseitigen, innerhalb von 48 Stunden behoben. Sollte eine Behebung innerhalb von 48 Stunden nicht möglich sein, so wird ein Plan zur Minderung der Schwachstelle, inkl. einer Priorisierung der Aktivitäten, erstellt und in dem dort festgelegten Zeitraum abgearbeitet. Sollte entschieden werden, eine Schwachstelle nicht zu beheben, so wird die begründete Entscheidung dokumentiert.

6.8 Zeitstempel

Die von den Systemen der Zertifizierungsstelle protokollierten Ereignisse werden mit zuverlässigen Zeitinformationen versehen, die Systemzeiten werden regelmäßig über das Network Time Protocol (NTP) synchronisiert.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

Die aufgezeigten Zertifikatsprofile gelten für alle Zertifikate, die ab dem Gültigkeitsbeginn dieser CPS ausgestellt werden. Bereits ausgestellte Zertifikate mit älteren Profilen behalten ihre Gültigkeit, sofern nicht explizit auf deren Ungültigkeit hingewiesen wird (Bestandschutz).

Alle Zertifikatsprofile entsprechen dem [RFC5280] sowie den Empfehlungen der ITU-T X.509.

Alle Zertifikate erhalten eine unter der jeweiligen CA eindeutige Seriennummer, welche von einem kryptographisch sicherem Pseudo-Zufallszahlengenerator und mit einer Entropie von 50 Bit generiert werden.

7.1.1 Versionsnummer

Alle X.509-Zertifikate werden in der Version 3 ausgestellt.

7.1.2 Zertifikatserweiterungen

Endteilnehmer-Zertifikate enthalten folgende Zertifikatserweiterungen:

- **authorityKeyIdentifier:** enthält den subjectKeyIdentifier der ausstellenden CA
- **keyUsage:** (*kritisch*), enthält die Werte gem. [RFC5280] je nach Anwendungsfall
- **certificatePolicies:** siehe Kap. 7.1.6
- **subjectAltName:**
  - Alle Zertifikate: <E-Mail-Adresse>
  - Win-Logon-Zertifikat: zusätzlich <UPN>
  - Server-Zertifikat: zusätzlich optional 1-3 <DNS-Name> und/oder <IP-Adr.>
  - Domain-Controller-Zertifikat: zusätzlich <GUID>
- (optional) **extendedKeyUsage:** enthält die Werte gem. [RFC5280] je nach Anwendungsfall
- **cRLDistributionPoints:** enthält die HTTP-URL der zugehörigen CRL
- **authorityInfoAccess:** enthält die HTTP-URL des OCSP-Responders (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp))

7.1.3 Algorithmen-OID

Zur Signatur von Zertifikaten der V-PKI-CAs werden derzeit die folgenden Algorithmen verwendet:

- **sha256WithRSAEncryption:** OID 1.2.840.113549.1.1.11
- **sha512WithRSAEncryption:** OID 1.2.840.113549.1.1.13

Zur Kennzeichnung des Schlüssels werden folgende OIDs gesetzt:

- Zertifikate zu RSA-Schlüsseln enthalten in der subjectPublicKeyInfo:
  - **rsaEncryption:** OID 1.2.840.113549.1.1.1,
- Zertifikate zu EC-Schlüsseln enthalten in der subjectPublicKeyInfo:
  - **ecPublicKey:** OID 1.2.840.10045.2.1 und zusätzlich:
    - **secp256r1**: OID 1.2.840.10045.3.1.7 oder
    - **secp384r1**: OID 1.3.132.0.34 oder
    - **brainpoolP256r1**: OID 1.3.36.3.3.2.8.1.1.7.

7.1.4 Namensformen

Die Endteilnehmer-Zertifikate enthalten folgende Namensbestandteile im Subject-DN:

- **commonName:**
  - Personen-Zertifikate: <Name Titel Vorname>
  - Pseudonym-Zertifikate: <Pseudonym> :PN
  - Gruppen-/Funktionszertifikate: FKT: bzw. GRP: <Funktion>/<Gruppe>[6]
  - Zertifikate für IT-Prozesse: <DNS-Name> oder <IP-Adresse>
- **serialNumber:** Nr. zur Unterscheidung von Endteilnehmern mit gleichem <commonName>
- **emailAdress:** <E-Mail-Adresse>
- (optional) **localityName**: Ort des Zertifikatsnehmers
- **organizationUnitName (1)**: <Sub-Domäne>
- (optional) **organizationUnitName (2)**: <zusätzliche Angaben>
- (optional) **organizationUnitName (3)**: <zusätzliche Angaben>
- **organizationName**: <Master-Domäne>
- **country**: ausschließlich „DE“

[6] bisher wurde hierfür der Präfix „GRP:“ verwendet, zukünftig sollte auf „FKT:“ geschwenkt werden.

7.1.5 Namensbeschränkungen

Es werden keine Namensbeschränkungen gesetzt.

7.1.6 OIDs der Erweiterung „CertificatePolicies“

In den Endteilnehmer-Zertifikaten wird die OID 1.3.6.1.4.1.7924.1.1 (Certificate Policy der V-PKI) gesetzt.

7.1.7 Verwendung der Erweiterung „Policy Constraints“

Die Erweiterung „Policy Constraints“ wird nicht gesetzt.

7.1.8 Syntax und Semantik der „Policy Qualifier“

Der Policy Qualifier wird konform zum [RFC5280] mit den in Kap. 7.1.2 festgelegten Inhalten gesetzt.

7.1.9 Verarbeitungssemantik für die kritische Erweiterung „Certificate Policies“

Die Erweiterung „certificatePolicies“ wird nicht als kritisch markiert, so dass es im Ermessen der Zertifikatsnutzer liegt, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

Alle Sperrlisten werden gemäß den Anforderungen des [RFC5280] ausgestellt und werden von der jeweiligen CA selbst unter Anwendung der erlaubten Algorithmen gemäß Kap. 7.1.3 signiert.

7.2.1 Versionsnummer(n)

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

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Sperrlisten enthalten folgende CRL-Erweiterungen:

- AuthorityKeyIdentifier
- cRLNumber

Die Sperrlisteneintragserweiterung reasonCode wird unterstützt. Es werden die folgenden CRLReasons unterstützt:

- unspecified (0)
- keyCompromise (1)
- cACompromise (2)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- certificateHold (6)

7.3 OCSP-Profil

Alle OCSP-Antworten werden gemäß den Anforderungen des [RFC6960] ausgestellt und von einem delegierten OCSP-Signer signiert, dessen Zertifikat von der jeweiligen CA ausgestellt ist. Alle OCSP-Signer-Zertifikate enthalten die Erweiterung id-pkix-ocsp-nocheck. Von Sub-CAs ausgestellte OCSP-Signer-Zertifikate besitzen eine Gültigkeitsdauer von 1 Monat.

7.3.1 Versionsnummer(n)

Es wird OCSP in der Version 1 gemäß [RFC6960] eingesetzt.

7.3.2 OCSP-Erweiterungen

Die Erweiterung revocationReason wird analog zum reasonCode der Sperrlisten gesetzt (siehe Kap. 7.2.2).

8 AUDITS UND ANDERE BEWERTUNGSKRITERIEN

8.1 Häufigkeit und Art der Prüfungen

Es werden von externen Auditoren jährlich Audits gemäß Kap. 8.4 durchgeführt. Die Audit-Perioden schließen hierbei direkt aneinander an und bilden eine ununterbrochene Folge.

Durch interne Auditoren wird zudem stichprobenartig eine zufällige Auswahl von Registrierungsstellen geprüft

8.2 Identität/Qualifikation der Prüfer

Externe Prüfungen gemäß Kap. 8.4 werden von unabhängigen und vom BSI zugelassenen ISO-27001-Auditoren durchgeführt.

Interne Auditoren, welche die in Kap. 8.1 aufgeführten Aufgaben wahrnehmen, verfügen über langjährige Erfahrung sowie hinreichende Expertise in den Bereichen Auditierung, PKI-Technologien und -Prozesse.

8.3 Beziehung des Prüfers zur geprüften Stelle

Es werden ausschließlich externe Prüfer beauftragt, welche unabhängig von der Deutschen Telekom Security GmbH und dem Prüfgegenstand sind.

Für interne Auditoren wird die Rollentrennung gemäß Kap. 5.2.4 beachtet.

8.4 Abgedeckte Bereiche der Prüfung

Die V-PKI-CAs werden gemäß [TR3145] in der Version 1.1 wie folgt geprüft:

- initial: TR-03145-Audit (mit ISO27001 als Voraussetzung)
- danach: TR-03145-Audit alle 3 Jahre
- dazwischen: jährliche Überwachungsaudits

8.5 Maßnahmen infolge von Mängeln

Alle festgestellten Mängel werden schnellstmöglich, jedoch spätestens innerhalb der vom Prüfer festgelegten Fristen beseitigt.

8.6 Mitteilung der Ergebnisse

Die von externen Prüfern erstellten Audit-Berichte werden auf Anfrage der Root-CA bereitgestellt.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

Die Höhe der zu entrichtenden Entgelte für die Ausstellung, Erneuerung und Verwaltung von Zertifikaten ist in den jeweiligen Verträgen geregelt.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Es werden keine Entgelte für den Zugriff auf Zertifikate erhoben.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

Es werden keine Entgelte für den Zugriff auf Sperr- oder Statusinformationen erhoben.

9.1.4 Entgelte für andere Leistungen

Es werden keine anderen Leistungen angeboten, welche mit einer Erhebung von Entgelten verbunden sind.

9.1.5 Erstattung von Entgelten

Die Erstattung von Entgelten ist in den jeweiligen Verträgen geregelt.

9.2 Finanzielle Verantwortlichkeiten

9.2.1 Versicherungsschutz

Die Telekom Security verfügt über einen hinreichenden Betriebs- und Vermögenshaftpflichtversicherungsschutz.

9.2.2 Sonstige finanzielle Ressourcen

Die Telekom Security verfügt als 100%-Tochter der Deutschen Telekom AG über die finanzielle Stabilität und Ressourcen, die zu einem zu [TSCP], [VPKICP] und [TR3145] konformen Betrieb inkl. einer geplanten Einstellung gemäß Kap. 5.8 erforderlich sind.

9.2.3 Versicherungs- oder Garantiedeckung für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang an vertraulichen Informationen

Alle Informationen im Kontext der V-PKI-CAs gelten als vertrauliche Informationen, sofern sie nicht gemäß Kap. 9.3.2 explizit als nicht vertrauliche Informationen eingestuft wurden.

9.3.2 Umfang an nicht vertraulichen Informationen

Alle in Kap. 2.2 genannten Informationen sowie sämtliche Informationen in ausgestellten und veröffentlichten Zertifikaten werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Telekom Security unterliegt den konzernweiten Richtlinien der Deutsch Telekom AG zum Schutz vertraulicher Informationen. Alle Mitarbeiter der Telekom Security sind dazu verpflichtet, die Konzernvorgaben zum Umgang mit vertraulichen Informationen zu berücksichtigen und einzuhalten.

Auftragnehmer oder Dritte werden ebenfalls vertraglich zur Einhaltung der Vorgaben verpflichtet.

9.4 Schutz von personenbezogenen Daten

9.4.1 Datenschutzkonzept

Die Deutsche Telekom AG hat zur Einhaltung aller Vorgaben des Bundesdatenschutzgesetzes [BDSG] konzernweite Richtlinien zum Umgang mit personenbezogenen Daten festgelegt und analog zum Umgang mit vertraulichen Informationen (siehe Kap. 9.3.1) entsprechende Schutzklassen auch für personenbezogene Daten festgelegt.

Die Telekom Security erfasst grundsätzlich nur personenbezogene Daten, die zur Erbringung der Dienstleistung erforderlich sind und verwendet diese Daten für keine anderen Zwecke.

Zum Schutz der personenbezogenen Daten vor unerlaubter Verarbeitung und Verlust sowie zur Wahrung deren Integrität und Vertraulichkeit werden angemessene technische und organisatorische Maßnahmen getroffen, welche in einem regelmäßig revidierten Datenschutzkonzept festgelegt sind.

9.4.2 Als privat zu behandelnde Informationen

Es werden alle personenbezogenen Informationen, welche nicht in Zertifikatsinhalten oder anderweitig veröffentlicht wurden, als vertrauliche Informationen behandelt.

9.4.3 Nicht als privat zu behandelnde Informationen

Nicht als vertraulich geltende personenbezogene Informationen sind alle Informationen, die zur Leistungserbringung veröffentlicht werden müssen (bspw. Zertifikatsinhalte).

9.4.4 Verantwortung für den Schutz personenbezogener Informationen

Alle Mitarbeiter der Telekom Security sind dazu verpflichtet, die Konzernvorgaben sowie gesetzliche Regelungen zum Umgang mit personenbezogenen Informationen zu berücksichtigen und einzuhalten. Auftragnehmer oder Dritte werden ebenfalls vertraglich zur Einhaltung der Vorgaben verpflichtet.

9.4.5 Hinweis und Zustimmung zur Verwendung privater Informationen

Als privat geltende Informationen gemäß Kap. 9.4.2 werden ausschließlich nach Information und Zustimmung des Betroffenen verarbeitet.

9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

Die Telekom Security legt die als privat geltenden Informationen gemäß Kap. 9.4.2 im Rahmen eines Gerichts- oder Verwaltungsverfahrens offen, wenn die Offenlegung per Gesetz oder Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet wird oder zur Durchsetzung von Rechtsansprüchen dient.

9.4.7 Andere Umstände der Offenlegung von Informationen

Nicht anwendbar.

9.5 Urheberrecht

Es gelten die gesetzlichen Vorschriften.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Telekom Security als Zertifizierungsstelle

Telekom Security sichert einen zuverlässigen, vertrauenswürdigen, diskriminierungsfreien und legalen Betrieb der Dienstleistung sowie die Einhaltung der Konformität zu [TSCP], [VPKICP] und [TR3145] zu.

Die den Endteilnehmern angebotenen Dienste und Produkte werden soweit möglich auch Menschen mit Behinderungen zugänglich gemacht. Sollten Maßnahmen nicht ausreichen, bietet das Trust Center zusätzlich einen kostenlosen telefonischen Support an, um Menschen mit Behinderungen bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten zu unterstützen.

Telekom Security trägt die Gesamtverantwortung für die Einhaltung der Konformität zu [TSCP], [VPKICP] und [TR3145]. Um sicherzustellen, dass auch die in die Identifizierungs-, Registrierungs- und Sperr-Prozesse eingebundenen externen Registrierungsstellen konform arbeiten, schließt Telekom Security mit den RAs entsprechende RA-Vereinbarungen ab, in denen die Aufgaben, Verantwortlichkeiten und Haftungsbedingungen der RAs festgelegt sind. Darüber hinaus stellt Telekom Security den RAs Handbücher zur Verfügung, in denen die Verfahrensweisen beschrieben sind.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Telekom Security sichert für ihre RAs die Umsetzung der in diesem Dokument beschriebenen Vorgehensweisen und Maßnahmen zu. Dazu zählen unter anderem:

- Antragsbearbeitung gemäß Kap. 4, z.B.:
  - Durchführung der Identifizierung und Authentifizierung der Antragsteller von Zertifikats-, Erneuerungs-, Änderungs- oder Sperranträgen
  - Genehmigung oder Ablehnung von Anträgen
- Organisatorische Maßnahmen gemäß Kap. 5.2, z.B.:
  - Etablierung vertrauenswürdiger Rollen
  - Bereitstellung hinreichender Personalressourcen
  - Unabhängigkeit des Personals
- Personelle Maßnahmen gemäß Kap. 5.3, z.B.:
  - Einsatz von vertrauenswürdigem und zuverlässigen Personal
  - Sicherstellung der Qualifikation des Personals durch initiale Schulungen bei Aufnahme der Tätigkeit sowie regelmäßige Widerholungsschulungen
  - Sanktionierung bei unbefugten Handlungen
- Archivierung der relevanten Unterlagen gemäß Kap. 5.5.
- Technische Maßnahmen gemäß Kap. 6.5, z.B.:
- hinreichender Schutz der in den RAs verwendeten technischen Systeme
- restriktives Accountmanagement der RA-Mitarbeiter

Die externen RAs verpflichten sich mit Unterzeichnung der RA-Vereinbarungen (siehe Kap. 9.6.1), alle o.g. Vorgehensweisen und Maßnahmen, sofern anwendbar, ebenfalls umzusetzen, Details werden in den RA-Vereinbarungen geregelt.

9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsnehmer

Die Zusicherungen und Gewährleistungen der Zertifikatsnehmer sind in den „Nutzungsbedingungen V-PKI-CAs“ festgelegt, welche die Telekom Security im Repository veröffentlicht (siehe Kap. 2.2).

Die Zertifikatsnehmer müssen die Akzeptanz der Nutzungsbedingungen vor Ausstellung der Zertifikate bestätigen (siehe Kap. 4.1.2).

Sofern sich neue Versionen der Nutzungsbedingungen auch auf die Akzeptanz des Dienstes für bestehende Zertifikate auswirken, werden alle Zertifikatsnehmer mit aktiven Zertifikaten über die Veröffentlichung der neuen Version informiert und es wird eine angemessene Frist zur Ablehnung der neuen Nutzungsbedingungen gesetzt.

Sollte innerhalb dieser Frist keine Ablehnung eingereicht werden, so gelten die neuen Nutzungsbedingungen als akzeptiert. Eine Ablehnung der neuen Nutzungsbedingungen hat die Sperrung der betroffenen Zertifikate zur Folge.

9.6.4 Zusicherungen und Gewährleistungen der Zertifikatsnutzer

Es existieren keine vertraglichen Vereinbarungen mit Zertifikatsnutzern. In den Nutzungsbedingungen sind jedoch Empfehlungen an die Zertifikatsnutzer enthalten, um die Vertrauenswürdigkeit eines Zertifikats für den jeweiligen Anwendungsfall zu überprüfen.

9.6.5 Zusicherungen und Gewährleistungen sonstiger Teilnehmer

Keine Bestimmungen.

9.7 Gewährleistungsausschlüsse

Etwaige Gewährleistungsausschlüsse werden in den Nutzungsbedingungen geregelt.

9.8 Haftungsbeschränkungen

Die Telekom Security haftet als TSP gemäß Artikel 13 der EU-Verordnung 910/2014 [eIDAS] für alle einer natürlichen oder juristischen Person vorsätzlich oder fahrlässig zugefügten Schäden.

Etwaige Haftungsbeschränkungen gemäß geltendem Recht werden in den Nutzungsbedingungen geregelt.

9.9 Schadensersatz

Etwaige Schadenersatzansprüche gegenüber der Telekom Security werden in den Nutzungsbedingungen geregelt.

9.10 Laufzeit und Aufhebung dieses CPS

9.10.1 Laufzeit

Dieses CPS gilt ab dem auf dem Deckblatt angegebenen Gültigkeitsdatum und hat eine Laufzeit von maximal einem Jahr (siehe dazu auch Kap. 9.12).

9.10.2 Aufhebung

Die Gültigkeit dieses Dokuments wird mit Inkraftsetzung einer neuen Version aufgehoben.

9.10.3 Wirkung einer Aufhebung und Fortführungen

Keine Bestimmungen.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Bestimmungen.

9.12 Änderungen an dieser CPS

9.12.1 Verfahren für Änderungen

Dieses CPS wird aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, mindestens aber jährlich einem Review unterzogen. Dazu überprüft das Compliance-Team des Trust Centers regelmäßig die zugrundeliegenden Anforderungen der in [TSCP#Anhang B] referenzierten Anforderungsquellen auf neue Versionen und verfolgt relevante Foren und Mailing-Listen.

Änderungen an diesem CPS sowie der jährliche Review werden in der Änderungshistorie dieses Dokuments aufgeführt und es wird eine neue Versionsnummer vergeben, auch wenn es im Rahmen der jährlichen Reviews zu keinerlei inhaltlichen Änderungen kam. Die Freigabe neuer Versionen geschieht gemäß Kap. 1.5.4.

Bei Änderungen, welche sich auf die Nutzungsbedingungen auswirken, werden diese entsprechend angepasst und in einer neuen Version bereitgestellt.

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Neue Versionen dieses CPS und der Nutzungsbedingungen werden gemäß Kap. 2 veröffentlicht. Alle RAs sowie die Root-CA werden über die Veröffentlichung neuer Versionen informiert.

9.12.3 Umstände, unter denen der OID geändert werden muss

Wenn sich Änderungen an diesem CPS ergeben, welche sich auf die Anwendbarkeit auswirken, so wird eine neue OID vergeben.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze eine Einigung herbei.

9.14 Geltendes Recht

Es gilt deutsches Recht.

9.15 Einhaltung geltenden Rechts

Die Telekom Security sichert zu, geltendes Recht einzuhalten.

9.16 Verschiedene Bestimmungen

9.16.1 Gesamte Vereinbarung

Keine Bestimmungen.

9.16.2 Zuordnung

Keine Bestimmungen.

9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieses CPS unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen dieser Erklärung nicht.

9.16.4 Rechtsdurchsetzung

Keine Bestimmungen.

9.16.5 Höhere Gewalt

Telekom Security ist nicht verantwortlich für Verzögerungen oder Nichterfüllung von Verpflichtungen gemäß dieser CPS, wenn die Ursache hierfür außerhalb der Kontrolle von Telekom Security liegt.

9.17 Sonstige Bestimmungen

Keine Bestimmungen.

A Anhang

A.1 Referenzen

[BDSG] Deutscher Bundestag: „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)“

[eIDAS] Europäisches Parlament, Rat der Europäischen Union: „Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“

[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[SOGIS] SOG-IS Crypto Working Group: SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms

[TSCP] Deutsche Telekom Security GmbH: “Trust Center Certificate Policy”

[TR2102-1] Bundesamt für Sicherheit in der Informationstechnik: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“

[TR3145] Bundesamt für Sicherheit in der Informationstechnik: „Technische Richtlinie TR-03145-1, Secure CA operation, Part 1, Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high'

[VPKICP] Bundesamt für Sicherheit in der Informationstechnik: Certificate Policy - Root-CA der PKI-1-Verwaltung

[X500] ITU Telecommunication Standardization Sector: “ITU-T X.500 Serie / ISO/IEC 9594, Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services”