Deutsche Telekom Security GmbH
Certification Practice Statement Public

Version: 06.00

Gültig ab: 01.09.2023

Status: Freigegeben

Letztes Review: 30.08.2023

ÄNDERUNGSHISTORIE

Tabelle 1: Änderungshistorie

Version	Stand	Änderungen / Kommentar
01.00	24.09.2021	Initialversion nach RFC 3647 Struktur, Beinhaltet die Ausgabe von Domain-validierten TLS-Zertifikaten
02.00	15.03.2022	Aufnahme neues CA-Zertifikat
03.00	13.08.2022	Erweiterung um OV, Generelle Überarbeitung
04.00	10.01.2023	Erweiterung um ▪ EV und QEVCP-w (ersetzt CPS Server.ID), ▪ S/MIME gemäß LCP und NCP (ersetzt den Anteil der öffentlichen Zertifikate der CPS cPKI und CPS Business.ID), ▪ Root-CPS (ersetzt Telekom Security CPS Root), generelle Überarbeitung
05.00	20.06.2023	Aufnahme neuer CA-Zertifikate und des neuen qualifizierten VDA Deutsche Telekom Security GmbH für QWAC, Entfernen der Methode 3.2.2.4.2, diverse Korrekturen
06.00	01.09.2023	Aufnahme S/MIME BR, neue CA Zertifikate

INHALTSVERZEICHNIS

Tabellenverzeichnis

1 EINLEITUNG

1.1 Überblick

Die Deutsche Telekom Security GmbH (vormals T-Systems International GmbH, nachfolgend Telekom Security genannt) betreibt in ihrem Trust Center als Vertrauensdiensteanbieter (Trust Service Provider (TSP[1])) verschiedene Stammzertifizierungsstellen (Root Certification Authorities, Root-CAs) sowie untergeordnete Zertifizierungsstellen (Subordinate Certification Authorities, Sub-CAs) für die Ausgabe von Zertifikaten an Kunden als auch Mitarbeiter des Konzerns Deutsche Telekom AG.

Die Deutsche Telekom AG ist als qualifizierter Vertrauensdiensteanbieter gemäß [eIDAS] zur Ausstellung von Zertifikaten für qualifizierte Signaturen (QES) zugelassen. Die Deutsche Telekom Security GmbH und T-Systems International GmbH sind als qualifizierte Vertrauensdiensteanbieter gemäß [eIDAS] zur Ausstellung von qualifizierten Website-Zertifikaten zugelassen.

Bei dem vorliegenden Dokument handelt es sich um das Certification Practice Statement (CPS) zur Ausstellung öffentlicher Zertifikate durch die Vertrauensdienste (Trust Services) "Business.ID", "Server.ID" und "cPKI" (Corporate PKI der Deutschen Telekom). Es beschreibt in der Struktur des [RFC3647] die Einhaltung und die Umsetzung der Anforderungen aus

- der Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42) [TSCP],
- ETSI EN 319 401,
- ETSI EN 319 411-1,
- ETSI EN 319 411-2,
- den aktuellen Versionen der folgenden unter http://www.cabfourm.org veröffentlichten Dokumente des CA/Browser Forums:
  - “CA/Browser-Forum Baseline Requirements“ [BR]
  - “CA/Browser-Forum EV-Guidelines“ [EVCG],
  - “CA/Browser-Forum Network and Certificate System Security Requirements“ [NCSSR],
  - “CA/Browser-Forum S/MIME Baseline Requirements” [SBR],
- diversen Root Store Policies (u.a. Mozilla [MOZRP], Microsoft [MSRP], Google [GCRP], Apple [APLRP] etc.).

Anwendbare Policies gemäß ETSI sind in Abhängigkeit von den Trust Services:

- DVCP, OVCP, EVCP und QEVCP-w für von Server.ID ausgestellte TLS-Zertifikate
- OVCP für TLS-Zertifikate, die von Business.ID ausgestellt wurden
- NCP für von Business.ID ausgestellte S/MIME-Zertifikate
- LCP für von cPKI ausgestellte S/MIME-Zertifikate

Anwendbare Nutzungsbedingungen (Terms of Use, TOU) sind in Abhängigkeit von den Trust Services:

- Nutzungsbedingungen Public [TOUP] für Server.ID und Business ID
- Nutzungsbedingungen Corporate PKI [TOUC] für cPKI

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

Anmerkung: Die in diesem Dokument getroffenen Aussagen gelten grundsätzlich für alle Zertifikate im Geltungsbereich dieser CPS. Einzelne Aussagen, die nur für bestimmte Zertifikatstypen gelten, sind durch Angabe des Zertifikatstyps ([TLS] oder [SMIME]) oder die anwendbare Policy ([DVCP], [OVCP], [EVCP], [QEVCP-w], [LCP] oder [NCP]) in eckigen Klammern gekennzeichnet.

[1] Nachfolgend werden in diesem Dokument die international gebräuchlichen, d.h. englischen Begriffe verwendet

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument trägt den Namen „Telekom Security CPS Public“ und wird durch die OID 1.3.6.1.4.1.7879.13.43 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 Public (43)}

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

Die in den folgenden Tabellen aufgeführten CA-Zertifikate liegen im Geltungsbereich dieser CPS.

Hinweis: Mit den seit 2020erstellten Root CAs wird der Aufbau von dedizierten PKI-Hierarchien für TLS sowie S/MIME verfolgt (noch nicht aktiv).

Tabelle 2: Root-CA-Zertifikate im Geltungsbereich dieser CPS

commonName	Issued	Fingerprint (SHA1)
Telekom Security TLS RSA Root 2023	2023-03-28	54d3acb3bd5756f6859dcee5c321e2d4ad83d093
Telekom Security SMIME RSA Root 2023	2023-03-28	893f6f1ce24d7ffbc3d3147a0580a7dee10a5e4d
Telekom Security SMIME ECC Root 2021	2021-03-18	b7f91d98ec2593f35014849aa87e22103cc43927
Telekom Security TLS ECC Root 2020	2020-08-25	c0f896c5a93b01062107da184248bce99d88d5ec
T-TeleSec GlobalRoot Class 3	2008-10-01	55a6723ecbf2eccdc3237470199d2abe11e381d1
T-TeleSec GlobalRoot Class 2	2008-10-01	590d2d7d884f402e617ea562321765cf17d894e9

Tabelle 3: Sub-CA-Zertifikate im Geltungsbereich dieser CPS

commonName	Issued	Fingerprint (SHA1)
Sub-CA-Zertifikate unter Telekom Security TLS RSA Root 2023		
Telekom Security EV RSA CA 23	28.03.2023	3e5248d06f0e34c4cd124a6e393233a238c44ab5
Sub-CA-Zertifikate unter Telekom Security SMIME RSA Root 2023		
Telekom Security SMIME RSA CA 23	28.03.2023	30c9fa9126455d4a3b43b876f40cf98fb611b7f6
Sub-CA-Zertifikate unter Telekom Security SMIME ECC Root 2021		
Telekom Security SMIME ECC CA 23	28.03.2023	dac817d71e6d20353384a6105560949145f31703
Sub-CA-Zertifikate unter Telekom Security TLS ECC Root 2021		
Telekom Security EV ECC CA 21	2021-04-21	165410be38f2c72b0c6a9ccf4de23c30f4633f48
Sub-CA-Zertifikate unter T-TeleSec GlobalRoot Class 3 ***(verwendet für [EVCP] und [QEVCP-w])***		
Telekom Security EV RSA CA 23A	2023-06-20	7764444bd25ed088f8fe060d1ea97872787365cf
Telekom Security ServerID EV Class 3 CA	2022-08-02	1aec57ea7253836cc7e8f561cc417adb5187e322
Telekom Security EV RSA CA 22	2022-06-21	578fc66913edC923f12df29c5993e6f25f9965dc
TeleSec ServerPass Extended Validation Class 3 CA	2014-02-11	c6d43f5978e02e1fc64cf6fa94ac4b4d3adc8593
Sub-CA-Zertifikate unter T-TeleSec GlobalRoot Class 2 ***(verwendet für [DVCP], [OVCP], [LCP] und [NCP])***		
Deutsche Telekom AG secure email CA E05	2023-08-09	afa8c6adf4842282ac3cdaf5b73774de3bc7b851
Telekom Security BusinessID SMIME CA 2023	2023-06-20	ed1f89f54b6953f05ee3ee76e53bcdf5a8c0e9bf
Deutsche Telekom AG secure email CA E04	2023-06-20	87c10bb432162aa03a17771519926d987d0ba5fa
Telekom Security ServerID OV Class 2 CA	2022-08-02	52869cef1a2195c416820c183b80c995bbbfbedc
TeleSec Business TLS-CA 2022	2022-06-21	075c5ad1ac3d5c0084bd29e8f266ab005f2b1994

Telekom Security OV RSA CA 22	2022-06-21	32cd823131f8abb068fa70e2f495ad9fbc89afa4
Telekom Security DV RSA CA 22	2022-02-22	01648268a45f9e0990acb5d391ad1876ccee0bed
TeleSec Business TLS-CA 21	2021-11-17	3a14e80766ad27dfaddce96a65195ccf874d91de
TeleSec Business CA 21	2021-11-17	2aeb1f8bf421d9ce2d54b05739800a0d031f2115
TeleSec Business TLS-CA 2021	2021-11-17	cce862ff3f6adeb1236666bab173d847c1b2df11
TeleSec Business CA 2021	2021-11-17	da389f6a255ef91f98fdd895159c7b152fe6d8fe
Telekom Security DV RSA CA 21	2021-04-21	99cc84f820818cf0eefe81ddf572cace4b3acb78
Deutsche Telekom AG secure email CA E03	2020-07-09	75c18d78fd56d2ed539f8b000e5d6c8b697e5bee
TeleSec ServerPass Class 2 CA	2014-02-11	7bc0048a1fd8f4238cccc9cc566dd38bff7e67e2
TeleSec Business CA 1	2012-11-29	57a8c5b5260e206353d4c346e3f60939e4f8b859

1.3.2 Registrierungsstellen (Registration Authorities, RA)

In Abhängigkeit vom Trust Service werden die Zertifikatsnehmer

- durch das Trust Center selbst (Server.ID),
- durch externe / Enterprise RAs (Business.ID) oder
- durch eine interne Enterprise RA der Deutschen Telekom (cPKI)

registriert.

Externe RAs sind vertraglich gebunden und durch technische Maßnahmen, u.a. auf bereits validierte Zertifikatsinhalte, so weit wie möglich eingeschränkt. Die Validierung der Kontrolle von Domains (einschließlich E-Mail-Domains für [SMIME]) und IP-Adressen wird jedoch nicht an externe RAs delegiert.

[EVCP], [QEVCP-w] Auch die Validierung von Zertifikatsanträgen wird nicht delegiert.

1.3.3 Zertifikatsnehmer

Hinweis: Aufgrund der teilweise unterschiedlichen Verwendung von Begriffen in den referenzierten Dokumenten werden die in diesem Dokument verwendeten Begriffe im Folgenden beschrieben.

Zertifikatsnehmer im Sinne dieses CPS sind Organisationen oder natürliche Personen, die in Verbindung mit einer Organisation identifiziert werden, welche Zertifikate von den oben genannten Trust Services beziehen und die durch die Akzeptanz der Nutzungsbedingungen rechtlich gebunden sind.

Organisationen im Sinne dieses CPS sind juristische Personen oder Organisationseinheiten, die in Verbindung mit einer juristischen Person identifiziert werden.

Organisationen können sein:

- Private Organisation (Private Organization):
  Eine nichtstaatliche juristische Person, deren Existenz durch eine Anmeldung bei oder einen Akt der Gründungsbehörde oder einer gleichwertigen Stelle begründet wurde
- Öffentliche Organisation (Government Entity):
  Eine von einer Regierung betriebene juristische Person, Behörde, Abteilung oder andere damit verbundene Organisationseinheiten
- Nicht-gewerbliche Organisationen (Non-commercial Entity):
  Internationale Organisationen, die im Rahmen einer Charta, eines Abkommens, einer Konvention oder eines gleichwertigen Instruments geschaffen wurden, welche(s) von oder im Namen von mehr als einer Regierung eines Landes unterzeichnet wurde
- Sonstige gewerbliche Organisationen (Business Entity):
  Organisationen, die nicht zu den zuvor genannten Organisationstypen zählen

[EVCP], [QEVCP-w] Ausschließlich Organisationen der DACH-Region (Deutschland, Österreich, Schweiz) werden als Zertifikatsnehmer akzeptiert.

Subjekt eines Zertifikats im Sinne dieses CPS ist der im Zertifikat in den Attributen des „Subject Distinguished Name“ oder der Erweiterung „subjectAltName“ benannte Anwender des privaten Schlüssels.

Subjekte können

- natürliche Personen, die in Verbindung mit einer Organisation stehen,
- Organisationen oder
- Geräte, die von oder im Namen einer natürlichen Person oder Organisation betrieben werden,

sein.

Antragsteller im Sinne dieses CPS sind die Personen, welche die Anträge bei den Trust Services einreichen. Es handelt sich dabei immer um natürliche Personen, die

- der Zertifikatsnehmer und/oder das Subjekt selbst,
- ein Vertretungsberechtigter des Zertifikatsnehmers (im Falle einer Organisation) oder
- eine andere, vom Zertifikatsnehmer beauftragte Person

sein können.

[EVCP] Ergänzend zum Antragsteller sind folgende Rollen implementiert:

- Antragsunterzeichner: Eine natürliche Person, die ausdrücklich befugt ist, den Zertifikatsnehmer zu vertreten und in dessen Namen Zertifikatsanträge zu unterzeichnen.
- Antragsgenehmiger: Eine natürliche Person, die ausdrücklich befugt ist, den Zertifikatsnehmer zu vertreten, und in dessen Namen Zertifikatsanträge zu genehmigen.

Anmerkung: Es darf eine Person mit mehreren der aufgeführten Rollen betraut werden und die Rollen dürfen mit mehreren Personen besetzt werden.

1.3.4 Vertrauende Dritte

Vertrauende Dritte sind Personen, Systeme oder IT-Prozesse, welche den unter dieser CPS ausgestellten Zertifikaten vertrauen.

1.3.5 Andere Teilnehmer

Keine Bestimmungen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Endteilnehmerzertifikate dürfen nur für die folgenden Anwendungen verwendet werden:

- [DVCP], [OVCP]: TLS-Server und Client-Authentifizierung von TLS-Servern.
- [EVCP], [QEVCP-w]: TLS-Server-Authentifizierung von Webservern.
- [SMIME]: Verschlüsselung und/oder Signatur von E-Mails, Dateien oder anderen Daten, sowie ggf. Client-Authentifizierung.

Die Anwendung muss den in den Zertifikaten in den Attributen keyUsage und extendedKeyUsage definierten Schlüsselverwendungen entsprechen.

[TLS] Zertifikate dürfen ausschließlich auf Servern installiert werden, die unter den im subjectAltName gelisteten Domainnamen oder IP-Adressen erreichbar sind.

[EVCP] Zertifikate dürfen ausschließlich auf Webservern installiert werden.

1.4.2 Unzulässige Verwendung von Zertifikaten

Eine Verwendung von Zertifikaten entgegen der in Kapitel 1.4.1 genannten Szenarien ist nicht zulässig.

Sämtliche Zertifikate sind nicht für die Verwendung in Steuerungs- und Kontrolleinrichtungen in gefährlichen Umgebungen oder Umgebungen, in denen ein ausfallsicherer Betrieb gewährleistet sein muss und ein Ausfall zu Schäden wie Personenschäden, Tod, mittleren und schweren Umweltschäden, sonstige Katastrophen führen kann, vorgesehen, ausgelegt oder zugelassen. Hierzu gehören nukleare Einrichtungen, Flugzeugnavigations- oder -kommunikationssysteme, Luftverkehr-Kontrollsysteme, Waffenkontrollsysteme etc.

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 diese CP ist das PKI Compliance Management des Trust Centers, welches per E-Mail unter trustcenter-roots@telekom.de zu erreichen ist.

Zertifikatsmissbräuche, Schlüsselkompromittierungen, fehlerhafte bzw. nicht-konforme Zertifikate, andere sicherheitsrelevante Zertifikatsprobleme oder der Verdacht auf solche Vorfälle können an diese E-Mail-Adresse gesendet werden. Bezüglich der Meldung von Schlüsselkompromittierungen sind die Instruktionen gemäß Kapitel 4.9.12 zu berücksichtigen.

1.5.3 Person für die Feststellung der Konformität dieser CPS zur CP

Zuständig für die Feststellung der Konformität dieser CPS zur [TSCP] ist das PKI Compliance Management des Trust Centers. Für Kontakte siehe Kap. 1.5.2.

1.5.4 Genehmigungsverfahren dieses CPS

Jede Version dieses CPS wird nach Feststellung der Konformität zur [TSCP] vom Management des Trust Centers freigegeben und behält seine Gültigkeit für neu ausgestellte Zertifikate sowie für bereits bestehende Zertifikate, bis sie widerrufen oder durch eine neue Version ersetzt wird.

1.6 Definitionen und Abkürzungen

Siehe [TSCP#1.6] bzgl. Definitionen, Abkürzungen und Verweisen. Darüber hinaus wird in diesem CPS auf die folgenden Dokumente verwiesen:

[TSCP] Deutsche Telekom Security GmbH, Trust Center Certificate Policy
[TOUP] Deutsche Telekom Security GmbH, Nutzungsbedingungen Public

[TOUC] Deutsche Telekom Security GmbH, Nutzungsbedingungen cPKI (Corporate PKI Deutsche Telekom)

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

Die Telekom Security betreibt ein Repository mit Informationen und Dokumenten (siehe Kap. 2.2) sowie Zertifikatsstatusdienste (siehe insbesondere Kap. 4.9 bzw. 4.10). Darüber hinaus werden diverse (LDAP-)Verzeichnisse für dedizierte Zwecke bereitgestellt.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Telekom Security betreibt ein PKI-Repository (https://www.telesec.de/de/service/downloads/pki-repository/), in dem sowohl aktuelle als auch abgelöste Versionen der folgenden Informationen und Dokumente veröffentlicht werden:

- Telekom Security CP [TSCP]
- Certification Practice Statements (CPS, beinhaltet sowohl dieses Dokument als auch die abgelösten CPS)
- Nutzungsbedingungen Public [TOUP]
- Allgemeine Geschäftsbedingungen (AGB)
- PKI Disclosure Statements (PDS)
- alle im Geltungsbereich dieser CPS befindlichen CAs
- Audit Bescheinigungen zu öffentlichen Root-CA-Zertifikaten der Telekom Security (Verlinkung zu den offiziellen Web-Seiten des Auditors)
- Leistungsbeschreibungen

Diese CPS Public wird in deutscher und englischer Sprache veröffentlicht. Die deutschen und englischen Versionen haben immer die gleiche Versionsnummer und werden inhaltlich synchronisiert. Im Streitfall ist jedoch die deutsche Version autoritativ.

Es werden alle erforderlichen Informationen zu CA-Zertifikaten in der „Common CA Database“ (CCADB) gemäß der CCADB-Policy [CCADB] (siehe https://www.ccadb.org) gepflegt.

Zu allen Root-CAs, unter denen TLS-Server-Zertifikate ausgestellt werden, werden jeweils Test-Web-Seiten mit einem gültigen, einem abgelaufenen und einem gesperrten TLS-Server-Zertifikat betrieben. Bei Root-CAs, unterhalb denen auch EV-Zertifikate ausgestellt werden, sind dies EV-Zertifikate. Die Links zu den Test-Webseiten einer jeden Root-CA können auf der Webseite des Trust Centers eingesehen werden (https://telesec.de/en/root-program/informations-about-ca-certificates/root-certificates/).

[TLS] Alle Zertifikate werden vor ihrer endgültigen Ausstellung in Form von „Pre-Zertifikaten“ in einer den Anforderungen genügenden Anzahl CTLogs veröffentlicht.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Neue Versionen dieser CPS werden mindestens jährlich sowie zusätzlich bei Bedarf im oben genannten Repository vor Inkrafttreten veröffentlicht.

Neue CA-Zertifikate im Geltungsbereich dieses CPS werden innerhalb von 7 Tagen nach ihrer Ausstellung und in jedem Falle vor Inbetriebnahme sowohl in der CCADB als auch im Repository veröffentlicht.

Audit Bescheinigungen werden innerhalb von 7 Tagen nach ihrer Ausstellung sowohl in der CCADB als auch im Repository veröffentlicht bzw. verlinkt.

2.4 Zugang zu den Verzeichnissen

Die in Kapitel 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 alle Zertifikate die Namen der Zertifikatsinhaber in Form eines Distinguished Names (subjectDN) gemäß [X500] und, im Falle von Endteilnehmerzertifikaten, in Form eines subjectAltName aufgenommen. Siehe Kapitel 7.1.4 für Details.

3.1.2 Aussagekraft von Namen

Alle CA-Zertifikate erhalten einen commonName, welcher einen gebräuchlichen Namen der jeweiligen Organisation der Deutschen Telekom bzw. dem DFN beinhaltet und die Zugehörigkeit zur Organisation unmissverständlich wiedergibt.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Wenn für einen Zertifikatstyp die Verwendung von Pseudonymen erlaubt ist, müssen die Pseudonyme so gewählt werden, dass eine Verwechslung mit existierenden Namen natürlicher Personen oder Organisationen vermieden wird.

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

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

Unter einer CA ausgestellte Zertifikate sind hinsichtlich der Zuordnung von subjectDN und Zertifikatsnehmer eindeutig, d.h. ein subjectDN wird nicht an unterschiedliche Zertifikatsnehmer vergeben. Sollten die Inhalte des subjectDN von mehreren Zertifikatsnehmern übereinstimmen, so werden weitere Identifier hinzugenommen, um Eindeutigkeit der subjectDN herzustellen.

Ausgenommen von dieser Regel sind domainvalidierte Zertifikate. Ein subjectDN kann in diesem Fall einem neuen Zertifikatsnehmer zugeordnet werden, wenn dieser die Kontrolle über die Domain nachgewiesen hat.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Markennamen, Markenzeichen und DBAs werden nicht unterstützt.

3.2 Initiale Validierung der Identität

Zur initialen Validierung der Identität einer natürlichen Person oder Organisation werden ausschließlich direkte Nachweise oder Bescheinigungen von angemessenen und autorisierten Quellen verwendet. Die

Nachweise können dabei in Papierform oder elektronisch erfasst werden und 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.

In den folgenden Kapiteln werden die angewandten Methoden selbst beschrieben. Welche Methoden im Kontext einer Policy verwendet werden, wird in Kapitel 4.2.1 beschrieben.

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Sofern der Schlüssel vom Antragsteller generiert wird, ist für den Besitznachweis ein mit dem privaten Schlüssel signierter PKCS#10-Request notwendig, welcher mindestens den im Attribut commonName aufzunehmenden Namen enthält.

3.2.2 Authentifizierung der Organisationsidentität

Die folgenden Methoden werden gemäß Kapitel 4.2.1 zur Validierung der Organisationsidentität verwendet.

QGIS – Qualified Government Information Source: Die rechtliche, physische und betriebliche Existenz und Identität einer Organisation werden über staatlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert. Beispiele für QGIS sind Handelsregister, berufsständige Körperschaften öffentlichen Rechts und das Bundeszentralamt für Steuern. Für eine Prüfung werden die vom Antragsteller bereitgestellten Informationen für eine automatisierte oder manuelle Suche in den entsprechenden Registern verwendet. Daraus resultierende Ergebnisse werden mit den bereitgestellten Informationen abgeglichen. Die für die Validierung verwendeten Quellen („Incorporation and Registration Agencies“) werden im Repository (https://telesec.de/de/service/downloads/pki-repository/) unter „Validation Resources“ veröffentlicht.

QIIS – Qualified Independent Information Source: Die rechtliche, physische und betriebliche Existenz und Identität einer Organisation werden über privatrechtlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert. Diese Quellen werden hinsichtlich ihrer Zuverlässigkeit evaluiert, bevor sie von Telekom Security als QIIS eingestuft werden. Beispiele für QIIS sind Wirtschaftsauskunftsdienste wie z.B. Dun&Bradstreet oder GLEIF. Für eine Prüfung werden die vom Antragsteller bereitgestellten Informationen automatisiert oder manuell mit der QIIS-Datenbank abgeglichen.

Attestation: Der Antragsteller weist die rechtliche, physische und betriebliche Existenz und Identität einer Organisation durch Vorlage eines durch einen Notar ausgestellten Bescheinigungsschreiben (Verified Professional Letter gemäß [EVCG]) oder durch Vorlage einer amtlichen Beglaubigung nach. Voraussetzung für die Akzeptanz eines notariellen Nachweises ist, dass der Notar in einem entsprechend anerkannten Notarverzeichnis geführt wird.

Onsite: Antragstellende Organisationen werden im Rahmen einer Vorort-Besichtigung durch Mitarbeiter der CA oder RA identifiziert.

OrgDB: Enterprise RAs von antragstellenden Organisationen können relevante organisationsinterne Zertifikatsdaten, bspw. Gerätekennungen, Namen organisatorischer Einheiten etc. aus einer zuverlässigen internen Datenbank oder vergleichbarer Datenquelle entnehmen. Die Datenquelle muss entsprechend geschützt und gepflegt werden, um die Korrektheit der Daten zu gewährleisten.

3.2.3 Authentifizierung von natürlichen Personen

Die folgenden Methoden werden gemäß Kapitel 4.2.1 zur Validierung der Identität natürlicher Personen verwendet.

PersIdent: Natürliche Personen werden anhand eines amtlichen Ausweises durch eine RA (intern/extern) persönlich identifiziert.

PostIdent: Natürliche Personen werden anhand eines amtlichen Ausweises über die Dienstleistung „PostIdent“ der Deutschen Post identifiziert.

eID: Natürliche Personen werden anhand einer elektronischen Identifizierung gemäß [eIDAS#24] identifiziert.

Attest: Natürliche Personen werden anhand eines notariellen Schreibens oder durch eine amtliche Beglaubigung identifiziert.

[SMIME] **HR-DB**: Enterprise RAs von antragstellenden Organisationen können relevante Zertifikatsdaten für Mitarbeiter aus einer zuverlässigen internen Datenbank oder vergleichbarer Datenquelle verwenden, sofern im Rahmen der standardmäßigen Prozesse eine persönliche oder vergleichbare Identifizierung gemäß den vorangegangenen Verfahren stattgefunden hat. Die Datenquelle muss entsprechend geschützt und gepflegt werden, um die Korrektheit der Daten zu gewährleisten.

3.2.4 Nicht überprüfte Informationen

Es werden ausschließlich gemäß den beschriebenen Methoden validierte Informationen in ein Zertifikat aufgenommen.

3.2.5 Validierung der Bevollmächtigung

In Abhängigkeit der anzuwendenden Policy wird die Authentizität eines Zertifikatsantrags und ggf. die Berechtigung eines Antragstellers, Zertifikate im Namen einer anderen natürlichen Person oder Organisation zu beantragen, geprüft.

[OVCP] Die Authentizität eines Zertifikatsantrags wird über eine verifizierte Methode der Kommunikation (Post, Telefon, Fax, E-Mail etc.) mit der ins Zertifikat aufzunehmenden Organisation validiert, wobei die gewählte Methode der Kommunikation auf einer Quelle basiert, die nicht vom Antragsteller beeinflusst werden kann (bspw. die in Kapitel 3.2.2 genannten Quellen). Organisationen können die natürlichen Personen, die berechtigt sind, Zertifikate zu beantragen, schriftlich festlegen. In diesem Fall werden nur Anträge von den angegebenen Personen akzeptiert. Auf schriftliche Anfrage einer Organisation stellt die Telekom Security eine Liste der für diese Organisation benannten Personen zur Verfügung. Für Enterprise RAs wird im Zuge der Einrichtung der Antragsteller identifiziert und, sofern dieser nicht selbst vertretungsberechtigt ist, wird eine von einem Vertretungsberechtigten unterschriebene Vollmacht eingefordert.

[EVCP], [QEVCP-w] Die Autorisierung des Antragsunterzeichners und des Antragsgenehmigers werden, sofern sie nicht selbst vertretungsberechtigt sind, über eine entsprechende Vollmacht validiert. Die Identifizierung des Antragsunterzeichners wird mithilfe einer der Methoden gemäß Kapitel 3.2.3 durchgeführt. Die Authentizität eines Zertifikatsantrags wird über eine verifizierte Methode der Kommunikation (Post, Telefon, Fax, E-Mail etc.) mit dem Antragsunterzeichner bzw. dem Antragsgenehmiger validiert.

[SMIME] Für Enterprise RAs wird im Zuge der Einrichtung der Antragsteller identifiziert und, sofern dieser nicht selbst vertretungsberechtigt ist, wird eine von einem Vertretungsberechtigten unterschriebene Vollmacht eingefordert.

3.2.6 Kriterien für Interoperabilität

Soweit erforderlich und sinnvoll, führt die Telekom Security Cross-Zertifizierungen der eigenen Root-CAs durch, z.B. durch Ausstellung eines Cross-Zertifikats von einem bekannten und vertrauenswürdigen Root-CA-Zertifikat auf ein neues Root-CA-Zertifikat, das noch nicht in allen Anwendungen bekannt und/oder als vertrauenswürdig anerkannt ist.

Alle Cross-Zertifikate werden in der CCADB veröffentlicht.

3.2.7 Validierung der Kontrolle über eine Domain oder IP-Adresse

Die folgenden Methoden werden zur Validierung der Kontrolle über eine Domain verwendet.

- **Email, Fax, SMS, or Postal Mail to Domain Contact (Methode nach [BR#3.2.2.4.2])**
  Senden eines Zufallswertes per E-Mail, Fax, SMS oder Post an den identifizierten Domain-Kontakt und Empfangen einer bestätigenden Antwort unter Verwendung des Zufallswertes.
  2023-03-29: Diese Methode wird nicht mehr unterstützt.
- **Constructed email to domain contact (Methode nach [BR#3.2.2.4.4])**
  Senden eines Zufallswertes an „admin“, „administrator“, „webmaster“, „hostmaster“, oder „postmaster“ der Domain und Empfangen einer bestätigenden Antwort unter Verwendung des Zufallswertes bestätigt.
- **DNS Change (Methode nach [BR#3.2.2.4.7])**
  Hinterlegung eines eindeutig vorgegebenen Zufallswerts im DNS TXT Record der mit einem vorgegebenen Präfix-Label versehenen Domain.
- **Validating Applicant as a Domain Contact (Methode nach [BR#3.2.2.4.12])**
  Validierung des Antragstellers als Domain-Kontakt. Diese Methode wird nur für Domains des Konzerns Deutsche Telekom AG verwendet.
- **Agreed-Upon Change to Website v2 (Methode nach [BR#3.2.2.4.18])**
  Hinterlegung eines eindeutig vorgegebenen Zufallswerts in einer Datei im „/.well-known/pki-validation“-Verzeichnis.
- **Agreed-Upon Change to Website – ACME (Methode nach [BR#3.2.2.4.19])**
  Nutzung der ACME HTTP Challenge wie in RFC 8555 Kapitel 8.3 definiert und durch die Anforderungen der [BR] ergänzt.

Für Wildcard-Zertifikate werden die Anforderungen der [BR#3.2.2.6] auf Basis der ICANN-Domains der Public Suffix List eingehalten. Die oben aufgeführten Methoden, mit Ausnahme von [BR#3.2.2.4.18] und [BR#3.2.2.4.19], werden auch für die Validierung von Wildcard-Domänen verwendet.

Die folgenden Methoden werden zur Validierung der Kontrolle über eine IP-Adresse verwendet:

- **Agreed-upon change to website (Methode nach [BR#3.2.2.5.1])**
  Hinterlegung eines eindeutig vorgegebenen Zufallswerts in einer Datei im „/.well-known/pki-validation“-Verzeichnis.
- **Email, Fax, SMS, or Postal Mail to IP Address Contact (Methode nach [BR#3.2.2.5.2])**
  Senden eines Zufallswertes per E-Mail, Fax, SMS oder Post und Empfangen einer bestätigenden Antwort unter Verwendung des Zufallswertes.
- **Reverse Address Lookup (Methode nach [BR#3.2.2.5.3])**
  Die Kontrolle des Antragstellers wird durch die Kontrolle über einen mittels reverse-IP lookup ermittelten Domain-Namen nachgewiesen (siehe Kapitel 3.2.7).
- **Phone Contact with IP Address Contact (Methode nach [BR#3.2.2.5.5])**
  Anruf bei der Telefonnummer des IP-Adresskontakts und Erhalt einer Antwort, die den Antrag des Antragstellers auf Validierung der IP-Adresse bestätigt.

3.2.8 Validierung der Kontrolle über eine E-Mail-Adresse

Die folgenden Methoden werden zur Validierung der Kontrolle über E-Mail-Adressen verwendet:

- **Validating authority over mailbox via domain**
  Nachweis der Kontrolle über eine E-Mail-Adresse durch Nachweis der Kontrolle über die gesamte Maildomain mittels einer der in Kapitel 3.2.7 gelisteten Methoden zur Kontrolle einer Domain.
- **Validating control over mailbox via email**
  Senden eines individuellen und befristet gültigen Tokens per E-Mail an die zu validierende E-Mailadresse und Eingabe des Token durch den Zertifikatsnehmer im Service-Portal.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Die Identifizierung und Authentifizierung geschieht in Abhängigkeit vom Trust Service und unter Berücksichtigung der Gültigkeitsdauer von Validierungen und Nachweisen gemäß Kapitel 4.2.1 durch die erfolgreiche Authentisierung des Zertifikatnehmers mittels Anmeldung am entsprechenden Kundenaccount, durch Angabe eines geheimen Service-Passworts oder auf Basis des bestehenden Zertifikats und privaten Schlüssels, sofern diese noch gültig sind.

3.3.2 Identifizierung und Authentifizierung für Schlüsselerneuerung nach einer Sperrung

Schlüsselerneuerung wird für gesperrte Zertifikate nicht unterstützt.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Zertifikatsnehmer können eine Sperrung eigener Zertifikate nach erfolgreicher Authentisierung an den jeweils bereitgestellten Portalen und Schnittstellen autorisieren.

Darüber hinaus haben die jeweils zuständige Registrierungsstelle (bspw. Enterprise RA) sowie die Zertifizierungsstelle selbst die Möglichkeit, eine Sperrung in Übereinstimmung mit dieser CPS auszulösen.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Zertifikatsanträge können grundsätzlich von den Antragstellern oder den Enterprise-RAs über die bereitgestellten Service-Portale und Schnittstellen gestellt werden.

Davon ausgenommen sind jedoch Entitäten, mit denen aufgrund rechtlicher oder konzern-interner Bestimmungen keine Geschäfte erlaubt sind.

4.1.2 Antragsprozess und -verantwortlichkeiten

Antragsteller können über die bereitgestellten Portale und Schnittstellen (bspw. ACME, CMP) Zertifikatsanträge stellen. In Abhängigkeit des Zertifikatstyps umfasst der Antragsprozess folgende Punkte (in ggf. anderer Reihenfolge):

- Generierung eines Schlüsselpaars gemäß den geltenden Vorgaben dieses CPS bzw. der Nutzungsbedingungen durch den Zertifikatsnehmer oder, falls erlaubt, durch die CA
- Bereitstellung der ins Zertifikat aufzunehmenden Attribute durch den Antragsteller, ggf. inklusive eines Certificate Signing Requests (CSR, z.B. PKCS#10)
- Akzeptanz der Nutzungsbedingungen, Datenschutzhinweise, Allgemeinen Geschäftsbedingungen
- Ggf. Bereitstellung zusätzlicher Nachweise

Von den Antragstellern werden bei Antragstellung mindestens die E-Mail-Adressen als Kontaktdaten eingefordert, sofern dies nicht bereits beim Anlegen der Accounts erfolgt ist.

4.2 Bearbeitung der Zertifikatsanträge

4.2.1 Durchführung der Identifizierung und Authentifizierung

Zertifikatsanträge werden auf Vollständigkeit, Korrektheit und Echtheit überprüft. Mit der Identifizierung und Authentifizierung verbundene manuelle Tätigkeiten werden ausschließlich von Personal in vertrauenswürdigen Rollen durchgeführt.

Domains, IP-Adressen, Mail-Domains: Alle in ein Zertifikat aufzunehmenden FQDNs, IP-Adressen und E-Mail-Adressen werden gemäß den in Kapitel 3.2.7 und Kapitel 3.2.8 beschriebenen Methoden validiert. Die Validierung von Domains (auch E-Mail-Domains) oder IP-Adressen und die Validierung von EV-Zertifikatsanträgen generell werden durch die CA selbst durchgeführt und nicht an externe RAs delegiert. Sofern eine Domain (Authorization Domain Name) entsprechend validiert wurde, kann eine Enterprise RA jedoch eigenmächtig Zertifikatsanträge für Subdomains bzw. E-Mail-Adressen unter der bereits validierten Domain validieren.

Organisation: Alle in ein Zertifikat aufzunehmenden oder für die eindeutige Identifizierung notwendigen Organisationsdaten, d.h. Organisationsname, Straßenname und Hausnummer, Stadt, Postleitzahl, Bundesland/Provinz/Gliedstaat, Land sowie ggf. Organisationstyp, Beziehungen zu Mutter- oder Tochtergesellschaften oder verbundenen Unternehmen sowie eine national anerkannte Identitätsnummer oder das Gründungsdatum werden mithilfe der in Kapitel 3.2.2 beschriebenen Methoden QGIS, QIIS, Attestation oder Onsite validiert, wobei die Methode QIIS nicht zur Validierung der Organisationsdaten im Kontext von [EV] oder [QEVCP-w] verwendet wird. Organisationsinterne Informationen wie Namen organisatorischer Einheiten (nur für S/MIME relevant) und Gerätekennungen in Verbindung mit einer Organisation können von einer Enterprise RA mittels der Methode OrgDB gemäß Kapitel 3.2.2 bezogen bzw. validiert werden.

Natürliche Person: Alle natürlichen Personen, die als Subjekt in ein Zertifikat aufgenommen werden oder im Rahmen des Antragsprozesses entsprechend der angewandten Policy validiert werden müssen, werden mit den in Kapitel 3.2.3 beschriebenen Methoden identifiziert. Die Identifizierung beinhaltet mindestens die für eine eindeutige Identifizierung notwendigen Attribute, insbesondere den vollständigen Namen.

[SMIME] Organisationsinterne Informationen zu Mitarbeitern wie Mitarbeiter-Kennungen oder E-Mail-Adressen (beinhaltet nicht die generelle Validierung des Domain-Anteils) können von einer Enterprise RA mittels der Methode HR-DB gemäß Kapitel 3.2.3 bezogen bzw. validiert werden.

Autorisierung und Authentizität: Die Validierung der Bevollmächtigung eines Antragstellers in Namen einer Organisation in einer bestimmten Rolle zu handeln bzw. Zertifikate zu beantragen sowie die Authentizität der jeweiligen Anträge werden gemäß Kapitel 3.2.5 validiert.

Vorherige Validierungen und Nachweise werden ggf. wiederverwendet, sofern sie nicht älter als nachfolgende Fristen sind:

- Kontrolle über (E-Mail-)Domain oder IP-Adresse: 398 Tage
- Kontrolle über E-Mail (validiert via E-Mail): 30 Tage
- Validierung einer Identität und Autorisierung gemäß Kapitel 3.2: 825 Tage
  (398 Tage für [EV] und [QEVCP-w])

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Unvollständige oder fehlerhafte Zertifikatsanträge werden abgelehnt bzw. die verbleibenden Informationen werden vom Antragsteller eingeholt oder, nachdem sie von einer zuverlässigen, unabhängigen Datenquelle bezogen wurden, durch den Antragsteller bestätigt.

[EVCP], [QEVCP-w] Nachträglich eingeholte Informationen werden vom Antragsunterzeichner bzw. Antragsgenehmiger bestätigt. Darüber hinaus wird jeder Antrag von einem weiteren, nicht in die bisherige Antragsprüfung involvierten RA-Mitarbeiter gegengeprüft (Vier-Augen-Prinzip).

Zertifikatsanträge werden abgelehnt, wenn der verwendete Schlüssel

- nachweislich mittels einer fehlerhaften Methode erzeugt wurde,
- über eine bekannte oder nachgewiesene Methode kompromittiert werden kann (inkludiert Debian Weak Keys, ROCA),
- als kompromittiert gilt,
- [TLS] zuvor von der CA selbst generiert wurde,
- die Qualitätskriterien gemäß Kapitel 6.1.5 und Kapitel 6.1.6 nicht erfüllt.

[TLS] Sowohl zu Beginn einer Antragstellung als auch unmittelbar vor der Ausstellung eines Zertifikats werden für alle im Antrag enthaltenen FQDN-Einträge die CAA-Records im DNS geprüft. Ein Zertifikatsantrag wird abgelehnt, falls in „issue“ bzw. „issuewild“ Einträge vorhanden sind und keiner dieser Einträge „telesec.de“ enthält. Weitere Einträge des CAA Records werden nicht unterstützt. Die CAA-Prüfung ist für 8 Stunden gültig. Sollte die Abfrage eines CAA-Records fehlschlagen, kann mit der Ausstellung des Zertifikats dennoch fortgefahren werden, sofern

- der Fehler außerhalb der Infrastruktur der Telekom Security liegt,
- die Abfrage mindestens einmal wiederholt wurde und
- die Zone der Domäne keine DNSSEC-Validierungskette zur ICANN-Root hat.

Telekom Security pflegt Denied- sowie High-Risk-Listen für Zertifikatsnehmer und Domains. Zertifikatsanträge werden abgelehnt oder einer erweiterten Prüfung unterzogen, wenn der Zertifikatsnehmer oder eine Domain in den genannten Listen enthalten sind. Dies umfasst bspw. Organisationsnamen und Domains, für welche aufgrund interner oder nationaler Bestimmungen keine Zertifikate von Telekom Security ausgestellt werden dürfen oder welche aufgrund ihrer Attraktivität ein erhöhtes Risiko besitzen, Ziel von Phishing, Missbrauch oder Betrug zu sein.

Für alle Anträge wird überprüft, dass die FQDNs unter einer ICANN-Domain liegen, welche in der Public Suffix List geführt wird. Für Wildcard-Zertifikate, deren FQDN-Anteil vom Typ „public suffix“ ist (Definition gemäß [BR], ICANN-Domain), muss der Zertifikatsnehmer seine rechtmäßige Kontrolle über den gesamten Domain Namespace nachweisen. Die Public Suffix List wird hierzu regelmäßig, spätestens jedoch alle 30 Tage abgefragt.

Wenn alle Validierungsschritte gemäß Kapitel 4.2.1 erfolgreich durchgeführt 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 sicher, dass bei der Ausstellung der Zertifikate die Integrität und Authentizität der ins Zertifikat zu schreibenden Daten durch technische, organisatorische und personelle Maßnahmen gewährleistet werden. Insbesondere wird sichergestellt, dass alle Aktivitäten, die eine Zertifikatsausstellung auslösen, von autorisierten RAs stammen.

Die Ausstellung von Root- und CA-Zertifikaten bedarf der Genehmigung durch das Management und wird in der sicheren Offline-CA-Umgebung des Trust Centers im Rahmen einer Zertifikatszeremonie durchgeführt. Die an der Zeremonie beteiligten vertrauenswürdigen Rollen und ihre Aufgaben vor, während und nach der Zeremonie sind in einer Arbeitsanweisung beschrieben. Dazu gehören u.a. die Arbeitsschritte zur Aktivierung der Offline-CA und der HSMs in einem Mehrpersonenprinzip mit unterschiedlichen Rollen. Eine Zertifikatszeremonie folgt einem festgelegten Protokoll, wird darin dokumentiert und von einem qualifizierten internen Auditor sowie einem qualifizierten externen Auditor einer Konformitätsbewertungsstelle überwacht (siehe Abschnitt 8.2). Die erfolgreiche Durchführung einer Zeremonie wird von den Auditoren im Protokoll bestätigt.

[TLS] Alle Zertifikate werden vor der eigentlichen Ausstellung in einer hinreichenden Anzahl von CT-Log-Servern (Certificate Transparency gemäß [RFC6962]) als „Pre-Zertifikate“ veröffentlicht und mittels mehrerer Lint-Tools geprüft. Die Signed Certificate Timestamps (SCTs) werden im endgültigen Zertifikat aufgenommen.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats

Die Zertifikatsnehmer werden per E-Mail über die Ausstellung eines Zertifikats informiert und/oder die ausgestellten Zertifikate werden über die Trust Service spezifischen Schnittstellen bereitgestellt.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Der Zertifikatsnehmer verpflichtet sich, das Zertifikat nach Erhalt zu prüfen und im Falle falscher Angaben im Zertifikat dieses unverzüglich der Telekom Security zu melden. Wenn keine diesbezügliche Meldung vor Verwendung des Zertifikats erfolgt, gilt das Zertifikat als akzeptiert.

4.4.2 Veröffentlichung des Zertifikats durch die TSP

Zertifikatsnehmer erhalten die für sie ausgestellten Zertifikate über die jeweiligen Schnittstellen. Darüber hinaus wird in Absprache mit Enterprise-Kunden die Veröffentlichung in öffentlichen oder geschützten Verzeichnissen unterstützt.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch den TSP

Keine Bestimmungen.

[TLS] Alle Zertifikate werden vor ihrer Ausstellung in mehreren CT-Log-Servern veröffentlicht, siehe dazu Kapitel 2.2 oder 4.3.1.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Bedingungen zur Nutzung von privaten Schlüsseln und Zertifikaten durch den Zertifikatsnehmer sind in den Nutzungsbedingungen beschrieben und beinhalten u.a. den Schutz des privaten Schlüssels und die Verwendung des Zertifikats entsprechend der vorgesehenen Verwendungszwecke. Zertifikatsnehmer werden durch Akzeptanz der Nutzungsbedingungen zu deren Einhaltung verpflichtet.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte

Vertrauende Dritte haben die Verantwortung, vor Verwendung 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.

Die Nutzungsbedingungen enthalten Empfehlungen und Informationen für Vertrauende Dritte.

4.6 Zertifikatserneuerung (Renewal)

4.6.1 Umstände für ein Renewal

Voraussetzung für ein Renewal ist, dass der bestehende Schlüssel nicht kompromittiert oder anderweitig unbrauchbar geworden ist und das Zertifikat nicht aufgrund eines Sicherheitsvorfalls gesperrt wurde.

[SMIME] Die Ausstellung von Folge-Zertifikaten mit gleichen Inhalten und gleichem Schlüssel ist in Abhängigkeit des verwendeten Schlüsselmediums möglich.

4.6.2 Antragsberechtigte für ein Renewal

Gemäß Kapitel 4.1.1.

4.6.3 Verarbeitung von Anträgen auf Renewal

Anträge auf Renewal werden wie neue Anträge verarbeitet, wobei auf bereits durchgeführte und noch gültige Validierungen (Fristen siehe Kapitel 4.2.1) zurückgegriffen wird, sodass eine Ausstellung ggf. automatisiert stattfindet.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Zertifikats-Neuausstellung

Gemäß Kapitel 4.3.2.

4.6.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Gemäß Kapitel 4.4.1.

4.6.6 Veröffentlichung erneuerter Zertifikate durch den TSP

Gemäß Kapitel 4.4.2.

4.6.7 Information Dritter über die Zertifikatsausstellung durch den TSP

Gemäß Kapitel 4.4.3.

4.7 Zertifikatserneuerung mit neuen Schlüsseln (Re-Keying)

4.7.1 Umstände für ein Re-Keying

Wenn ein privater Schlüssel ausgetauscht werden soll, der private Schlüssel verloren gegangen ist oder andere Gründe vorliegen, die einen Schlüsselwechsel erfordern, so kann ein Folgezertifikat mit neuem Schlüssel, jedoch ansonsten gleichbleibenden Zertifikatsinhalten beantragt werden. Voraussetzung ist, dass das bestehende Zertifikat nicht gesperrt ist.

[SMIME] Re-keying ist nur für Zertifikate möglich, die nicht auf einer Smartcard basieren.

4.7.2 Antragsberechtigte für ein Re-Keying

Gemäß Kapitel 4.1.1.

4.7.3 Verarbeitung von Anträgen auf Re-Keying

Anträge auf Re-Keying werden wie neue Anträge verarbeitet, wobei auf bereits durchgeführte und noch gültige Validierungen (Fristen siehe Kapitel 4.2.1) zurückgegriffen wird, sodass die Ausstellung ggf. automatisiert stattfindet.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Zertifikats-Neuausstellung

Gemäß Kapitel 4.3.2.

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

Gemäß Kapitel 4.4.1.

4.7.6 Veröffentlichung von Re-Key-Zertifikaten durch den TSP

Gemäß Kapitel 4.4.2.

4.7.7 Information Dritter über die Zertifikatsausstellung durch den TSP

Gemäß Kapitel 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Änderung von Zertifikatsdaten

Für die Änderung von Zertifikatsdaten ist ein Antrag für ein neues Zertifikat zu stellen. Ein dedizierter Prozess zur Änderung von Zertifikatsdaten wird nicht angeboten.

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 Zertifikatsnehmers 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 den 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

Ein Sub-CA-Zertifikat wird gesperrt, wenn

- festgestellt wird, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- festgestellt wird, dass der private Schlüssel kompromittiert oder einer nicht autorisierten Person oder Organisation bekannt gegeben wurde oder nicht mehr den Anforderungen (siehe Kap. 6.1.5 und 6.1.6) entspricht,
- festgestellt wird, dass das Zertifikat missbräuchlich eingesetzt wurde,
- festgestellt wird, dass das Sub-CA-Zertifikat nicht konform zu dieser CPS herausgegeben oder betrieben wurde,
- festgestellt wird, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist,
- der Betrieb der Root-CA oder der Sub-CA eingestellt wird und keine Regelungen zur Weiterführung des Sperrservice getroffen wurden,
- das Recht der Root-CA oder Sub-CA, Zertifikate gemäß den Anforderungen dieser CP auszustellen erlischt oder widerrufen oder beendet wird und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden,
- gesetzliche Vorschriften, richterliche Urteile oder eine Weisung einer aufsichtsführenden Behörde vorliegen.

Darüber hinaus wird ein Sub-CA-Zertifikat gesperrt, wenn der Betreiber der Sub-CA die Sperrung, auch ohne Angabe von Gründen, beantragt. In diesem Fall ist ein schriftlicher Sperrantrag erforderlich, der von der Geschäftsleitung des Trust Centers (im Falle eines Sub-CA-Zertifikats der Telekom Security) bzw. von einem Bevollmächtigten des DFN (im Falle eines Sub-CA-Zertifikats des DFN) unterzeichnet sein muss.

Ein Endteilnehmer-Zertifikat wird gesperrt, wenn

- ein autorisierter Sperrantrag, auch ohne Angabe von Gründen, vom Zertifikatsnehmer oder, sofern anwendbar, der zuständigen RA vorliegt
- relevante Angaben im Zertifikat nicht (mehr) korrekt sind
- keine Autorisierung des Zertifikats (mehr) vorliegt, dazu zählen:
  - eine Information vom Zertifikatsnehmer liegt vor, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll
  - [TLS] es kann der Kontrolle über einen/eine im Zertifikat angegebenen FQDN oder IP-Adresse nicht mehr vertraut werden
  - [TLS] die Verwendung eines/einer im Zertifikat angegebenen FQDN oder einer IP-Adresse ist nicht mehr zulässig
  - [SMIME] die Verwendung einer im Zertifikat angegebenen E-Mail-Adresse ist nicht mehr zulässig
  - [SMIME] es kann der Domain-Autorisierung oder der Kontrolle über die Mailbox nicht mehr vertraut werden
- eine Schlüsselschwäche oder -Kompromittierung nachgewiesen wird, dazu zählen:
  - Telekom Security wird nachgewiesen, dass der private Schlüssel kompromittiert oder einer unautorisierten Person übergeben wurde
  - Telekom Security wird nachgewiesen, dass ein schwacher privater Schlüssel verwendet wird, welcher leicht auf Basis des öffentlichen Schlüssels berechnet werden kann (z.B. „Debian weak key“) oder unter Verwendung einer mangelhaften Methode generiert wurde oder andere Methoden bekannt sind, die den privaten Schlüssel gefährden
  - der private Schlüssel genügt nicht mehr den Anforderungen gemäß Kap. 6.1.5 und 6.1.6
- ein Verstoß gegen die CP, CPS oder die Nutzungsbedingungen nachgewiesen wird, dazu zählen
  - das Zertifikat wurde nicht in Übereinstimmung mit dem relevanten CPS ausgestellt
  - das Zertifikat wurde missbräuchlich eingesetzt
  - der Zertifikatsnehmer wurde, sofern anwendbar, suspendiert bzw. gesperrt

- [TLS] ein Wildcard-Zertifikat wurde zur Authentifizierung eines betrügerisch irreführenden Sub-FQDN verwendet

Darüber hinaus MÜSSEN alle betroffenen Zertifikate gesperrt werden, wenn

- Telekom Security ihren Betrieb einstellt und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen hat,
- Telekom Security die Berechtigung verliert, bestimmte Zertifikatstypen auszustellen und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen hat oder
- der private Schlüssel einer CA kompromittiert wurde.

Gesperrte Zertifikate werden nicht wieder entsperrt.

Die Sperrgründe werden gemäß der Vorgaben der [TSCP] gesetzt.

4.9.2 Berechtigte Sperrantragsteller

Die Sperrung eines Zertifikats kann durch die CA, die zuständige Enterprise RA oder den Zertifikatsnehmer bzw. einen berechtigten Vertreter des Zertifikatsnehmers initiiert werden.

Darüber hinaus kann die Sperrung eines Zertifikats durch weitere Parteien ausgelöst werden, wenn gegenüber dem Telekom Security nachgewiesen werden kann, dass einer der in Kapitel 4.9.1 aufgeführten Sperrgründe vorliegt. Siehe dazu Kapitel 1.5.2 bzw. 4.9.12.

4.9.3 Verfahren zur Beantragung von Sperrungen

Zertifikatsnehmer bzw. deren berechtigte Vertreter oder ggf. zuständige Enterprise RA können eine Sperrung eigener Zertifikate rund um die Uhr über die Funktionen des eigenen Kundenaccounts autorisieren oder nach Bereitstellung eines je Zertifikat individuellen Sperr-Passworts über die bereitgestellten Support-Schnittstellen veranlassen.

Darüber hinaus bietet das Trust Center eine E-Mail-Schnittstelle an, über die Missbrauchs- sowie Problemmeldungen zu Zertifikaten gemeldet werden können (siehe dazu Kapitel 1.5.2). Telekom Security bearbeitet diese Meldungen und leitet bei Vorliegen eines entsprechenden Sperrgrunds die Sperrung von betroffenen Zertifikaten ein. Der Meldende des Problems wird über den Erhalt der Meldung sowie ggf. dadurch resultierende Sperrungen der betroffenen Zertifikate informiert.

4.9.4 Fristen zur Beantragung einer Sperrung

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

4.9.5 Fristen zur Verarbeitung von Sperranträgen

Endteilnehmerzertifikate werden so schnell wie möglich gesperrt, spätestens jedoch innerhalb von 24 Stunden nach Eingang eines autorisierten Sperrantrags. Dieser Zeitraum umfasst die Zeit zur Übergabe des Sperrstatus an die Zertifikatsstatusdienste. Dies gilt nicht für Sperrungen, die für einen späteren Zeitpunkt beantragt werden, z. B. aufgrund einer geplanten Beendigung der Teilnahme. Für Sperrungen, die nicht auf autorisierten Sperranträgen, sondern auf anderen in Kapitel 4.9.1 aufgeführten Sperrgründen beruhen, gelten die folgenden Sperrfristen:

- Endteilnehmerzertifikate werden innerhalb von 24 Stunden gesperrt, wenn eine Schlüsselschwäche oder Kompromittierung oder eine fehlende Berechtigung eines Zertifikats nachgewiesen wird oder die Telekom Security ihre Berechtigung zur Ausstellung von Zertifikaten gemäß [BR] verliert.

- Endteilnehmerzertifikate werden so schnell wie möglich, spätestens jedoch innerhalb von 5 Tagen gesperrt, wenn ein Verstoß gegen die CP, CPS oder Nutzungsbedingungen nachgewiesen wird.

Telekom Security wird in begründeten Fällen Zertifikate zu einem von einem relevanten Root Store Betreiber festgelegten Datum sperren, welches von den vorgenannten Fristen abweichen kann.

Bei Eingang einer Problemmeldung zu einem Zertifikat werden innerhalb von 24 Stunden die Fakten und Umstände untersucht und es werden dem Zertifikatsnehmer sowie der meldenden Person eine erste Rückmeldung zu den bis dahin vorliegenden Erkenntnissen gegeben. Anschließend werden mit dem Zertifikatsnehmer und der meldenden Person die Analyseergebnisse besprochen und es wird entschieden, ob eine Sperrung erforderlich ist. Falls eine Sperrung erforderlich ist, wird unter Beachtung der zeitlichen Vorgaben aus Kap. 4.9.1 und Berücksichtigung der folgenden Aspekte der Zeitpunkt der Sperrung festgelegt:

- Art des mutmaßlichen Problems (Umfang, Kontext, Schweregrad, Ausmaß, Schadensrisiko)
- Auswirkungen einer Sperrung (direkte und kollaterale Auswirkungen auf Endteilnehmer vertrauende Dritte)
- Anzahl der erhaltenen Problemmeldungen zu einem Zertifikat oder Zertifikatsnehmer
- Meldende Entität
- Einschlägige Rechtsvorschriften

4.9.6 Anforderungen an Dritte zur Prüfung von Sperrinformationen

Vertrauende Dritte 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, welche Informationen zu gesperrten CA-Zertifikaten enthalten (Certification Authority Revocation List (CARL)), werden spätestens alle 6 Monate sowie ggf. bei Bedarf aktualisiert.

Sperrlisten, welche Informationen zu gesperrten Endteilnehmer-Zertifikaten enthalten (Certificate Revocation List (CRL)), werden regelmäßig alle 24 Stunden sowie ggf. bei Bedarf aktualisiert.

4.9.8 Maximale Latenzzeit von Sperrlisten

Neu erstellte CARLs und 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 entsprechenden Zertifikatserweiterung aufgeführt.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

Vertrauende Dritte sind dazu angehalten, bei der Prüfung eines Zertifikatsstatus per OCSP die Vorgaben gemäß [RFC6960] zu berücksichtigen.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine Bestimmung.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Zertifikatsnehmer können eine Schlüsselkompromittierung über die ihnen bereitgestellten Schnittstellen melden. Siehe dazu auch Kapitel 4.9.3.

Darüber hinaus kann jede Partei eine Schlüsselkompromittierung über die in Kapitel 1.5.2 genannte E-Mailadresse melden. Entsprechende Meldungen sollten einen CSR beinhalten, welcher mit dem kompromittierten privaten Schlüssel erstellt und signiert wurde. Der commonName im CSR soll eine entsprechend eindeutige Bezeichnung beinhalten, welche auf die Kompromittierung des Schlüssels hinweist (bspw. „Compromised Key“). Ebenso sollte das betroffene Zertifikat selbst oder zumindest eine Referenz auf dieses beigefügt sein.

4.9.13 Umstände für eine Suspendierung

Suspendierung wird ausschließlich für S/MIME-Zertifikate unterstützt, welche für Mitarbeiter der Deutschen Telekom AG ausgestellt wurden. Eine Suspendierung wird bei

- temporärer Nicht-Verfügbarkeit der Smartcard des Mitarbeiters,
- längerer geplanter Abwesenheit von Mitarbeitern,
- Verdacht der unerlaubten Verwendung einer Smartcard des Mitarbeiters,
- zeitnah geplantem Austritt eines Mitarbeiters aus dem Unternehmen (wird nachträglich in Sperrung umgewandelt)

vorgenommen.

4.9.14 Berechtigte Antragsteller für eine Suspendierung

Suspendierungen können durch den Zertifikatsnehmer, die RA oder CA vorgenommen werden.

4.9.15 Ablauf einer Suspendierung

Die Suspendierung von Zertifikaten wird durch automatisierte Prozesse ausgelöst oder durch autorisierte Personen nach entsprechender Authentisierung beauftragt und anschließend umgesetzt.

4.9.16 Begrenzung der Suspendierungsperiode

Die Suspendierungsperiode ist für manche Suspendierungsgründe (bspw. bei Verlust einer Smartcard) auf maximal 30 Tage begrenzt, bevor das Zertifikat automatisch gesperrt wird. Ansonsten existiert keine allgemeine Begrenzung.

4.10 Zertifikatsstatusdienste

Mindestens über die gesamte Gültigkeitsdauer eines Zertifikats werden sowohl von der CAs signierte Sperrlisten als auch von delegierten OCSP-Signern signierte OCSP-Auskünfte bereitgestellt.

[TLS] Dies gilt auch für Pre-Zertifikate.

4.10.1 Betriebliche Vorgaben

Alle Zertifikatsstatusdienste werden 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 und geloggt.

OCSP-Antworten werden auf Anfrage generiert und erhalten einen Wert im nextUpdate-Feld, der 5 Tage nach dem thisUpdate-Wert liegt, werden jedoch maximal für 2 Stunden für weitere Anfragen wiederverwendet.

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

Der Wert des nextUpdate-Felds einer CARL liegt maximal 6 Monate nach dem Wert des thisUpdate-Felds.

Der Wert des nextUpdate-Felds einer CRL liegt maximal 5 Tage nach dem Wert des thisUpdate-Felds.

Abhängig vom Trust Service werden gesperrte Zertifikate nach ihrem Ablauf entweder mindestens noch in die nächste reguläre Sperrliste aufgenommen oder sie werden nach ihrem Ablauf nicht aus Sperrlisten entfernt.

[QEVCP-w] Gesperrte Zertifikate werden nach ihrem Gültigkeitsende nicht von Sperrlisten entfernt.

4.10.2 Verfügbarkeit

Die Zertifikatsstatusdienste stehen 7x24h zur Verfügung. Es sind Maßnahmen getroffen worden, die im Falle einer Störung die Wiederherstellung der Verfügbarkeit der Zertifikatsstatusdienste innerhalb von 12 Stunden gewährleisten. Darüber hinaus werden größtmögliche Bemühungen unternommen, Störungen so schnell wie möglich zu beheben.

Es stehen ausreichende Kapazitäten zur Verfügung, so dass die Antwortzeit der Statusdienste unter normalen Betriebsbedingungen 10 Sekunden nicht überschreitet.

4.10.3 Optionale Merkmale

Keine Bestimmungen.

4.11 Kündigung durch Zertifikatsinhaber

Wenn mit der Kündigung eine Sperrung von Zertifikaten verknüpft sein sollte, gelten die in Kapitel 4.9.1 beschriebenen Bestimmungen.

4.12 Schlüsselhinterlegung und Wiederherstellung

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 Informationssicherheitsmanagementsystem (ISMS), welches nach ISO 27001 zertifiziert ist.

Das ISMS selbst sowie weitere Sicherheitsrichtlinien, Sicherheitskonzepte und andere Dokumente stellen die Einhaltung der in der [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 Rechenzentren (u.a. georedundantes 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 der Gebäude ist für den sicheren Betrieb kritischer Systeme ausgelegt und erfüllt die Anforderungen an eine Hochsicherheitszone.

Die für den Betrieb des Trust Centers relevanten Rechenzentrumsbereiche sind durch zusätzliche Einhausungen von anderen Bereichen getrennt und nach „Trusted Site Infrastructure 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
- Leiter VDA: ist Ansprechpartner und Auskunftsperson der qualifizierten Vertrauensdiensteanbieter (VDA) „Deutsche Telekom AG“, „T-Systems International GmbH“ bzw. “Deutsche Telekom Security GmbH“ für die nationalen Aufsichtsstellen
- Solution Manager: verantwortet und verwaltet einen Trust Service
- Trust Center Information Security Officer: hat die übergreifende Verantwortung für die Implementierung von Sicherheitsmaßnahmen
- Registrierungsmitarbeiter/Validierungsspezialist: prüft und bearbeitet Anträge zur Zertifikatsausstellung, -Suspendierung, -Sperrung oder Erneuerung
- Administrator: installiert, konfiguriert und wartet die Systeme der Trust Services
- interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten z.B. Protokolldaten, Datenbanken und papierbasierte Dokumentationen der Trust Services
- Compliance-Manager: prüft regelmäßig die den Trust Services zugrunde liegenden Anforderungen, stimmt diese mit den Solution Managern ab und koordiniert die erforderlichen Prüfungen durch externe Auditoren.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Für alle in Kap. 5.2.1 aufgeführten Rollen 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 mindestens ein Vier-Augen-Prinzip benötigt wird, sind:

- Generierung, Sicherung und Wiederherstellung von CA-Schlüsseln
- Jegliche Tätigkeiten an der Offline-CA:
  - Ausstellung von Zertifikaten und Sperrlisten
  - Sperrung von Zertifikaten
  - Änderungen an der Konfiguration
- Jeglicher Zugriff auf die Offline-HSMs (inkl. Backup-HSMs)
- Validierungen von EV-Zertifikatsanträgen
- Bewertung von Sicherheitsvorfällen
- Aktivitäten im Rahmen des Change-Managements

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Die Identifizierung geeigneter Personen zur Besetzung von Rollen, die Übertragung der Rollen (Authentifizierung) sowie deren Entzug erfolgen nach einem dokumentierten Prozess, welcher u.a. die Klärung des Bedarfs, den 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 Person unter Vorlage eines amtlichen Ausweises 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 Kapitel 5.2.4) entstehen und die Unabhängigkeit gewahrt wird, d.h. dass

- die Bereiche, die mit der Generierung und Sperrung von Zertifikaten betraut sind, bei ihren Entscheidungen über die Einrichtung, Bereitstellung, Aufrechterhaltung und Aussetzung von Trust Services 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 Trust Services 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 und 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:

- Leiter Trust Center und/oder Leiter VDA
- Trust Center Information Security Officer und/oder interner Auditor
- Registrierungsmitarbeiter/Validierungsspezialist
- Administrator

Personen in den genannten Rollen können nur dann Antragsteller für Zertifikate sein, wenn diese Zertifikate im Namen der Person selbst oder des Trust Centers der Telekom Security 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 organisatorischen Betrieb der angebotenen Trust Services. Darüber hinaus ist sie durch Ausbildung und Erfahrung versiert in den Bereichen Informationssicherheit (inkl. Risikomanagement, Sicherheitsverfahren für Personal etc.) und PKI-Technologien.

Mitarbeiter erfüllen die Anforderung an hinreichendes Expertenwissen zur korrekten Ausübung ihrer Tätigkeiten aufgrund 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).

5.3.2 Verfahren zur Hintergrundprüfung

Alle Mitarbeiter in vertrauenswürdigen Rollen wurden anhand amtlicher Ausweisdokumente identifiziert und 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.

5.3.3 Schulungsanforderungen

Alle mit Registrierungstätigkeiten betrauten Mitarbeiter werden zu folgenden Themen geschult und geprüft:

- Public Key Infrastrukturen
- Allgemeine Bedrohungen für den Informationsüberprüfungsprozess, einschließlich Phishing und Social-Engineering
- Authentifizierungs- und Überprüfungsrichtlinien sowie -verfahren gemäß [TSCP], dieser CPS sowie [BR] und [EVCG], sofern anwendbar

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

5.3.4 Nachschulungsintervalle und -anforderungen

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

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

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Keine Bestimmungen.

5.3.6 Sanktionen bei unbefugten Handlungen

Mitarbeiter sind rechenschaftspflichtig für ihr Handeln. Verstöße gegen Vorgaben haben arbeitsrechtliche Konsequenzen entsprechend der Schwere des Verstoßes.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Unabhängige Auftragnehmer, namentlich externe RAs bzw. Enterprise RAs, werden vertraglich verpflichtet, die hier genannten Prozesse und Maßnahmen, sofern anwendbar, ebenfalls einzuhalten.

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. Darüber hinaus werden relevante Handbücher für Systeme und Prozesse sowie FAQs bereitgestellt.

Die Informationssicherheitsrichtlinien sowie die darin festgelegten Sicherheitsrollen und Zuständigkeiten sind in entsprechenden Konzerndokumenten beschrieben und stehen allen Mitarbeitern zur Verfügung.

5.4 Protokollierungsverfahren

5.4.1 Zu protokollierende Ereignisse

Die folgenden Ereignisse (gemäß der detaillierten Auflistung in [TSCP#5.4.1]) werden kontinuierlich inkl. einer Beschreibung des Ereignisses, des präzisen Zeitpunkts und, sofern anwendbar, der Identität des Auslösers protokolliert:

- Alle wesentlichen Zertifikats-Lebenszyklus-Ereignisse der Zertifikats- und Schlüsselmanagement-systeme sowie Statusdienste
- Alle sicherheitsrelevanten Ereignisse an den PKI- und Sicherheitssystemen
- 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 (siehe Kap. 6.8).

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 im Bedarfsfall ausgewertet, z.B. bei Fehlerbehebungs- oder Analysetätigkeiten.

5.4.3 Aufbewahrungszeitraum für Logdaten

Alle Logdaten zum Zertifikats-Lebenszyklus werden bis zwei Jahre nach Ablauf der zugehörigen Zertifikate und, bei CA-Zertifikaten, zwei Jahre nach Löschung der CA-Schlüssel aufbewahrt.

Alle anderen Logdaten werden für zwei Jahre nach ihrem Eintreten 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 oder 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 ereignisauslösenden Person

Keine Bestimmungen.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Bestimmungen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Art der archivierten Datensätze

Die folgenden Aufzeichnungen gemäß der detaillierten Auflistung in [TSCP#5.5.1] werden mit ggf. Angabe von Datum, Uhrzeit und Identität der handelnden Person archiviert.

- Antrags-/Zertifikatshistorie sowie, falls anwendbar, Lebenszyklus von Schlüsseln
- Nachweise (Registrierungsinformationen) im Rahmen von Ausstellung, Erneuerung, Sperrung von Zertifikaten
  [TLS] Dies umfasst die Methode gemäß [BR#3.2.2.4] und [BR#3.2.2.5], die zur Validierung der Kontrolle über Domänen und IP-Adressen verwendet wird, sowie die Version des [BR], auf der die Validierung basiert.
- Alle veröffentlichten CP, CPS und Nutzungsbedingungen,
- Zertifizierungsunterlagen und Auditberichte
- Relevante Dokumentation bzgl. der Sicherheit der Systeme

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Alle in Kap. 5.5.1 genannten Aufzeichnungen, mit Ausnahme der Dokumentation bzgl. der Sicherheit der Systeme, werden für sieben Jahre aufbewahrt. Für Aufzeichnungen mit Bezug zur Zertifikatshistorie beginnt diese Frist mit Ablauf der Zertifikate und, im Falle von CA-Zertifikaten, mit Löschung der CA-Schlüssel.

Die relevante Dokumentation bzgl. der Sicherheit der Systeme wird für zwei Jahre aufbewahrt.

5.5.3 Schutz von Archiven

Es sind technische und organisatorische Maßnahmen etabliert, welche die Verfügbarkeit, Integrität und Vertraulichkeit der Aufzeichnungen im Rahmen der Aufbewahrung sicherstellen und überwachen.

Der Zugriff auf elektronisch abgelegte Daten sowie der Zutritt zu den Papierarchiven ist auf autorisierte Mitarbeiter des Trust Centers beschränkt.

5.5.4 Backup-Verfahren für Archive

Die elektronischen Ablagen 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)

Es kommen ausschließlich interne Archivsysteme zum Einsatz.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

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

Für den Zugriff auf die Daten ist eine begründete Anfrage bei einer der folgenden Rollen (gemäß Kap. 5.2.1) zu stellen:

- Leiter Trust Center
- Leiter VDA
- Trust Center Information Security Officer
- Solution Manager des betroffenen Trust Services

Nach Prüfung der Begründung werden die Informationen über die autorisierten Mitarbeiter (gemäß Kap. 5.5.3) zur Verfügung gestellt.

5.6 Schlüsselwechsel

Vor Ablauf eines CA-Zertifikats wird rechtzeitig ein neues CA-Zertifikat ausgestellt. Dabei wird der Zeitraum zwischen der 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. Die Verbreitung der neu ausgestellten CA-Zertifikate geschieht analog zu bereits bestehenden CA-Zertifikaten wie in Kapitel 2.2 beschrieben.

5.7 Kompromittierung und Notfall-Wiederherstellung

5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

Die Notfalldokumentation des Trust Centers berücksichtigt alle Anforderungen aus [TSCP#5.7.1] und wird bei Bedarf Auditoren gegenüber offengelegt.

Mitarbeiter verfügen über mehrere Möglichkeiten (technische Schnittstelle, direkter Kontakt zum ISMS, Mitarbeiter-Portale) 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 einen Trust Service oder auf personenbezogene Daten werden innerhalb von 24 Stunden an die zuständigen Behörden gemeldet, je nach Art und Kontext des Vorfalls.

Natürliche Personen und Organisationen, welche Trust Services der Telekom Security in Anspruch nehmen und potenziell von einem Sicherheitsvorfall negativ betroffen sind, werden umgehend über den Sicherheitsvorfall informiert.

Sollte ein Vorfall einen Verstoß gegen eine Root Store Policy darstellen, so wird vom Trust Center PKI Compliance Management zeitnah ein Incident Report unter Berücksichtigung der jeweiligen Vorgaben erstellt. Die Ausstellung betroffener Zertifikatstypen wird ggf. eingestellt, bis die Ursache beseitigt wurde oder weitere Schäden ausgeschlossen werden können.

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

Eine Kompromittierung, der Verdacht auf Kompromittierung oder der Verlust eines privaten CA-Schlüssels werden 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 sowie aller betroffenen Endteilnehmerzertifikate eingeleitet und alle betroffenen Endteilnehmer, Root Stores sowie weitere Instanzen, mit denen entsprechende Vereinbarungen abgeschlossen wurden, informiert.

5.7.4 Geschäftsfortführung nach einem Notfall

Die Geschäftsfortführung bzw. die Bereitstellung der für einen konformen Weiterbetrieb benötigten Dienste und Systeme wird durch technische und organisatorische Maßnahmen gesichert. Dazu gehören neben einem georedundanten Betrieb auch entsprechend [TSCP#5.7.1] aufgebaute Notfalldokumentation bzw. Notfallmanagement. 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

Sollte die Fortführung eines Trust Services nicht möglich sein, wird eine sichere Beendigung gemäß eines fortlaufend aktualisierten Beendigungsplans gewährleistet, bei dem die potenziellen Störungen für Zertifikatsnehmer und Dritte minimiert werden.

Alle betroffenen Zertifikatsnehmer, Root Stores und Unterauftragnehmer werden frühzeitig über eine geplante Beendigung informiert. Darüber hinaus werden entsprechende Informationen auf den Webseiten des Trust Centers bereitgestellt.

Der Betrieb der Statusdienste wird bis zum Ablauf der Gültigkeit aller Endteilnehmerzertifikate an die Deutsche Telekom AG oder die T-Systems International GmbH übergeben, welche als qualifizierte Vertrauensdiensteanbieter (VDA) gemäß Vertrauensdienstegesetz fungieren. Ebenso werden die gemäß Kapitel 5.5.1 archivierten Aufzeichnungen der Deutschen Telekom AG oder der T-Systems International GmbH zur Aufbewahrung bis zum Ablauf der festgelegten Aufbewahrungsfrist übergeben. Kundendaten und sonstige Daten, welche nicht aufbewahrt werden müssen, werden gelöscht.

Alle zum Zeitpunkt der geplanten Außerbetriebnahme noch nicht gesperrten Zertifikate werden gesperrt und die privaten Schlüssel der betroffenen CAs werden zerstört.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

6.1.1.1 Generierung von CA- und OCSP-Signer-Schlüsselpaaren

Die Generierung von CA- und OCSP-Signer-Schlüsselpaaren setzt die Freigabe des Managements voraus und wird in der sicheren Umgebung des Trust Centers im Rahmen einer Schlüssel-Zeremonie durchgeführt. Die an der Zeremonie beteiligten vertrauenswürdigen Rollen und deren Aufgaben vor, während und nach der Schlüsselzeremonie sind in einer Arbeitsanweisung beschrieben. Dies beinhaltet u.a. die Arbeitsschritte zur Aktivierung der HSMs, Schlüsselgenerierung und Backup im Mehr-Personen-Prinzip mit unterschiedlichen Rollen. Die Generierung der Schlüssel wird grundsätzlich auf den HSMs gemäß Kapitel 6.2.1 ausgeführt, welche auch für den späteren Betrieb vorgesehen sind, d.h.CA- und OCSP-Signer-Schlüsselpaare werden nicht von der ausstellenden (Root-) CA generiert.

Alle Zeremonien für CA-Schlüssel werden von einem qualifizierten internen Auditor und von einem qualifizierten externen Auditor einer Konformitätsbewertungsstelle (siehe Kapitel 8.2) überwacht. Die erfolgreiche Durchführung einer Zeremonie wird durch die Auditoren in den Protokollen bestätigt.

6.1.1.2 Generierung von RA-Schlüsseln

RA-Schlüsselpaare werden in Smartcards gemäß Kap. 6.2.1 generiert.

6.1.1.3 Generierung von Endteilnehmer-Schlüsseln

[TLS] Schlüsselpaare werden vom Zertifikatsnehmer selbst erzeugt.

[SMIME] Schlüsselpaare werden vom Zertifikatsnehmer oder von der CA generiert.

Die CA generiert Endteilnehmer-Schlüsselpaare in zertifizierten kryptographischen Modulen (HSM oder Smartcard) und schützt die Schlüssel hinsichtlich Vertraulichkeit und Integrität.

Zertifikatsnehmer, welche ihre Schlüssel selbst generieren, werden über die zulässigen Schlüsselalgorithmen und -parameter informiert.

6.1.2 Bereitstellung der privaten Schlüssel an Zertifikatsnehmer

Private Schlüssel für Endteilnehmer-Zertifikate werden in PIN-geschützten Smartcards oder in Form von passwortgeschützten PKCS#12-Dateien über gesicherte Kanäle an die Zertifikatsnehmer ausgegeben. Entsprechende Passwörter oder PINs werden über anderweitige, sichere Kanäle den Endteilnehmern übermittelt.

6.1.3 Übergabe öffentlicher Schlüssel an den TSP

Öffentliche Schlüssel werden von den Antragstellern mittels PKCS#10-Requests über gesicherte Kommunikationswege übergeben.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

Alle CA-Zertifikate werden wie in Kap. 2.2 beschrieben veröffentlicht.

6.1.5 Schlüssellängen

Es werden ausschließlich RSA-Schlüssel generiert bzw. akzeptiert, welche eine Länge von mindestens 2048 Bit und eine durch 8 teilbare Länge des Modulo aufweisen.

Es werden ausschließlich EC-Schlüssel generiert bzw. akzeptiert, welche auf den Kurven NIST P-256 oder NIST P-384 liegen.

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Bei RSA-Schlüsseln wird geprüft, dass der Wert des Exponenten eine ungerade Zahl größer oder gleich 3 ist und im Bereich von 2^{16} und 2^{256}-1 liegt sowie, dass der Modulo eine ungerade Zahl ist, die nicht die Potenz einer Primzahl ist und keine Faktoren hat, die kleiner als 752 sind.

Bei EC-Schlüsseln wird geprüft, ob es sich um einen normierten Punkt handelt, der auf der gewünschten Kurve liegt, ein Vielfaches des Generatorpunkts ist und nicht der unendlich ferne Punkt der Kurve ist.

6.1.7 Schlüsselverwendung

Alle Zertifikate enthalten eine gemäß Kapitel 7.1.2 definierte keyUsage- und extendedKeyUsage-Erweiterung, welche die zulässige Verwendung der mit dem Zertifikat verbundenen Schlüssel gemäß [RFC5280] vorgibt.

Die Verwendung eines privaten Schlüssels einer Root CA ist beschränkt auf das Signieren

- ihres eigenen Root-CA-Zertifikats
- der Sub-CA-Zertifikate,
- der OCSP-Signer-Zertifikate und
- der Sperrlisten (CARLs).

Die Verwendung eines privaten Schlüssels einer Sub-CA ist beschränkt auf das Signieren

- der Endteilnehmerzertifikate,
- der OCSP-Signer-Zertifikate
- der Sperrlisten (CRLs).

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

Alle eingesetzte HSMs sind nach FIPS 140-2 Level 3 zertifiziert und werden in dem entsprechenden FIPS-Modus betrieben. Zum Schutz der HSMs während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet.

Alle eingesetzten Smartcards sind nach CC EAL4+ evaluiert.

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 Kapitel 6.1.1, 6.2.4 und 6.2.8. Beim Import und Export der Schlüssel in die bzw. aus den Backup-HSM kommen Authentisierungstoken zum Einsatz, über die ein Mehr-Personen-Prinzip erzwungen wird.

6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung privater Schlüssel findet nicht statt.

6.2.4 Sicherung privater Schlüssel

Private CA-Schlüssel werden ausschließlich im Vier-Augen-Prinzip im Rahmen einer Key-Zeremonie auf Backup-HSM gesichert, welche unter einem vergleichbaren Sicherheitsniveau wie die in Betrieb befindlichen HSMs aufbewahrt werden.

Bei den Endteilnehmer-Schlüsseln werden nur die privaten Schlüssel für Verschlüsselungszertifikate von Mitarbeitern der Deutschen Telekom AG gesichert. Die Schlüssel werden mittels Verschlüsselungsschlüssel geschützt, welche selbst wiederum in HSMs vorgehalten werden.

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 verschlüsselt zu Zwecken der Sicherung in bzw. Rücksicherung von Backup-HSMs statt (siehe Kapitel 6.2.4). Die Arbeitsschritte werden im Rahmen einer Schlüssel-Zeremonie und mindestens Vier-Augen-Prinzip durchgeführt.

Eine Übertragung privater RA- oder Endteilnehmer-Schlüssel in bzw. aus Smartcards ist nicht möglich, mit Ausnahme der privaten Schlüssel für Verschlüsselungszertifikate von Mitarbeitern der Deutschen Telekom AG (siehe Abschnitt 6.2.4), die nur in Smartcards importiert, aber nicht wieder exportiert werden können.

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 der Zertifikatsnehmer müssen zur initialen Aktivierung aus dem "Null-PIN"-Zustand in den Betriebszustand mittels Setzen 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

Private CA-Schlüssel werden zerstört, wenn sie nicht länger benötigt werden oder wenn die zugehörigen Zertifikate abgelaufen sind oder gesperrt wurden.

Die Zerstörung von 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 kryptografische Module 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.

6.2.11 Bewertung kryptografischer Module

Siehe Kap. 6.2.1.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des öffentlichen Schlüssels

Die öffentlichen Schlüssel werden im Rahmen der Archivierung der Zertifikate gemäß Kap. 5.5.2 archiviert.

6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Das Gültigkeitsende eines Zertifikats überschreitet nicht das Gültigkeitsende des ausstellenden CA-Zertifikats.

Es gelten die folgenden maximalen Gültigkeitsdauern für Zertifikate:

- Root-CA-Zertifikate 25 Jahre
- Sub-CA-Zertifikate 10 Jahre
- [TLS] Endteilnehmer-Zertifikate 397 Tage
- [SMIME] Endteilnehmer-Zertifikate 825 Tage (Bestandszertifikate: bis zu 1185 Tage)

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

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

[SMIME] Die PINs und PUKs für Endteilnehmer-Schlüssel auf Smartcards werden entweder durch einen sicheren Zufallszahlengenerator der CA erzeugt und im Rahmen der Personalisierung der Smartcards

installiert, oder vom Zertifikatsnehmer nach Erhalt der Smartcard im Null-PIN-Status und Prüfung ihrer Unversehrtheit vergeben.

6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten der HSM sind nur Personen in vertrauenswürdigen Rollen bekannt. Der Kreis der wissenden Personen ist dabei auf das minimal erforderliche Maß eingeschränkt. Hinsichtlich der HSM für Root CAs sind die Aktivierungsdaten den jeweiligen Personen nur in Teilen bekannt, sodass keine Person alleinigen Zugriff erlangen kann.

Endteilnehmer haben die PINs und PUKs von Smartcards gemäß den Nutzungsbedingungen eigenverantwortlich zu schützen.

6.4.3 Andere Aspekte der Aktivierungsdaten

Keine Bestimmungen.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Es werden ausschließlich vertrauenswürdige Systeme eingesetzt, 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 der Deutschen Telekom 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 internen Sicherheitsrichtlinien beschrieben.

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.

Alle Accounts werden gemäß den Anforderungen aus [TSCP#6.5.1] mit Multi-Faktor-Authentifizierung oder starken Passwörtern geschützt.

Die zur Zertifikatserzeugung und ggf. -sperrung erfassten Daten inkl. der Protokolldaten gemäß Kap. 5.4.1 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

Es wird Software renommierter Hersteller eingesetzt, 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 in einem Testsystem ins Wirksystem überführt.

Die Entwicklungs-, Test- und Produktivumgebungen des Trust Centers 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. Änderungen, die sich auf das festgelegte Sicherheitsniveau auswirken, werden zuvor vom Management und ggf. vom ISMS freigegeben.

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

Systeme loggen alle in Kapitel 5.4.1 genannten sicherheitsrelevanten Ereignisse.

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

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 Konfigurationen der

Systeme werden hinsichtlich der Einhaltung dieser Regeln in regelmäßigen Abständen und bei Bedarf geprüft.

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.

Das Zertifikatsmanagementsystem und die dazugehörigen HSMs der Root-CAs werden auf einer reinen Offline-CA betrieben, d.h. in einem physisch abgeschotteten Netzwerk ohne Netzverbindung zu anderen Netzwerken.

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

Alle externen Netzanbindungen sind redundant aufgebaut.

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

Bei Inbetriebnahme oder signifikanten Änderungen an der Infrastruktur bzw. Anwendungen, mindestens jedoch einmal pro Jahr, werden Penetrationstests durchgeführt.

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

Alle Systeme werden regelmäßig (mehrfach täglich) über einen Zeitserver und das Network Time Protocol (NTP) mit exakten Zeitinformationen synchronisiert, so dass die Zeitstempel in Logs und Aufzeichnungen verlässlich sind.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

Anmerkung: Die in diesem Kapitel beschriebenen Zertifikatsprofile spiegeln die aktuelle Praxis wider. Ältere Zertifikate von vor Gültigkeitsbeginn dieser CPS, können Abweichungen aufweisen. Sie behalten jedoch ihre Gültigkeit bei, sofern nicht explizit auf deren Ungültigkeit hingewiesen wird.

Alle Zertifikatsprofile entsprechen [RFC5280] sowie [X.509].

Alle Zertifikate erhalten eine unter der jeweiligen CA eindeutige Seriennummer, welche von einem kryptographisch sicherem Pseudo-Zufallszahlengenerator und mit einer Entropie von mindestens 126 Bit generiert werden.

Die Gültigkeitsdauer eines jeden Zertifikats beginnt mit dem Ausstellungszeitpunkt oder gegebenenfalls später, die Gültigkeit wird jedoch niemals rückdatiert.

7.1.1 Versionsnummer

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

7.1.2 Zertifikatserweiterungen

7.1.2.1 Root-CA-Zertifikate

Es werden ausschließlich die folgenden Zertifikatserweiterungen gesetzt:

- **authorityKeyIdentifier** (optional): Enthält „keyIdentifier“ gem. [RFC5280 #4.2.1.1].
- **subjectKeyIdentifier**: Enthält „keyIdentifier“ gem. [RFC5280 #4.2.1.2].
- **keyUsage** (kritisch): Enthält „keyCertSign“ und „cRLSign“
- **basicConstraints** (kritisch): Das „cA“-Flag wird auf „true“ gesetzt. Die „pathLenConstraint“ wird nicht gesetzt.

7.1.2.2 Sub-CA-Zertifikate

Es werden ausschließlich die folgenden Zertifikatserweiterungen gesetzt:

- **authorityKeyIdentifier**: Enthält „keyIdentifier“ gem. [RFC5280 #4.2.1.1].
- **subjectKeyIdentifier**: Enthält „keyIdentifier“ gem. [RFC5280 #4.2.1.2].
- **keyUsage** (kritisch): Enthält „keyCertSign“ und „cRLSign“
- **certificatePolicies**: Enthält diejenigen Policy-OIDs gemäß Kapitel 7.1.6, welche unter der jeweiligen Sub-CA ausgestellt werden dürfen. Alternativ wird die Policy-OID „anyPolicy“ (2.5.29.32.0) gesetzt, um keine derartige Einschränkung vorzunehmen. Sub-CA-Zertifikate werden jedoch in jeden Fall zur Ausstellung von nur einem Zertifikatstyp ([TLS] oder [SMIME]) verwendet. Der Qualifier cPSuri wird optional gesetzt und beinhaltet eine entsprechende http-URL auf eine CPS oder ein Repository.
- **basicConstraints** (kritisch): Das „cA“-Flag wird auf „true“ gesetzt. Die „pathLenConstraint“ wird auf „0“ gesetzt.
- **extendedKeyUsage**:
  - [TLS] Sub-CA-Zertifikate enthalten „id-kp-serverAuth“ und optional „id-kp-clientAuth“.
  - [SMIME] Sub-CA-Zertifikate enthalten „id-kp-emailProtection“ und optional „id-kp-clientAuth“ .
- **cRLDistributionPoints**: Enthält mindestens eine http-URL auf die CRL der ausstellenden CA. Teilweise sind zusätzliche Einträge für LDAP vorhanden.

- **authorityInfoAccess**: Enthält jeweils eine entsprechende http-URL zu accessMethod 1.3.6.1.5.5.7.48.1 (ocsp) und accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers).
  Teilweise sind zusätzliche Einträge für LDAP vorhanden.

7.1.2.3 Endteilnehmer-Zertifikate

Es werden ausschließlich die folgenden Zertifikatserweiterungen gesetzt:

- **authorityKeyIdentifier**: Enthält „keyIdentifier“ gem. RFC5280 #4.2.1.1.
- **subjectKeyIdentifier**: Enthält „keyIdentifier“ gem. RFC5280 #4.2.1.2.
- **keyUsage** (kritisch):
  - [TLS] Enthält „digitalSignature“ und optional „keyEncipherment“ (nur RSA Schlüssel) oder „keyAgreement“ (nur ECC Schlüssel).
  - [SMIME] Enthält eine dem jeweiligen Verwendungszweck entsprechende Kombination aus den Werten „digitalSignature“, „keyEncipherment“ und „dataEncipherment“ gemäß [RFC5280].
- **certificatePolicies**: Gemäß Kapitel 7.1.6. Der Qualifier cPSuri wird gesetzt und beinhaltet eine entsprechende http-URL auf eine CPS oder ein Repository mit CPS.
- **subjectAlternativeName**: Gemäß Kapitel 7.1.4
- **basicConstraints** (kritisch): Die Erweiterung wird optional gesetzt. Wenn sie gesetzt wird, so wird das „cA“-Flag auf „false“ und die „pathLenConstraint“ nicht gesetzt.
- **extendedKeyUsage**:
  - [TLS] Enthält „id-kp-serverAuth“ und optional „id-kp-clientAuth“.
  - [SMIME] Enthält „id-kp-emailProtection“ und optional „id-kp-clientAuth“.
- **cRLDistributionPoints**: Enthält mindestens eine http-URL auf die CRL der ausstellenden CA.
  - [SMIME] Enthält optional weitere Einträge für LDAP.
- **authorityInfoAccess**: Enthält jeweils eine entsprechende http-URL zu accessMethod 1.3.6.1.5.5.7.48.1 (ocsp) und accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers).
- [SMIME] Enthält optional weitere Einträge für LDAP.
- **cabfOrganizationIdentifier**: [EVCP], [QEVCP-w] Inhalt und Syntax gemäß [EVCG#9.8.2].
- **signedCertificateTimestampList**: [TLS] Enthält SCTs aus verschiedenen CT-Logs gemäß den Vorgaben der relevanten Root Stores hinsichtlich Anzahl der SCTs und anerkannter CT-Log-Server unterschiedlicher Organisationen.
- **qcStatements**: [QEVCP-w] Gemäß ETSI EN 319 412-5.
- **Microsoft-spezifische Erweiterungen**: [SMIME] Enthält ggf. zusätzlich die Microsoft-spezifischen Zertifikatserweiterungen
  - certificateTemplate und
  - applicationCertPolicies.

7.1.3 Algorithmen-OID

Es werden zur Signatur von Zertifikaten, CARLs, CRLs sowie OCSP-Antworten ausschließlich die folgenden Algorithmen verwendet:

- sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
- sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13)
- RSASSA-PSS (OID 1.2.840.113549.1.1.10)
  - MGF-1 with SHA-256 and a salt length of 32 bytes
  - MGF-1 with SHA-384 and a salt length of 48 bytes
  - MGF-1 with SHA-512 and a salt length of 64 bytes
- ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)
- ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)

Zertifikate zu RSA-Schlüsseln enthalten die OID 1.2.840.113549.1.1.1 (rsa-Encryption) in der subjectPublicKeyInfo.

Zertifikate zu ECDSA-Schlüsseln enthalten die OID 1.2.840.10045.2.1 (ecPublicKey) und zusätzlich die OID 1.2.840.10045.3.1.7 (prime256v1) bzw. 1.3.1.32.0.34 (secp384r1) der verwendeten Kurve in der subjectPublicKeyInfo.

Die in [BR#7.1.3] und [MOZRP#5.1] genannten Encodings werden eingehalten.

7.1.4 Namensformen

Grundsätzlich gilt, dass

- in allen Zertifikaten der Name des Ausstellers („Issuer-DN“) identisch (byte-for-byte) zum „Subject-DN“ des ausstellenden CA-Zertifikats gesetzt wird,
- die Attribute commonName, organizationIdentifier, organizationName, countryName maximal einmal gesetzt werden,
- nicht nur Metadaten (bspw. Leerzeichen, „n/a“ oder „-“) gesetzt werden.

7.1.4.1 Root-CA-Zertifikate

Es werden ausschließlich die folgenden Attribute gesetzt:

- **commonName**: Enthält einen eindeutig vergebenen Namen, welcher die Zugehörigkeit zur Deutschen Telekom AG oder einer verbundenen Organisation reflektiert.
- **organizationName**: Enthält den Organisationsnamen der Deutschen Telekom AG oder einer verbundenen Organisation.
- **countryName**: Enthält immer den Wert „DE“.

In Bestandszertifikaten sind ggf. weitere Attribute gesetzt, bspw. **organizationalUnitName**.

7.1.4.2 Sub-CA-Zertifikate

Es werden ausschließlich die folgenden Attribute gesetzt:

- **commonName**: Enthält einen unter der jeweiligen Root-CA eindeutig vergebenen Namen, welcher die Zugehörigkeit zur Deutschen Telekom AG oder einer verbundenen Organisation reflektiert.
- **organizationName**: Enthält den Organisationsnamen der Deutschen Telekom AG oder einer verbundenen Organisation.
- **countryName**: Enthält immer den Wert „DE“.

In Bestandszertifikaten sind ggf. weitere Attribute gesetzt, bspw. **organizationalUnitName**.

7.1.4.3 Endteilnehmer-Zertifikate

Alle Endteilnehmer-Zertifikate enthalten einen subjectAltName und einen subjectDN gemäß Kapitel 3.1.

Es werden ausschließlich die folgenden Inhalte für die jeweils angegebenen Zertifikatstypen gesetzt:

subjectAltName:

- [TLS] Enthält mindestens einen Eintrag des Typs dNSName bzw. iPAddress gemäß Validierung. Es werden keine interne Namen (Definition gemäß [BR]), reservierte IP-Adressen oder .onion-Domains aufgenommen. FQDNs bestehen aus P-Labels oder Non-Reserved LDH-Labels.
- [SMIME] Enthält mindestens eine E-Mail-Adresse als RFC822Name gemäß Validierung. Darüber hinaus werden ggf. weitere Namen (bspw. UPN) gesetzt.

subjectDistinguishedName:

- **commonName**
  - [TLS] Enthält genau einen im subjectAltName gelisteten FQDN bzw. eine IP-Adresse.
  - [SMIME] Enthält den Namen der natürlichen Person, Organisation oder eine im subjectAltName gelistete E-Mail-Adresse.
- **emailAddress**
  [SMIME] Wird optional gesetzt und enthält eine im subjectAltName gelistete E-Mail-Adresse.
- **givenName + surname**
  [SMIME] Enthält für natürliche Personen den jeweiligen Vor- und Nachnamen gemäß Validierung, sofern kein Pseudonym gesetzt wird. Namen mit nur einem Namensbestandteil werden im surname aufgeführt.
- **pseudonym**
  [SMIME] Das Attribut wird optional und unter Berücksichtigung von Kapitel 3.1.3 gesetzt. Wenn es gesetzt wird, werden die Attribute givenName und surname nicht gesetzt.
- **streetAddress + postalCode**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] Die Attribute werden optional und gemäß Validierung gesetzt.
- **localityName + stateOrProvinceName**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] Es wird mindestens eins der Attribute gemäß Validierung gesetzt.
- **countryName**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] Enthält den ISO-3166-1 Ländercode (zwei Zeichen) gemäß Validierung. Bei Verwendung von Pseudonymen (nur SMIME) wird alternativ der Wert „DE“ (Land des Sitzes der Telekom Security) gesetzt.
- **organizationIdentifier**
  [SMIME] Enthält für juristische Personen oder organisatorische Einheiten in Verbindung mit juristischen Personen einen Wert gemäß [TSCP#7.1.4].
- **organizationName**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] Enthält den gemäß Kapitel 3.2.2 validierten Organisationsnamen. Bei Bedarf können gebräuchliche Abkürzungen verwendet werden und die Rechtsform kann entfallen, sofern die Eindeutigkeit der Organisation erhalten bleibt.
- **organizationalUnitName**
  [SMIME] Das Attribut wird optional gesetzt und enthält gemäß Kapitel 3.2.2 validierte Namen von Affiliates des Subjekts.
- **businessCategory**
  [EVCP], [QEVCP-w] Gemäß [TSCP#7.1.4] bzw. [EVCG#9.2.3].
- **jurisdictionOfIncorporationLocalityName, -StateOrProvinceName, -CountryName**
  [EVCP], [QEVCP-w] Gemäß [TSCP#7.1.4] bzw. [EVCG#9.2.4].
- **serialNumber**
  - [EVCP], [QEVCP-w] Gemäß [TSCP#7.1.4] bzw. [EVCG#9.2.5].
  - [SMIME] Das Attribut wird optional gesetzt, um ggf. unterschiedliche Entitäten mit ansonsten gleichen subjectDistinguishedNames zu unterscheiden.

7.1.5 Namensbeschränkungen

Es werden keine Namensbeschränkungen gesetzt.

7.1.6 OIDs der Erweiterung „CertificatePolicies“

[TLS] Es werden die jeweiligen Policy-OIDs gemäß [BR] bzw. [EVCG] gesetzt. Diese werden in Abhängigkeit vom Trust Service optional durch die jeweiligen Policy-OIDs gemäß ETSI und/oder die spezifischen OIDs

- 1.3.6.1.4.1.7879.13.23.1 (für OV)

- 1.3.6.1.4.1.7879.13.24.1 (für EV)

der Telekom Security ergänzt.

[QEVCP-w] Für qualifizierte Website-Zertifikate wird zusätzlich die entsprechende Policy-OID gemäß ETSI gesetzt.

[SMIME] Es werden die jeweiligen Policy-OIDs gemäß [SBR] gesetzt. Diese werden in Abhängigkeit vom Trust Service optional durch die jeweiligen Policy-OIDs gemäß ETSI und/oder die spezifische OID

- 1.3.6.1.4.1.7879.13.26 (Deutsche Telekom Corporate PKI)

der Telekom Security 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“

Wenn ein Policy Qualifier gesetzt ist, enthält dieser einen Verweis auf das entsprechende CPS (CPSuri).

7.1.9 Verarbeitungssemantik für die kritische Erweiterung „Certificate Policies“

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

7.2 Sperrlistenprofile

Alle Sperrlisten werden gemäß den Anforderungen des [RFC5280] ausgestellt und von der jeweiligen CA selbst 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
- expiredCertsOnCRL (optional)

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

- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- [SMIME] certificateHold (6) (nur für Deutsche Telekom AG)

- privilegeWithdrawn (7)

Die CRLReason keyCompromise (1) hat Vorrang gegenüber allen anderen Sperrgründen und Sperrgründe werden ggf. nachträglich auf keyCompromise geändert, wenn eine Kompromittierung des Schlüssels nachträglich bekannt wird.

Sollte für ein TLS-Zertifikat kein Sperrgrund bekannt sein, also CRLReason unspecified (0) zutreffen, so wird die Sperrlisteneintragserweiterung reasonCode nicht gesetzt.

7.3 OCSP-Profil

Alle OCSP-Antworten werden gemäß den Anforderungen des [RFC6960] ausgestellt und von einem delegierten OCSP-Signer signiert. Die OCSP-Signer-Zertifikate werden von der jeweiligen CA mit einer kurzen Gültigkeit ausgestellt und enthalten die Erweiterung id-pkix-ocsp-nocheck.

OCSP-Antworten für gesperrte Zertifikate enthalten den Sperrgrund im Attribut revocationReason innerhalb der RevokedInfo. Hinsichtlich der Sperrgründe gelten die in Abschnitt 7.2.2 gemachten Angaben.

7.3.1 Versionsnummer(n)

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

7.3.2 OCSP-Erweiterungen

OCSP-Signer, welche Statusinformationen zu qualifizierten Zertifikaten bereitstellen, verwenden die Erweiterung ArchiveCutOff. Weitere Erweiterungen werden nicht gesetzt.

8 AUDITS UND ANDERE BEWERTUNGS-KRITERIEN

8.1 Häufigkeit und Art der Prüfungen

Es werden von externen Auditoren jährlich Audits gemäß Kapitel 8.4 durchgeführt. Die Audit-Perioden schließen direkt aneinander an, überschreiten nicht die Dauer eines Jahres und bilden eine ununterbrochene Folge, von der Erzeugung eines CA-Schlüsselpaares bis zu dessen Zerstörung und dem Entzug des Vertrauens ("Cradle-to-Grave").

Darüber hinaus werden alle Schlüsselgenerierungen und Zertifikatsausstellungen für alle CAs, welche im Geltungsbereich dieser CPS liegen, durch externe Auditoren überwacht und attestiert.

Durch interne Auditoren werden monatliche Selbstüberprüfungen durchgeführt, welche stichprobenartig eine zufällige Auswahl von mindestens einem Zertifikat (TLS) bzw. 30 Zertifikaten (SMIME) und mindestens 3% der seit der letzten Prüfung ausgestellten Zertifikate betreffen (6% bei [EVCP]).

Die Praktiken von externen RAs werden stichprobenartig geprüft.

8.2 Identität/Qualifikation der Prüfer

Externe Prüfungen gemäß Kapitel 8.1 werden von qualifizierten Auditoren durchgeführt, die über folgende Qualifikationen und Fähigkeiten verfügen:

- Die Auditoren sind unabhängig vom Prüfgegenstand
- Die Auditoren können Prüfungen durchführen, welche die in geeigneten Prüfungsschemata gemäß Kap. 8.4 festgelegten Kriterien erfüllen,
- Die Auditoren sind kompetent in der Prüfung von PKI-Technologien, Informationssicherheits-Tools und -Techniken, Informationstechnologien und Sicherheitsüberprüfungen und beherrschen die Funktion der Bestätigung als Drittpartei.
- Die Auditoren sind durch Gesetz, staatliche Vorschriften oder berufsethische Regeln gebunden.
- Die Auditoren unterhalten eine Berufshaftpflicht-, Fehler- und Unterlassungsversicherung mit einer Deckungssumme von mindestens einer Million US-Dollar.
- Die Prüfstelle ist gemäß ISO 17065 unter Anwendung der in ETSI EN 319 403 festgelegten Anforderungen bei der „DAkkS“ (Deutsche Akkreditierungsstelle) akkreditiert und Mitglied des „ACAB’c“ (Accredited Conformity Assessment Bodies‘ Council).

Interne Auditoren, welche die in Kapitel 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 AG und dem Prüfgegenstand sind.

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

8.4 Abgedeckte Bereiche der Prüfung

Die Trust Services der Telekom Security im Geltungsbereich dieser CPS inklusive aller dazugehörigen CAs werden gemäß ETSI EN 319 411-1 bzw. ETSI EN 319 411-2 in der jeweils aktuellen Version geprüft.

In Abhängigkeit vom Trust Service werden die ETSI-Policies NCP, LCP, DVCP, OVCP, EVCP oder QEVCP-w angewendet.

Für qualifizierte Trust Services umfasst das Audit zusätzlich die Konformitätsbewertung nach [eIDAS].

8.5 Maßnahmen infolge von Mängeln

Werden Mängel festgestellt, welche Verstöße gegen die [BR], [SBR], [EVCG], [MSRP], [MOZRP], [GCRP] oder [APLRP] darstellen, so werden diese schnellstmöglich den jeweiligen Root-Programmen gemeldet.

Darüber hinaus werden festgestellte Mängel schnellstmöglich beseitigt. Hierbei werden konzerninterne sowie, im Falle von Audits nach ETSI, die je Finding vorgegeben Fristen eingehalten.

8.6 Mitteilung der Ergebnisse

Die von externen Prüfern gemäß [CCADB#5.1] erstellten Audit Bescheinigungen aller CAs werden unverzüglich, spätestens jedoch innerhalb von 3 Monaten nach Ende der Prüfung in der „Common CA Database“ (CCADB) veröffentlicht. Sollte die Frist von 3 Monaten nicht eingehalten werden können, wird das Trust Center ein vom externen Prüfer unterzeichnetes Erläuterungsschreiben vorlegen.

Konformitätsbewertungsberichte für qualifizierte Dienste werden innerhalb von drei Tagen nach Erhalt an das Bundesamt für Sicherheit in der Informationstechnik (BSI) übermittelt.

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 Leistungsbeschreibungen bzw. 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 erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts und sind in den Allgemeinen Geschäftsbedingungen oder sonstigen vertraglichen Vereinbarungen konkretisiert.

9.2 Finanzielle Verantwortlichkeiten

9.2.1 Versicherungsschutz

Die Telekom Security verfügt über die Deutsche Telekom AG über einen hinreichenden Betriebs- und Vermögenshaftpflichtversicherungsschutz gemäß [TSCP#9.2.1].

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 zur [TSCP] konformen Betrieb inkl. einer geplanten Einstellung gemäß Kapitel 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 Trust Services gelten als vertrauliche Informationen, sofern sie nicht gemäß Kapitel 9.3.2 explizit als nicht vertrauliche Informationen eingestuft wurden.

9.3.2 Umfang an nicht vertraulichen Informationen

Alle in Kapitel 2.2 genannten Informationen sowie sämtliche Informationen in veröffentlichten Zertifikaten werden als öffentlich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Telekom Security unterliegt den konzernweiten Richtlinien der Deutsche 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 Konzernvorgaben verpflichtet.

9.4 Schutz von personenbezogenen Daten

9.4.1 Datenschutzkonzept

Die Deutsche Telekom AG hat zur Einhaltung aller Vorgaben der Datenschutz-Grundverordnung [DSGVO] konzernweite Richtlinien zum Umgang mit personenbezogenen Daten festgelegt und entsprechende Schutzklassen 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 privat behandelt.

9.4.3 Nicht als privat zu behandelnde Informationen

Nicht als privat zu behandelnde 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 Zertifizierungsstellenbetreiber

Telekom Security sichert die in [TSCP#9.6.1] geforderten Zusicherungen und Gewährleistungen zu. Insbesondere sichert Telekom Security einen zuverlässigen, vertrauenswürdigen, diskriminierungsfreien und legalen Betrieb der Trust Services sowie die Einhaltung der Konformität zur [TSCP] zu. Die Trust Services 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.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Telekom Security sichert die in [TSCP#9.6.2] geforderten Zusicherungen und Gewährleistungen der RAs zu.

Externe RAs werden vertraglich an die Einhaltung der in [TSCP#9.6.2] geforderten Zusicherungen und Gewährleistungen gebunden und regelmäßig auf Konformität geprüft (siehe Kapitel 8.1). Die Gesamtverantwortung liegt jedoch weiterhin bei der Telekom Security.

9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsnehmer

Die Zusicherungen und Gewährleistungen der Zertifikatnehmer sowie die bereitzustellenden Informationen sind in [TOUP] bzw. [TOUC] definiert, die von den Zertifikatnehmern bei der Beantragung eines Zertifikats akzeptiert werden müssen. [TOUP] und [TOUC] berücksichtigen alle Anforderungen aus [TSCP#9.6.3].

9.6.4 Zusicherungen und Gewährleistungen vertrauender Dritter

Es existieren keine vertraglichen Vereinbarungen mit vertrauenden Dritten. In den Nutzungsbedingungen bzw. PKI Disclosure Statements sind jedoch Empfehlungen an Dritte 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 Allgemeinen Geschäftsbedingungen oder anderen anwendbaren vertraglichen Vereinbarungen geregelt.

9.8 Haftungsbeschränkungen

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

Mit delegierten Dritten sind hinsichtlich Haftung entsprechend vertragliche Vereinbarungen getroffen, die Gesamtverantwortung verbleibt jedoch bei Telekom Security.

Etwaige Haftungsbeschränkungen gemäß geltendem Recht werden in den Allgemeinen Geschäftsbedingungen oder anderen anwendbaren vertraglichen Vereinbarungen geregelt.

9.9 Schadensersatz

Etwaige Schadenersatzansprüche gegenüber der Telekom Security werden in den Allgemeinen Geschäftsbedingungen oder anderen anwendbaren vertraglichen Vereinbarungen geregelt.

9.10 Laufzeit und Aufhebung

9.10.1 Laufzeit

Dieses CPS gilt ab dem auf dem Deckblatt angegebenen Gültigkeitsdatum, bis es durch eine neue Version ersetzt wird (maximal ein Jahr, siehe Kapitel 9.12).

9.10.2 Aufhebung

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

9.10.3 Effekt einer Aufhebung und Fortführungen

Keine Bestimmungen.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Bestimmungen.

9.12 Änderungen

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 PKI Compliance Management des Trust Centers regelmäßig die zugrundeliegenden Anforderungen der in der [TSCP#Anhang B] referenzierten Anforderungsquellen auf neue Versionen und verfolgt relevante Foren und Mailing-Listen.

Änderungen an diesem CPS sowie das jährliche Review werden in der Änderungshistorie dieses Dokuments aufgeführt und es wird eine neue Versionsnummer vergeben, auch wenn es im Rahmen des jährlichen Reviews zu keinerlei inhaltlichen Änderungen kam. Die Freigabe neuer Versionen geschieht gemäß Kapitel 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 werden gemäß Kapitel 2 veröffentlicht.

Neue Versionen der Nutzungsbedingungen, die sich auf die Akzeptanz eines Dienstes durch die Zertifikatsnehmer oder auf Vertrauende Dritte auswirken könnten, werden rechtzeitig den Zertifikatsnehmern, Vertrauenden Dritten und, sofern anwendbar, Bewertungsstellen und Aufsichts- oder anderen Regulierungsbehörden bekannt gegeben.

9.12.3 Umstände, unter denen der OID geändert werden muss

Wenn sich Änderungen an diesem CPS ergeben, welche sich auf die Anwendbarkeit auswirken, 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.