ERKLÄRUNG ZUM ZERTIFIZIERUNGSBETRIEB (CERTIFICATION PRACTICE STATEMENT, CPS) DER SHARED-BUSINESS-CA

TELESEC SHARED-BUSINESS-CA

DEUTSCHE TELEKOM SECURITY GMBH

VERSION:	13.00
GÜLTIG AB:	30.04.2021
STATUS:	FREIGABE
KLASSIFIZIERUNG:	ÖFFENTLICH
LETZTE ÜBERPRÜFUNG:	28.04.2021

IMPRESSUM

HERAUSGEBER

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

Telefon: 0228 181-0
E-Mail: info@telekom.de
Internet: www.telekom.de/security
Pflichtangaben: www.telekom.com/pflichtangaben-dtsec

Aufsichtsrat: N.N (Vorsitzender)
Geschäftsführung: Thomas Fetten (Sprecher), Dr. Klaus Schmitz, Thomas Tschersich

Handelsregister: Amtsgericht Bonn HRB 15241
Sitz der Gesellschaft Bonn
Umsatzsteuer-Identifikationsnummer. DE 254595345
WEEE-Register-Nummer DE 56768674

Kurzinformation:	Dieses Dokument beschreibt die Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA des PKI-Service TeleSec Shared-Business-CA.
Dateiname:	Shared-Business-CA_CPS_13.00_DE.docx
Dokumentennummer:	n.n.
Dokumentenbezeichnung:	Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA des PKI-Service TeleSec Shared-Business-CA.
Version:	13.00
Gültig ab:	30.04.2021
Status:	Freigabe
Klassifizierung:	Öffentlich
Letzte Überprüfung:	28.04.2021
Autor:	Telekom Security
Inhaltlich geprüft:	Telekom Security
Freigegeben von:	Telekom Security, Leiter TC Produkte, Netphen, 02.03.2021
Ansprechpartner:	tc-solutions.lastlevel@t-systems.com

ÄNDERUNGSHISTORIE

VERSION:	STAND:	BEARBEITER:	ÄNDERUNGEN / KOMMENTAR:
1.0	06.04.2010	UV	Finale Abstimmung
1.1	01.07.2012	CD, UV	Einarbeiten der Anforderungen der Baseline Requirements des CA/Browser Forums in der Version 1.0
01.20	27.03.2013	UV	Vollständige Überarbeitung
01.21	02.07.2013	UV	Einarbeitung Änderungen von Lothar Eickholt
02.00	18.07.2013	AT	Freigabe dieser Version
02.10	07.04.2014	UV	Überarbeitung der Kapitel 1.1.1, 1.2, 1.3.1.1, 1.3.1.2, 2.2, 3.1.1, 3.1.1.2 bis 3.1.1.14, 3.2.2, 3.2.5.1, 3.2.5.2, 4.5.1, 4.6.1, 4.9.1, 5.5.2, 7.1.2.9, 7.1.3, 7.1.6.2, 7.2, 7.3, 9.2, 9.9, 9.16.5, A.1, A.2, C.1, Entfernung des Kapitels 1.3.1.3, Einfügen eines neuen Kapitels 3.1.1.15
02.20	04.04.2014	LE	Qualitätssicherung der Vers. 02.10 und Freigabe dieser Version
02.30	22.04.2016	UV	Vollständige Überarbeitung
02.31	19.05.2016	VM, MS, UV	Qualitätssicherung der Vers. 02.30
03.00	20.05.2016	ME	Freigabe dieser Version
03.10	21.04.2017	UV	Überarbeitung
03.20	09.05.2017	LE	Qualitätssicherung, Überarbeitung der Kapitel 3.1.1.1, 3.1.1.1.1, 3.1.1.1.8, 3.1.1.1.9, 4.1.2.2.2 und 4.9.1
04.00	15.05.2017	UV	Freigabe und Veröffentlichung dieser Version
04.10	14.05.2018	UV	Überarbeitung der Kapitel 1, 1.3.1.1.1, 1.3.1.1.2, 1.3.1.2.1, 1.3.1.2.2, 1.5.3, 1.5.4, 2.2, 2.3, 3.1.1, 3.1.1.1, 3.1.1.1.1, 3.1.1.1.6, 3.1.1.1.8, 3.1.1.1.9, 3.1.1.1.12, 3.1.3, 3.1.6, 3.2.2.1, 3.2.3.1, 3.2.3.2, 3.2.5.3, 3.3, 4.1.1, 4.1.2.2.2, 4.2.1.2, 4.2.2, 4.2.2.1.1, 4.2.2.1.2, 4.2.2.2, 4.3.1.1, 4.3.1.2, 4.4.2, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.3, 4.9.1.1, 4.9.1.2, 4.9.2, 4.9.3.1, 4.9.3.2.1, 4.9.3.3.2, 4.9.3.5, 4.10.1, 5, 5.1.1, 5.2, 5.3.3.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.8, 5.5.1, 5.5.2, 5.6, 5.8.2, 6.3.2, 6.5, 7.1, 7.1.11, 7.3, 7.3.1, 8, 8.4, 8.6, 9.4.1, 9.7, 9.8.1, 9.8.2, 9.9, C.1, C.2, Ergänzung der Kapitel 3.2.2.2 ff, 4.4.4, 7.1.2.9.1, 7.1.2.9.2 Auswechselung Bild 2
04.20	15.05.2018	UV	Freigabe abgebrochen
04.30	04.06.2018	LE	Anpassung DSGVO
05.00	07.06.2018	UV	Freigabe und Veröffentlichung dieser Version
05.10	24.07.2018	UV	Überarbeitung der Kapitel
05.20	15.08.2018	UV	Änderungen kenntlich gemacht und zur Abnahme an den TÜV gesendet.
05.30	02.10.2018	LE	Kapitel 1.3.1, 1.5.2, 2.1, 2.2, 2.4 und 3.1.1.1.6 ergänzt, In den Kapiteln 3.2.2.2.1, 3.2.5.2, 3.3, 4.2.2.1.1 und 6.3.2 wurde anstelle von „27 Monaten“ durch 825 Tage ersetzt, Kapitel 3.2.2.2 aktualisiert, Kapitel 3.2.5.2, 3.2.5.3, 4.1.2.2 aktualisiert, Kapitel 3.4 Internetadresse aktualisiert, Kapitel 4.3 aktualisiert, Kapitel 4.9.7, 4.9.1.1, 4.9.3.2, 4.10.1 aktualisiert, Änderungen in Kapitel 5 und 6, Kapitel 7.2 und 8 aktualisiert, Kapitel 9.17.1 hinzu gefügt, Kapitel 9.17.1 hinzu gefügt

VERSION:	STAND:	BEARBEITER:	ÄNDERUNGEN / KOMMENTAR:
05.31	11.10.2018	GK	QS für Version 06.00
06.00	11.10.2018	DD	Freigabe
06.10 bis 06.60	23.05.2019	UV, LE, AJ	Überarbeitung der Kapitel 1.2, 1.3.1.1.1, 1.3.1.1.2, 1.3.1.2.1, 1.3.1.2.2, 1.3.2.2, 1.3.2.2.2, 1.5.1, 1.5.2, 2.1, 2.2, 3.1.1.1, 3.1.1.1.6, 3.1.1.1.9, 3.1.1.1.10, 3.1.1.1.11, 3.1.1.1.12, 3.1.1.2, 3.1.1.2.3, 3.1.1.2.3, 3.1.6, 3.2.2.1, 3.2.2.2, 3.2.2.2.4.3, 3.2.2.2.4.5, 3.2.2.2.4.6, 3.2.2.2.4.7, 3.2.2.2.5, 3.2.2.2.5.1, 3.2.2.2.5.2, 3.2.2.2.5.3, 3.2.2.2.5.4, 3.2.2.2.5.5, 3.2.2.2.5.6, 3.2.2.2.5.7, 3.2.3.3, 3.2.5.1, 3.2.5.3, 4.2.1.1, 4.4.2, 4.9.1.1, 4.9.3.2, 4.9.7, 4.12, 5.1.1, 5.5.1, 5.5.2, 5.5.3, 5.7.4, 5.8.1, 6.1.1, 6.1.2, 6.1.6, 6.2, 6.2.4, 6.2.4.3, 6.2.5,, 6.2.6, 6.2.7, 6.2.8.3, 6.2.8.3, 6.2.8.4, 6.2.9, 6.5, 6.5.1.1, 7.1, 7.1.2.9.1, 7.1.2.9.2, 7.1.3, 7.1.4.1, 7.1.4.2, 7.1.4.3, 7.1.6.2, 7.1.6.3, 7.1.6.4, 7.2, 8.7, 9.6.4, 9.7
06.61	27.05.2019	GK	QS für Version 07.00
07.00	27.05.2019	ME	Zur Freigabe
07.10	21.08.2019	UV, AJ	Alle Einträge gelöscht, die die Shared Business CA 3, Shared Business CA 4 und Deutsche Telekom Root CA 2 betreffen (Kapitel 1.1.2, 1.3.1.1.1, 1.3.1.2.1, 1.3.3, 1.3.5, 1.5.4, 2.2, 3.1.1.1.5, 3.2.3.4, 3.2.4, 4.1.1, 4.2.1.2, 4.2.2.1.1, 4.2.2.2, 4.5.1, 4.9.7, 6.1.4, 6.3.2, 7.1.2.4, 7.1.2.9.1, 7.1.6.1, 8.1, 8.4, 9.6.3 und Quellennachweis) Ergänzung der Internal Business CA 5 (Kapitel 1.3.1.2.2, 2.2, 6.3.2, 7.1.2.4), Begriffsdefinitionen
07.20	21.08.2019	GK	QS für Version 08.00
08.00	23.08.2019	ME	Freigabe
08.10	05.02.2020	UV	Überarbeitung der Kapitel 1.1.1, 2.2, 3.1.1.1.1 bis 3.1.1.1.9, 3.2.2.2.4.1, 3.2.2.2.4.6, 3.2.2.2.4.12 bis 3.2.2.2.4.19, 3.2.2.2.5 ff, 4.1, 4.1.2.2.2, 4.2, 4.2.1.2, 4.4.4, 4.5.1, 4.9.1.1, 4.9.6, 4.9.9, 4.9.10, 4.9.14 bis 4.9.16, 4.10.1, 4.11, 5.2.1, 5.3.6.1, 5.4, 5.5.2, 5.8.2, 6.1.5, 6.1.6, 7.1.3, 7.1.4.3, 7.1.6.3.1 bis 7.1.6.3.3, 7.3.2, 9.6.1, C.2, Quellennachweis, Überarbeitung aller Tabellen
08.20	05.04.2020	UV	Abstimmungsversion
08.30	16.03.2020	UV	Ergänzung Abstimmungsversion in Kapitel 2.3, 3.1.1.1.6, 3.1.1.1.7, 3.1.1.1.13, 3.1.1.2, 3.2.2.2.4.7, 3.2.3 (Überschrift), 3.2.5 (Überschrift), 3.2.5.3, 3.2.6, 4.2, 4.2.2.1.2, 4.2.2.2, 4.3 (Überschrift), 4.9.1.1, 4.9.3 (Überschrift), 4.10.1, 6.2.5, 6.3, 7.1, 7.1.2.1, 7.1.2.3, 7.1.2.5, 7.1.2.9.1, 7.1.4.2, 7.1.5, 7.1.6.3.2, 8, 8.1, 8.3, 8.4, 8.6, 8.7, 9.12.1
08.40	20.03.2020	AJ	Überarbeitung der Kapitel 1.3.1.1.1, 1.3.1.1.2, 1.3.1.2.1, 1.3.1.2.2, 1.3.3, 3.1.1, 3.1.1.1.2, 3.1.1.1.6, 3.1.1.1.13, 3.1.3, 5.2.1
08.50	23.03.2020	UV	Finalisierung
08.90	23.03.2020	GK	Formale QS
09.00	23.03.2020	HH	Freigabe von Version 09.00
09.10	28.05.2020	UV	Organisationsänderung auf Deutsche Telekom Security GmbH
09.20	29.05.2020	UV	Finalisierung

VERSION:	STAND:	BEARBEITER:	ÄNDERUNGEN / KOMMENTAR:
09.30	29.05.2020	GK	Formale QS
10.00	03.06.2020	HH	Freigabe von Version 10.00
10.10	09.06.2020	UV	Änderung Kurzname Telekom Security
10.20	16.06.2020	UV	Überarbeitung der Kapitel 1.1.1, 1.1.2, 1.3.1, 1.3.1.3.2, 1.3.2.2.1, 1.3.2.2.2, 1.3.4, 2.1, 3.2.2.1, 3.3, 4.1.2.2.1, 4.1.2.2.2, 4.2.1.1, 5.4.1.3, 5.5.1, 5.5.2, 5.5.5, 6.1.1, 6.2.3, 6.2.4, 6.2.4.2, 6.2.4.3, 6.2.5, 6.3.2, 6.4.2.2, 6.5.2, 8.7, Anlage A, Anlage B
10.90	31.08.2020	Telekom Security	Formale QS
11.00	31.08.2020	Telekom Security	Freigabe von Version 11.00
11.10	26.01.2021	Telekom Security	Trennung CP/CPS, u.a. neu Kapitel 1.1.3
11.20	01.03.2021	Telekom Security	QS
11.90	02.03.2021	Telekom Security	Formale QS
12.00	02.03.2021	Telekom Security	Freigabe von Version 12.00
12.10	16.04.2021	Telekom Security	Überarbeitung Kapitel 5.7.1 und 6.5.2
12.20	28.04.2021	Telekom Security	Überarbeitung Kapitel 4.9.12
12.90	29.04.2021	Telekom Security	Formale QS
13.00	29.04.2021	Telekom Security	Freigabe von Version 13.00

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 EINLEITUNG

Das Trust Center wird durch die Konzerneinheit Deutsche Telekom Security GmbH (im Folgenden „Telekom Security“ genannt) betrieben, die nach einem Betriebsübergang aus der T-Systems International GmbH zum 01.07.2020 entstand.

Das Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Wurzel-Instanzen (Roots) für unterschiedliche elektronische Zertifikate. Die Zertifizierungsstellen der Zertifikats-Dienstleistungen unterscheiden sich hinsichtlich der Anwendungskontexte für Zertifikate, der konkreten Ausprägung der technischen Schnittstellen, Registrierungsverfahren, der Zertifikatsprofile, der Prozesse bei Sperrungen, sowie der Veröffentlichung von Informationen.

Im Jahre 2013 wurde ein Informations-Sicherheits-Managementsystem (ISMS) für das Trust Center etabliert. Das ISMS stellt Verfahren und Regeln zur Verfügung, um die Informationssicherheit zielgerichtet zu steuern, zu kontrollieren, zu überprüfen, dauerhaft verbessern zu können und aufrecht zu erhalten.

1.1 Überblick

1.1.1 PKI-Service TeleSec Shared-Business-CA

TeleSec Shared-Business-CA (im Folgenden auch „SBCA“ genannt) ist eine zentral, im Trust Center der Telekom Security, betriebene PKI-Dienstleistung zur Generierung und Verwaltung von unterschiedlichen X.509v3-Zertifikatstypen, die insbesondere Einsatz finden bei E-Mail-Security, starker Authentifizierung (Client-Server), Remote-VPN, Servern und aktiven Netzkomponenten (z.B. Router, Gateways).

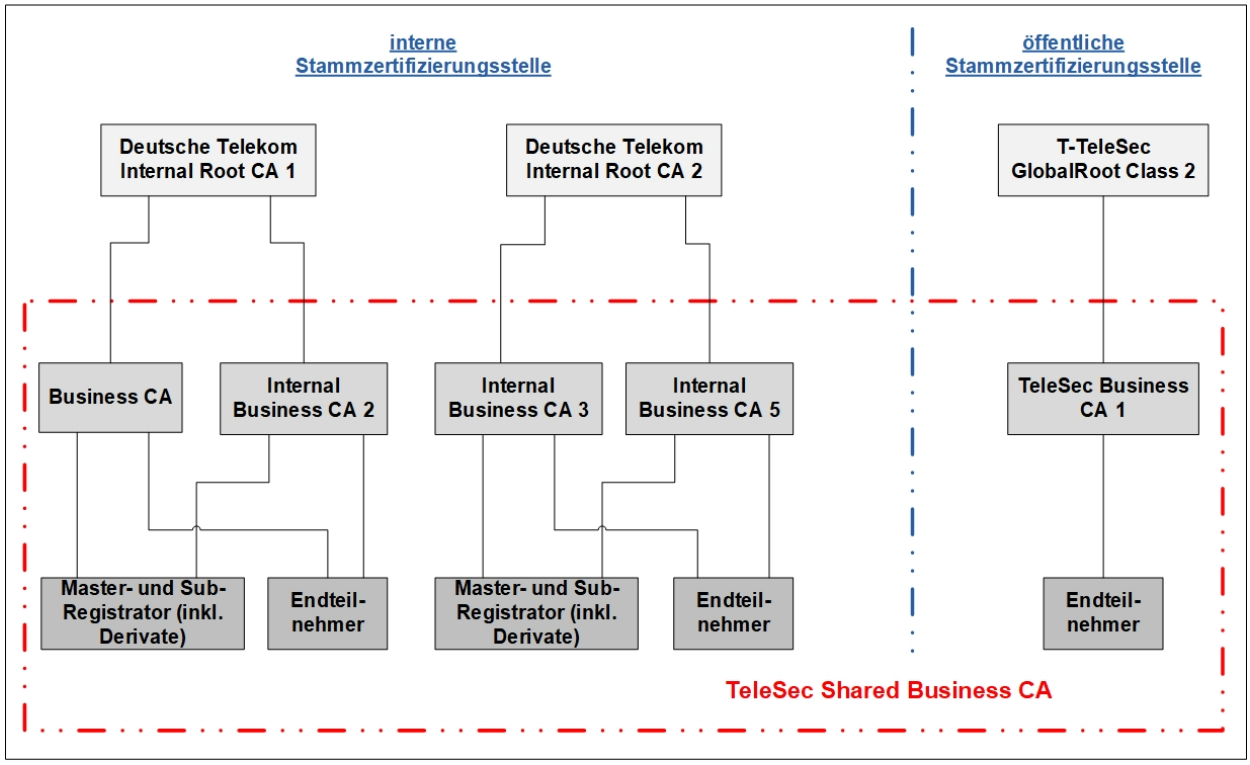
Mit TeleSec Shared-Business-CA (SBCA) bietet die Telekom Security dem Kunden eine vollständige PKI-Lösung an, dessen Infrastruktur im hochsicheren Trust Center der Telekom Security installiert ist und von qualifiziertem Personal betrieben wird. Zur sicheren Abgrenzung und Verwaltung des eigenen Datenbestands erhält jeder Kunde, im Folgenden auch „Mandant“ genannt, eine eigens für ihn eingerichtete Master-Domäne. Zur Abbildung der Organisationsstruktur kann er die Master-Domäne in einzelne eigenständige Zuständigkeitsbereiche gliedern, innerhalb derer er selbst Zertifikate für Endteilnehmer (Benutzer, Geräte) beantragen und verwalten kann.

Alle Kunden erhalten einen, per zertifikatsbasierter SSL/TLS-Client-Authentifizierung gesicherten, dedizierten Zugang auf ihren eigenen PKI-Mandanten (Master-Domäne), um die PKI-Funktionen nutzen können. Alle sicherheitsrelevanten Aktionen erfolgen über eine verschlüsselte Verbindung (HTTPS).

Unter dem PKI-Service TeleSec Shared-Business-CA selbst sind unterschiedliche Zwischenzertifizierungsstellen (Intermediate-CAs, Sub-CAs) subsummiert, die auch hierarchisch unterschiedlichen Stammzertifizierungsstellen unterstehen.

In Abbildung 1 ist die Übersicht des PKI-Service „TeleSec Shared-Business-CA“ mit all ihren Stamm- und Zwischenzertifizierungsstellen (Root- und Intermediate-CAs, Sub-CAs) grafisch dargestellt. Der Geltungsbereich dieses Dokuments umfasst die im rot gestrichelten Bereich enthaltenen Zwischenzertifizierungsstellen (Intermediate-CAs, Sub-CAs) dieser Abbildung.

Abbildung 1: Übersicht der PKI-Dienstleistung „TeleSec Shared-Business-CA“ mit den jeweiligen Stamm- und Zwischenzertifizierungsstellen (Root- und Intermediate-CAs, Sub-CAs)



Für die jeweiligen Stammzertifizierungsstellen (Roots) bestehen jeweils eigene Zertifizierungsrichtlinien (engl. Certificate Policy, CP) und Erklärungen zum Zertifizierungsbetrieb (Certification Practice Statement, CPS).

Die Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) des Dienstes TeleSec Shared-Business-CA (SBCA), im Folgenden kurz „CPS“ genannt, der Telekom Security beinhaltet die Tätigkeiten des Trust Center Betreibers in der Funktion als Certification Authority (CA) und Registration Authority (RA) als auch der Registration Authority (RA) der beauftragte Drittpartei (Delegated Third Party).

Im Einzelnen behandelt diese CPS die folgenden Regelungen:

- Veröffentlichungen und Verzeichnisdienst,
- Authentifizierung von PKI Teilnehmern,
- Ausstellung von Zertifikaten,
- Erneuerung von Zertifikaten (Re-Zertifizierung),
- Sperrung und Suspendierung von Zertifikaten,
- bauliche und organisatorische Sicherheitsmaßnahmen,
- technische Sicherheitsmaßnahmen,
- Zertifikatsprofile,
- Auditierung,
- Verbindliche Hinweise zur Zertifikatsnutzung und –prüfung
- verschiedene Rahmenbedingungen.

Der formale Aufbau dieser CPS folgt dem internationalen Standard RFC3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ [RFC3647] der Internet Society.

Rechtliche und kommerzielle Aspekte der TeleSec Shared-Business-CA werden vertraglich geregelt.

1.1.2 Einhaltung der Baseline Requirements des CA/Browser-Forums

Das Trust Center der der Telekom Security stellt sicher, dass die Root-CA „T-TeleSec GlobalRoot Class 2“ mit den jeweiligen untergeordneten Zwischenzertifizierungsstellen die Anforderungen und Regelungen der jeweils aktuellen veröffentlichten Version der [CAB-BR] (https://cabforum.org/baseline-requirements/) erfüllen und einhalten.

Im Falle eines Widerspruchs zwischen dem vorliegenden Dokument und den [CAB-BR] haben die Regelungen aus den [CAB-BR] Vorrang.

1.1.3 Einhaltung der übergreifenden Zertifizierungsrichtline des Trust Centers

Das Trust Center sichert zu, dass für TeleSec Shared-Business-CA die Anforderungen der übergreifenden Zertifizierungsrichtline des Trust Centers der Telekom Security [Trust Center CP] mit der OID 1.3.6.1.4.1.7879.13.42) umgesetzt sind bzw. eingehalten werden. Die [Trust Center CP] (ist im Internet veröffentlicht unter https://www.telesec.de/de/service/downloads/pki-repository/).

Im Falle eines Widerspruchs zwischen dem vorliegenden Dokument und den [Trust Center CP] haben die Regelungen aus den [Trust Center CP] Vorrang.

1.2 Name und Kennzeichnung des Dokuments

Das vorliegende Dokument stellt die CPS des PKI-Dienstes TeleSec Shared-Business-CA der der Telekom Security dar.

Name:	Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA
Version:	13.00
Gültig ab:	30.04.2021
Letzte Überprüfung:	28.04.2021
OID dieser CPS:	1.3.6.1.4.1.7879.13.25

1.3 PKI-Beteiligte

1.3.1 Zertifizierungsstellen

Die Zertifizierungsstelle (Certification Authority, CA) ist der Teil einer Public Key Infrastruktur, die Zertifikate ausstellt, verteilt und Prüfmöglichkeiten (Validierung) zur Verfügung stellt. Die Zwischenzertifizierungsstelle ihrerseits oder weitere Zwischenzertifizierungsstellen unterstehen hierarchisch einer Stammzertifizierungsstelle (Root-CA), die den „Vertrauensanker“ (Root-CA-Zertifikat) darstellt.

Für TeleSec Shared-Business-CA stehen, je nach Anforderung, unterschiedliche Stamm- und Zwischenzertifizierungsstellen (Root-CAs, Sub-CAs) zur Verfügung. Anforderungen an die Stammzertifizierungsstellen sowie an die von der Stammzertifizierungsstelle ausgestellten Zertifikate der Zwischenzertifizierungsstelle sind im CP/CPS der jeweiligen Root-CA dokumentiert.

Zwischenzertifizierungsstellen, die nicht mehr produktiv Endteilnehmer-Zertifikate ausstellen, werden bis auf weiteres noch für die Signatur von Sperrlisten und/oder OCSP-Antworten verwendet.

Die Stammzertifizierungsstelle und die korrespondierende Zwischenzertifizierungsstelle kann variieren,

- wenn in der verwendeten Anwendung (z.B. Webbrowser) das Zertifikat der Stammzertifizierungsstelle noch nicht als vertrauenswürdig implementiert ist, oder

- wenn die verwendete Anwendung (z.B. Webbrowser) einer Validierungslogik folgt, die nicht auf die direkte Stammzertifizierungsstelle prüft.

In diesen Fällen wird optional auf eine andere definierte Stammzertifizierungsstelle referenziert.

Das Validierungsmodell basiert auf dem Schalenmodell, d.h. jedes Zertifikat ist maximal so lange gültig, wie das darüber liegende ausstellende Zertifikat gültig ist.

1.3.1.1 Stammzertifizierungsstelle

1.3.1.1.1 Öffentliche Stammzertifizierungsstellen

Regelungen zur öffentlichen Stammzertifizierungsstelle sind in der CP bzw. CPS der „T-TeleSec GlobalRoot Class 2“ [CP/CPS Class2] dokumentiert.

In Tabelle 1 sind die vollständigen Issuer- und Subject Distuinguished Names (Issuer DN, Subject DN) der genannten Zertifizierungsstellen gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch deren Zertifikats-Gültigkeit dargestellt.

Tabelle 1: Subject DN „T-TeleSec GlobalRoot Class 2“

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	T-TeleSec GlobalRoot Class 2
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	T-TeleSec GlobalRoot Class 2
Signaturhashalgorithmus:	SHA-256
Gültig von:	01.10.2008
Gültig bis:	01.10.2033
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	91 E2 F5 78 8D 58 10 EB A7 BA 58 73 7D E1 54 8A 8E CA CD 01 45 98 BC 0B 14 3E 04 1B 17 05 25 52
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	59 0d 2d 7d 88 4f 40 2e 61 7e a5 62 32 17 65 cf 17 d8 94 e9

1.3.1.1.2 Interne Stammzertifizierungsstelle

Regelungen zur internen Stammzertifizierungsstelle sind in der CP/CPS der „Deutsche Telekom Internal Root CA 1“ [CP/CPS DTIRCA1] und „Deutsche Telekom Internal Root CA 2“ [CP/CPS DTIRCA2] dokumentiert.

In Tabelle 2 und Tabelle 3 sind die vollständigen Issuer- und Subject Distuinguished Names (Issuer DN, Subject DN) der genannten Zertifizierungsstellen gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch deren Zertifikats-Gültigkeit enthalten.

Tabelle 2: Subject DN „Deutsche Telekom Internal Root CA 1“

Aussteller (Issuer)	
Country Name (C):	DE

Organization Name (O):	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Signaturhashalgorithmus:	SHA-1
Gültig von:	15.11.2007
Gültig bis:	15.11.2027
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	E0 1A B4 F7 CE 75 0F F4 3B FE 52 13 78 79 FE 11 A0 83 66 CE 9C C5 40 75 1A 33 38 A4 9F BB 7B D4
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	15 33 9a a2 30 f5 34 0e 7b fc aa fd 75 4a a1 4c ed d4 98 58

Tabelle 3: Subject DN „Deutsche Telekom Internal Root CA 2“

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Signaturhashalgorithmus:	SHA-256
Gültig von:	03.08.2017
Gültig bis:	03.08.2037
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	C3 2A E6 04 47 39 1E 48 63 C2 44 55 1D EB C8 7B 40 FF 51 80 45 19 3E E4 67 33 86 57 9D 50 D0 FD
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	12 f7 14 bd ec 4d 2e 3c 27 82 ce 1f cb 8a fe 19 b8 4a ed 8c

1.3.1.2 Zwischenzertifizierungsstellen

1.3.1.2.1 Zertifizierungsstellen unterhalb einer öffentlichen Stammzertifizierungsstelle

Endteilnehmer-Zertifikate (z.B. für Benutzer, Server), deren Verwendungszweck eine „öffentliche Stammzertifizierungsstelle (Public Root)“ erfordert, werden von den folgenden untergeordneten Zertifizierungsstellen (Zwischenzertifizierungsstellen) ausgestellt:

- TeleSec Business CA 1

Im Falle, dass der Verwendungszweck von Zertifikaten nicht den Vorgaben einer „öffentlichen Stammzertifizierungsstelle“ genügen (z.B. zur Verwaltung des PKI-Mandanten, Router, Domain-Controller), oder Vorgaben bzw. Vorschriften (z.B. Root-Programme der Betriebssystem- und Browserhersteller, Baseline Requirements des CA/Browser-Forums [CAB-BR]) dies einschränken oder verhindern, werden diese Zertifikate von einer Zwischenzertifizierungsstelle ausgestellt, die hierarchisch der „Deutsche Telekom Internal Root CA 1“ oder „Deutsche Telekom Internal Root CA 2“untersteht.

Der Common Name (CN) des Ausstellers (Issuer) referenziert auf die zuständige Stammzertifizierungsstelle.

In Tabelle 4 sind die vollständigen Issuer- und Subject Distuinguished Names (Issuer DN, Subject DN) der genannten Zertifizierungsstellen gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch deren Zertifikats-Gültigkeit enthalten.

Tabelle 4: Issuer und Subject DN „TeleSec Business CA 1“

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	T-TeleSec GlobalRoot Class 2
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	TeleSec Business CA 1
Signaturhashalgorithmus:	SHA-256
Gültig von:	29.11.2012
Gültig bis:	29.11.2024
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	44 EB F0 12 3E 27 FF 1D B0 49 7B D2 DA E1 81 55 B2 A4 14 E6 BC D9 C6 C8 FB 8F 48 39 84 49 B9 E9
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	57 a8 c5 b5 26 0e 20 63 53 d4 c3 46 e3 f6 09 39 e4 f8 b8 59

1.3.1.2.2 Zertifizierungsstelle unterhalb einer internen Stammzertifizierungsstelle

Endteilnehmer-Zertifikate (z.B. für Registratoren, Benutzer (SmartCard-LogOn), Router/Gateway, Domain-Controller), die die Verwendung einer „internen Stammzertifizierungsstelle (Internal Root)“ genügen, werden von folgenden untergeordneten Zertifizierungsstellen (Zwischenzertifizierungsstellen) ausgestellt:

- Internal Business CA 3

- Internal Business CA 5
- Internal Business CA 2
- Business CA

Der Common Name (CN) des Ausstellers (Issuer) referenziert auf die zuständige Stammzertifizierungsstelle.

In Tabelle 5 bis Tabelle 8 sind die vollständigen Issuer- und Subject Distuinguished Names (Issuer DN, Subject DN) der genannten Zertifizierungsstellen gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch deren Zertifikats-Gültigkeit enthalten.

Tabelle 5: Issuer und Subject DN "Internal Business CA 2"

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
State (S):	Nordrhein Westfalen
PostalCode:	57250
Locality (L):	Netphen
Street:	Untere Industriestr. 20
Common Name (CN):	Internal Business CA 2
Signaturhashalgorithmus:	SHA-256
Gültig von:	11.02.2014
Gültig bis:	15.11.2027
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	F1 50 C0 1B 68 79 11 62 59 01 F1 1E 71 AD D8 EB DE 58 10 D8 3E 92 F4 96 F8 B5 0E 24 82 6A 65 B5
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	68 19 96 1d d2 59 10 16 b7 ec e0 c6 6f 2b 04 78 08 7f 11 44

Tabelle 6: Issuer und Subject DN „Business CA"

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	T-Systems Trust Center

Common Name (CN):	Business CA
Signaturhashalgorithmus:	SHA-1
Gültig von:	08.11.2011
Gültig bis:	08.11.2023
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	DD 9B C2 05 FC 9C 72 0D C9 C5 2E 62 59 34 E6 6F 56 10 41 68 01 78 6F F2 9A C1 9B 68 DE 7F 77 54
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	8b 52 1b 55 f0 be 1c 79 50 ca a5 d4 af 37 06 a2 60 b6 35 50

Tabelle 7: Issuer und Subject DN “Internal Business CA 3”

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Internal Business CA 3
Signaturhashalgorithmus:	SHA-256
Gültig von:	03.08.2017
Gültig bis:	03.08.2029
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	6F 32 57 FE 69 12 70 37 65 DE 86 59 F1 37 51 6B 53 99 A3 8A 72 93 7D 1C AB 94 1D DC 4B EC 9C 85
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	ee fa 12 59 ca d4 93 a3 c8 04 a3 2f ac 18 59 b4 31 0c e5 18

Tabelle 8: Issuer und Subject DN “Internal Business CA 5”

Aussteller (Issuer)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Antragsteller (Subject)	
Country Name (C):	DE
Organization Name (O):	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Internal Business CA 5
Signaturhashalgorithmus:	SHA-256

Gültig von:	10.09.2019
Gültig bis:	10.09.2031
Fingerabdruckalgorithmus:	SHA-256
Fingerabdruck:	81 13 F5 8B 3C 55 4B D4 18 88 87 54 11 6C 79 1D 6F D0 4A B6 B0 81 57 63 FB 4A 0C 45 E9 2F DB CB
Fingerabdruckalgorithmus:	SHA-1
Fingerabdruck:	cc 78 ef 3c 34 89 38 df 05 7b 1d 1f 4f 9a b6 7e ae 3c b1 68

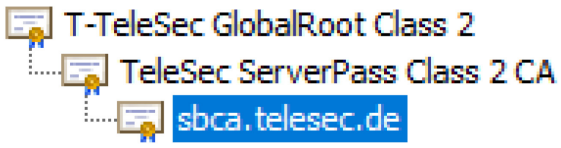
1.3.1.3 Zertifikate zur Unterstützung des PKI-Betriebs

1.3.1.3.1 Web-Server des PKI-Service „TeleSec Shared-Business-CA“

Der Zugriff des Mandanten auf die PKI-Funktionen der SBCA erfolgt über das Internet. Der Web-Server der SBCA ist mit einem SSL-Zertifikat ausgestattet, so dass alle Aktionen über das sichere Protokoll HTTPS erfolgen. Die Funktionen werden nach erfolgreicher rollenbasierter Authentifizierung bereitgestellt.

In Abbildung 2 ist die Zertifikatshierarchie des Web-Servers „sbca.telesec.de“ mit dem jeweiligen Zertifikat der Stammzertifizierungsstelle (Root-CA) und der Zwischenzertifizierungsstelle dargestellt.

Abbildung 2: Übersicht der Zertifikatshierarchie des Webservers „sbca.telesec.de“



1.3.1.3.2 OCSP-Responder des PKI-Service „TeleSec Shared-Business-CA“

Von jeder Zwischenzertifizierungsstelle werden für die Erbringung des OCSP-Service Zertifikate für den OCSP-Responder ausgestellt. Dieser Zertifikatstyp steht ausschließlich nur dem PKI-Betreiber der Telekom Security zur Verfügung.

Technische Details zu OCSP sind in den Kapiteln 7.3 ff beschrieben.

1.3.2 Registrierungsstellen

Eine Registrierungsstelle (Registration Authority, RA) ist eine Stelle, die die Authentifizierung von Zertifikatsantragstellern durchführt, Zertifikatsanträge bearbeitet (genehmigt, ablehnt, zurückgestellt), Sperranträge bearbeitet oder weiterleitet, ggf. Zertifikatserneuerungen als auch eine Sicherungskopie des Schlüsselmaterials (Soft-PSE) für einen Antragsteller erstellt.

Grundsätzlich muss jede Registrierungsstelle gewährleisten, dass kein Unberechtigter in den Besitz eines entsprechenden Zertifikats gelangt.

Im Rahmen des PKI-Service TeleSec Shared-Business-CA sind folgende Registrierungsstellen etabliert:

- Interne Registrierungsstelle, der Telekom Security, und
- Externe Registrierungsstelle(n), die bei den Mandanten betrieben werden.

1.3.2.1 Interne Registrierungsstelle

Die interne Registrierungsstelle wird durch die vertrauenswürdige Rolle (Trusted Role) des Trust-Center-Operator wahrgenommen, der im Trust Center der Telekom Security lokalisiert ist. Weitere interne Registrierungsstellen sind nicht etabliert.

Die interne Registrierungsstelle hat insbesondere folgende Aufgaben:

- Entgegennahme von Aufträgen und Prüfung der Identifikationsunterlagen zur Einrichtung (Konfiguration) der Master-Domäne(n) bzw. PKI-Mandanten,
- Einrichtung der Master-Domäne(n) und Ausstellung von Master-Registrator-Zertifikaten auf Smartcard zur Verwaltung des Mandanten,
- Konfiguration und Konfigurationsänderungen der Master-Domäne(n) nach erfolgreicher Prüfung der Identifikationsunterlagen,
- Ausstellung von weiteren Master-Registrator-Zertifikaten auf Smartcard,
- Sperrung von Master-Registrator-Zertifikaten.

Die interne Registrierungsstelle darf auch Master-Domänen-übergreifend Master-Registrator-, Sub-Registrator- und Endteilnehmer-Zertifikate sperren, sofern der Mandant dies beauftragt hat oder missbräuchliche Verwendung zu vermuten bzw. nachgewiesen ist.

Damit übernimmt diese Registrierungsstelle übergeordnete Funktionen und zeigt sich für die Zulassung und den Widerruf untergeordneter Registrierungsstellen verantwortlich, die bei den Mandanten lokalisiert sind.

1.3.2.2 Externe Registrierungsstelle

Die externe Registrierungsstelle wird durch die vertrauenswürdigen Rollen (Trusted Roles) des Master-Registrators und Sub-Registrators wahrgenommen, der beim Mandanten oder vom Mandanten bevollmächtigten Dritten lokalisiert ist. Weitere externe Registrierungsstellen sind nicht etabliert.

Die externe Registrierungsstelle hat insbesondere folgende Aufgaben:

- Entgegennahme von Zertifikatsanträge innerhalb des definierten Verantwortungsbereiches,
- Prüfung der Anträge nach den vorgegebenen Richtlinien (z.B. Arbeitsanweisung),
- Beantragung des Zertifikats/ der Zertifikate in Folge der Freigabe eines Zertifikatsantrags, oder
- Freigabe dieser Zertifikatsanträge nach erfolgreicher Prüfung, ansonsten Ablehnung oder Zurückstellung (Wiedervorlage) des Antrags,
- Entgegennahme des/der von der SBCA erzeugten Zertifikat(e) und Übergabe an den Zertifikatsinhaber bzw. eine autorisierte Person,
- Entgegennahme und Prüfung von Zertifikatssperrungsaufträgen innerhalb des definierten Verantwortungsbereiches oder ggf. Weiterleitung dieser an die interne Registrierungsstelle oder Service Desk,
- Durchführung einer Zertifikatssperrung als Folge einer positiven Prüfung eines Sperrauftrags, und
- Generierung einer neuen und damit aktuellen Zertifikatssperrliste (CRL).

Die externe Registrierungsstelle (Externe RA), auch als „beauftragte Drittpartei“ bezeichnet, wird betrieblich und vertraglich dem Trust Center Betrieb zugeordnet und unterliegt den Regelungen dieser CPS. Ob die Registrierungsstelle dabei nur Zertifikate für das eigene Unternehmen/Unternehmensverbund ausstellt (Enterprise RA) oder auch für Dritte, ist nicht relevant.

1.3.2.2.1 Master-Registrator

Der Master-Registrator stellt die hierarchisch oberste Rolle einer externen Registrierungsstelle dar und liegt in der Verantwortung des Mandanten. Die Verwaltungsfunktionen stehen über der Master-Registrator-Webseite zur Verfügung. Das Master-Registrator-Zertifikat wird von der Telekom Security ausschließlich auf einer Smartcard ausgestellt (siehe Kapitel 1.3.2.1).

Der Master-Registrator hat insbesondere folgende Aufgaben:

- Vertretung des Mandanten gegenüber der Zertifizierungsstelle,
- Einrichtung, Konfiguration und Verwaltung von Zuständigkeitsbereichen (Sub-Domänen),
- Ausstellung von Sub-Registrator-Zertifikaten für Personen, die der Mandant bestimmt,
- Sperrung von Sub-Registrator-Zertifikaten nach Vorliegen eines Sperrgrundes/Sperrantrags,
- Sperrung von Endteilnehmer-Zertifikaten nach Vorliegen eines Sperrgrundes/Sperrantrags.

Die externe Registrierungsstelle liegt in der vollständigen Verantwortung des Mandanten. Mit dem Master-Registrator-Zertifikat authentisiert sich der Benutzer an der Master-Registrator-Webseite. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

1.3.2.2.2 Sub-Registrator

Der Sub-Registrator stellt hierarchisch die unterste als auch operative Rolle der externen Registrierungsstelle dar und liegt in der Verantwortung des Mandanten. Die Funktionen (z.B. Ausstellung, Genehmigung, Sperrung, Erneuerung von Zertifikaten) stehen nach erfolgreicher zertifikatsbasierender SSL/TLS-Client-Authentifizierung an der Sub-Registrator-Webseite zur Verfügung. Das Sub-Registrator-Zertifikat wurde vom Master-Registrator auf Smartcard oder als Soft-PSE bereitgestellt (siehe Kapitel 1.3.2.2.1, 6.1.1, 6.4.2.2).

Der Sub-Registrator hat insbesondere folgende Aufgaben:

- Authentifizierung von Antragstellern,
- Genehmigung, Ablehnung oder Wiedervorlage von Zertifikatsanträgen nach erfolgreicher Identitätsprüfung (siehe auch Dezentrale Registrierung, Kapitel 3.2.3),
- Beantragung und Abruf von Endteilnehmer-Zertifikaten nach erfolgreicher Identitätsprüfung (siehe auch Zentrale Registrierung, Kapitel 3.2.3),
- Sperrung von Endteilnehmer-Zertifikaten nach Vorliegen eines Sperrgrundes/Sperrantrags.

Das vom Master-Registrator ausgestellte Sub-Registrator-Zertifikat (inkl. Derivate) enthält einen für die SBCA eindeutigen Namen (Common Name).

Diese Registrierungsstelle liegt in der vollständigen Verantwortung des Mandanten. Mit dem Sub-Registrator-Zertifikat autorisiert sich dieser an der Sub-Registrator-Webseite. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

Als weitere optionale Funktion steht eine Schnittstelle zur Verfügung, die auf dem Protokoll CMP (Certificate Management Protocol) basiert und Zertifikats-Management von X.509-Zertifikaten innerhalb einer Public-Key-Infrastruktur (PKI) unterstützt.

In Bezug auf die TeleSec Shared-Business-CA bietet die Zertifizierungsstelle (CA) eine Server-basierende Schnittstelle, die von einer beim Mandanten (externe Registrierungsstelle (RA)) befindlichen Anwendung (Client) angesprochen werden kann, um Zertifikate beantragen, sperren und erneuern zu können (weitere Details sind im Dokument „Leistungsbeschreibung TeleSec Shared-Business-CA“ beschrieben).

Um über die CMP-Schnittstelle interagieren zu können, muss sich der „CMP-Client“ des Mandanten per zertifikatsbasierter SSL/TLS-Client-Authentifizierung anmelden.

Folgendes Derivate des Sub-Registrators steht dafür zur Verfügung:

- Sub-RA-CMP

Für dieses Zertifikats-Derivat besteht die Option der Rollentrennung. Bei Aktivierung dieser Rollentrennung kann die CMP-Rolle keine weiteren Rollen (Sub-RA, Sub-RA-PWD, Sub-RA-P12) zugewiesen werden. Bei einer Deaktivierung dieser Rollentrennung ist das CMP-Zertifikat auch als Sub-RA-Zertifikat nutzbar.

In den nachfolgenden Kapiteln werden diese Rollen bzw. Zertifikatstypen auch als „Derivate“ der Sub-Registratoren bezeichnet.

1.3.3 Endteilnehmer (End Entity)

Im Kontext der TeleSec Shared-Business-CA werden unter Endteilnehmer alle Zertifikatsnutzer verstanden, auf die ein Zertifikat ausgestellt werden kann und selbst keine Rolle einer Zertifizierungsstelle repräsentieren. Diese sind im Einzelnen:

- Benutzerzertifikate
  - natürliche Personen
  - Pseudonym
  - Juristische Personen
  - Personen- Funktionsgruppen und Rollen
  - Roboter und Automaten
- Gerätezertifikate
  - Server
  - Router
  - Gateways
  - Mail-Gateways
  - Domain-Controller

Um den technischen Anforderungen gerecht zu werden, bietet SBCA für die Endteilnehmer unterschiedliche Zertifikatstypen an. Tabelle 9 bis Tabelle 15 zeigt die Zuordnung der Zertifikatstypen zu den verschiedenen Endteilnehmer an.

Tabelle 9: Zuordnung Zertifikatstyp Benutzer zu Endteilnehmer

Zertifikatstyp:	Benutzer
Anwendungsgebiet (beispielhaft):	Mail-Security (S/MIME), Anmeldung als TLS/SSL-Client an einer Web-basierenden Anwendung/Appliance, Anmeldung an einem Microsoft-Netzwerk, Anmeldung an einer Citrix-Appliance
Endteilnehmer:	natürliche Personen, Pseudonym, Juristische Personen, Personen- Funktionsgruppen und Rollen, Roboter und Automaten

Tabelle 10: Zuordnung Zertifikatstyp Server zu Endteilnehmer

Zertifikatstyp:	Server
Anwendungsgebiet (beispielhaft):	TLS/SSL-Server-Authentifikation
Endteilnehmer:	Gerätezertifikate

Tabelle 11: Zuordnung Zertifikatstyp Router/Gateway zu Endteilnehmer

Zertifikatstyp:	Router/Gateway
Anwendungsgebiet (beispielhaft):	VPN, Authentifikation innerhalb von Router-Netzwerken
Endteilnehmer:	Gerätezertifikate

Tabelle 12: Zuordnung Zertifikatstyp Mail-Gateway zu Endteilnehmer

Zertifikatstyp:	Mail-Gateway
Anwendungsgebiet (beispielhaft):	Virtuelle Poststelle, Authentifikation eines Mail-Gateway/Appliance
Endteilnehmer:	Gerätezertifikate

Tabelle 13: Zuordnung Zertifikatstyp Domain-Controller zu Endteilnehmer

Zertifikatstyp:	Domain-Controller
Anwendungsgebiet (beispielhaft):	Authentifikation der Anmeldestelle innerhalb eines Microsoft-Netzwerks
Endteilnehmer:	Gerätezertifiakte

Zertifikate für Rolleninhaber Master-Registrator bzw. Sub-Registrator sind immer Zertifikatstypen vom Sub-Typ „natürliche Personen“.

In den folgenden Kapiteln wird weitestgehend der Namen des Zertifikatstyps als Synonym für den jeweiligen Endteilnehmer verwendet. D.h. unter Benutzer-Zertifikaten werden die Zertifikate für natürliche Personen, Personen- und Funktionsgruppen, Pseudonym, Rolleninhaber subsummiert, unter Geräte-Zertifikaten werden alle Server-, Router/Gateway-, Mail-Gateway und Domain-Controller-Zertifikate verstanden!

Zertifikate für OCSP-Responder fallen auch unter Endteilnehmer, werden aber an dieser Stelle nicht weiter berücksichtigt, da sie nur zur Erbringung des Service TeleSec Shared-Business-CA verwendet, nicht aber dem Kunden zur Verfügung gestellt werden.

Der Verwendungszweck der Endteilnehmer-Zertifikate ist beschrieben in dem Kapitel 1.4.1.2. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

Im Gegensatz zu natürlichen Personen stimmt im Falle von Geräten das Subjekt (Zertifikatantragssteller) nicht mit dem Endteilnehmer überein, auf das sich das Zertifikat bezieht. Das Subjekt ist entweder der Zertifikatnehmer oder ein Gerät, das der Kontrolle des Zertifikatnehmers untersteht oder von diesem betrieben wird. Der Endteilnehmer ist Inhaber des privaten und öffentlichen Schlüssels und trägt die letztendliche Verantwortung für den Gebrauch und die Sicherung des privaten Schlüssels und des zugehörigen Zertifikats. Im Falle von natürlichen Personen stellt der Endteilnehmer gleichzeitig auch das Subjekt dar.

Als Endteilnehmer ist nicht die Institution Auftraggeber/Vertragspartner oder Mandanten (z.B. Musterfirma) zu verstehen. Es ist aber dennoch möglich, dass auf diesen Repräsentanten auch ein Endteilnehmer-Zertifikat ausgestellt wird (z.B. Max Mustermann als Vertretungsberechtigter für Musterfirma).

Welche Bedeutung die Verwendung der Begriffe Endteilnehmer und Subjekt im Einzelfall haben, hängt daher vom Kontext ab, in dem die Begriffe verwendet werden.

1.3.4 Vertrauender Dritter

Ein vertrauender Dritter (Relying Parties) ist eine natürliche Person oder Subjekt, die/das sich auf die Vertrauenswürdigkeit des von der SBCA gemäß der Darstellung in dieser CPS ausgestellten Zertifikats und/oder digitalen Signatur verlässt.

Unter Vertrauende Dritte werden auch beispielsweise Software-Hersteller verstanden, die Zertifikate der Stamm- und Zwischenzertifizierungsstellen der SBCA in die Zertifikatsspeicher integrieren.

1.3.5 Andere Teilnehmer

Eine Personen- und Funktionsgruppe als auch ein Gerät wird jeweils durch eine autorisierte Person verantwortet, die für diese Aufgabe vom Mandanten bevollmächtigt ist. Die autorisierte Person wird wie eine natürliche Person identifiziert und registriert. Die autorisierte Person ist verantwortlich für die sichere Verteilung, Nutzung und ggf. Sperrung des Zertifikats. Im Falle, dass die autorisierte Person nicht für die Verteilung oder Sperrung verantwortlich sein soll, wird diese Funktion auf den Rolleninhaber „Schlüsselverantwortlichen“ übertragen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Zertifikate der SBCA dürfen nur im zulässigen und geltenden gesetzlichen Rahmen verwendet werden. Dies gilt insbesondere unter Beachtung der länderspezifischen geltenden Ausfuhr- und Einfuhrbestimmungen.

1.4.1.1 Sicherheitsniveau

Bei Zertifikaten mit mittlerem Sicherheitsniveau handelt es sich um Zertifikate, die sich für die Sicherung verschiedenster Geschäftsprozesse (z.B. digitale Signatur und Verschlüsselung von E-Mails) innerhalb und außerhalb Firmen, Organisationen, Behörden und Institutionen eignen, die ein mittleres Sicherheitsniveau zum Nachweis der Authentizität, Integrität und Vertraulichkeit des Endteilnehmers erfordern. Ferner sind die Zertifikate geeignet zur Endteilnehmer-Authentifizierung an Applikationen und Netzen oder zur Authentifizierung aktiven Netzwerkkomponenten untereinander.

1.4.1.2 Zertifikate für Benutzer und Geräte

Diese Zertifikatstypen werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Erweiterungen „Schlüsselverwendung“ und „Erweiterte Schlüsselverwendung“ und den Festlegungen der CPS eingesetzt.

Voraussetzung ist aber, dass ein Vertrauender Dritter dem Zertifikat in angemessener Weise vertrauen kann und der Verwendungszweck nicht durch gesetzlich oder auf Grund von Einschränkungen der „Telekom Security CP“ oder sonstigen Vereinbarungen verboten ist. Einige Beispiele sind:

- Authentifizierung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPSec, XML-SIG, SOAP),
- Authentifizierung im Rahmen von Prozessen (Windows Log-On, Festplattenverschlüsselung),
- Verschlüsselung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPSec, S/MIME, XML-ENC, SOAP),
- Digitale Signatur im Rahmen von Kommunikationsprotokollen (z.B. S/MIME)

In Tabelle 14 ist das Sicherheitsniveaus bezogen auf die Verwendungszwecke dargestellt.

Tabelle 14: Sicherheitsniveau bezogen auf Verwendungszweck

Sicherheitsniveau:	Mittel
Verwendungszweck:	Signatur und/oder Verschlüsselung
Verwendungszweck:	Authentifizierung

1.4.2 Unzulässige Verwendung von Zertifikaten

Zertifikate der SBCA dürfen nicht im Rahmen folgender Zwecke verwendet werden:

- Steuerungs- und Kontrolleinrichtungen in gefährlichen Umgebungen,
- Umgebungen, in denen ein ausfallsicherer Betrieb gefordert ist (z.B. der Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder -kommunikationssystemen, Luftverkehrs-Kontrollsystemen oder Waffenkontrollsystemen), wobei ein Ausfall zu Schäden (z.B. Personenschäden, Tod, mittleren und schweren Umweltschäden, sonstige Katastrophen) führen kann.

Es ist verboten Endteilnehmer-Zertifikate als CA- oder Root-CA-Zertifikate zu verwenden.

1.5 Verwaltung der Richtlinie

1.5.1 Zuständigkeit für die Erklärung

Diese CPS wird herausgegeben von:

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

1.5.2 Kontaktinformationen

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

Telefon: +49 (0) 1805-268204
Festnetz: 0,14 €/Minute, Mobilfunknetz: max. 0,42 €/Minute
E-Mail: telesec_support@t-systems.com
Internet: https://www.telesec.de/de/service/kontakt/anfragemitteilung

Die Meldung von Missbrauch, Kompromittierung von Zertifikaten und Schlüsseln des Trust Center der Telekom Security können unter der URL https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden 7x24h abgesetzt werden. Eine möglichst präzise und umfangreiche Darstellung sollte im Feld „Text“ erfolgen, so dass eine Bewertung durch Telekom Security frühzeitig erfolgen kann und adäquate Maßnahmen eingeleitet werden können. Telekom Security meldet sich in der Regel innerhalb von 24h mit einer ersten Einschätzung über die angegebenen Kommunikationskanäle. Telekom Security wird ggf. Strafverfolgungsbehörden und Aufsichtsbehörden einschalten. Die Eingabe der Meldung wird als Einverständnis gewertet, dass Daten ohne weitere Einwilligung in einem solchen Fall an Behörden weitergegeben werden können.

1.5.3 Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP entscheidet

Der in Kapitel 1.5.1 benannte Herausgeber ist für dieses Dokument verantwortlich. Die Genehmigung erfolgt durch das Change Advisory Board des Herausgebers.

1.5.4 Genehmigungsverfahren dieser CPS

Dieses Dokument (CPS) behält seine Gültigkeit, solange es nicht vom Herausgeber (siehe Kapitel 1.5.1) widerrufen wird. Es wird bei Bedarf fortgeschrieben, und erhält dann jeweils eine neue aufsteigende Versionsnummer (siehe auch Kapitel 9.12.1 und 9.12.2).

Der in Kapitel 1.5.1 benannte Herausgeber ist für dieses Dokument (CPS) verantwortlich. Die Freigabe erfolgt durch einen formalen Dokumentenfreigabeprozess.

Relevante Änderungsanforderungen oder Änderungen des laufenden PKI-Betriebs der TeleSec Shared-Business-CA werden rechtzeitig fachlich bewertet und auf die Einhaltung dieser und der übergeordneten CP/CPS der Root-CA „T-TeleSec GlobalRoot Class 2“, „Deutsche Telekom Internal Root CA 1“ und „Deutsche Telekom Internal Root CA 2“ hin überprüft. Im Bedarfsfall werden die Änderungen in das jeweilige Dokument eingearbeitet.

1.6 Definitionen und Abkürzungen

Abkürzungen und Begriffsdefinitionen finden Sie im Anhang A: Abkürzungen und Anhang B: Glossar

Das Quellenverzeichnis finden Sie in Anhang C: Quellennachweise

2 VERANTWORTLICHKEITEN VON VERÖFFENTLICHUNGEN UND ABLAGEN

2.1 Ablagen

Telekom Security betreibt für den Dienst TeleSec Shared-Business-CA einen Verzeichnisdienst und eine zentrale Datenablage. Telekom Security ist für deren Inhalte verantwortlich.

Extrakte dieser Datenbanken stellen in aufbereiteter Form die Basis dar, um Zertifikatsinformationen und Zertifikatssperrlisten (CRL) auf dem Verzeichnisdienst zu veröffentlichen oder den Validierungsdienst (OCSP-Responder) mit Statusinformationen zu versorgen.

Weiterhin werden für die Öffentlichkeit relevante Dokumente in Form einer zentralen Datenablage (Repository) zur Verfügung gestellt. Dies umfasst insbesondere die entsprechenden CP/CPS Dokumente der beteiligten Stamm- und Zwischenzertifizierungsstellen. Dieses Verzeichnis ist 7x24h Stunden verfügbar. Die Ausfallzeit beträgt maximal 1,5 Tage im monatlichen Mittel.

Telekom Security setzt geeignete Mechanismen zum Schutz der zentralen Datenablage (Repository) gegen nicht autorisierte Manipulationsversuche (hinzufügen, löschen, ändern) ein.

2.2 Veröffentlichung von Zertifikatsinformationen

TeleSec Shared-Business-CA veröffentlicht folgende Informationen über https://www.telesec.de/de/sbca:

- Diese Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA des PKI-Service TeleSec Shared-Business-CA in der aktuellen und vorherigen Versionen (https://www.telesec.de/de/service/downloads/pki-repository).
- Die PKI-Offenlegungspflichten unter https://www.telesec.de/de/service/downloads/pki-repository
- Alle Root- und korrespondierende Sub-CA-Zertifikate, die im PKI-Service TeleSec Shared-Business-CA Verwendung finden (https://www.telesec.de/de/root-programm/root-programm/ueberblick).
- Downloadbereich für
  - Leistungsbeschreibung TeleSec Shared-Business-CA
  - Allgemeine Geschäftsbedingungen (AGB) TeleSec-Produkte

  unter https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen
- Wichtige Informationen
  - Neuigkeiten zum PKI-Service TeleSec Shared-Business-CA https://www.telesec.de/de/produkte/shared-business-ca/ankuendigungen

Zusätzlich werden alle Master-Registratoren informiert bei

- der Kompromittierung oder Verdacht auf Kompromittierung des privaten Schlüssels einer Root-CA- oder Sub-CA,
- der Außerbetriebnahme der Root-CA oder Sperrung einer Sub-CA,
- sicherheitsrelevanten Änderungen dieser Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA.

Zusätzlich erfolgen bei sicherheitskritischen Vorfällen eine direkte Benachrichtigung der Master-Registratoren und zusätzlich bekannte Ansprechpartner des PKI-Mandanten in schriftlicher Form oder per E-Mail.

TeleSec Shared-Business-CA bietet über den Link https://www.telesec.de/de/root-programm/support/pki-service-ermitteln eine Umkehrsuche an. Nach dem Hochladen eines Endteilnehmer-Zertifikats (binär oder base64-kodiert) werden folgende Informationen angezeigt:

- Aussteller (Issuer-DN)
- Antragsteller (Subject-DN)
- Zertifikatsseriennummer
- Gültigkeitsbeginn
- Gültigkeitsende
- Länge des öffentlichen Schlüssels (Bit)
- Signaturalgorithmus
- Link zur Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Shared-Business-CA
- Link zur Leistungsbeschreibung
- Link zur Allgemeinen Geschäftsbedingung (AGB)
- Link zu den PKI-Offenlegungspflichten und Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA
- Link zu den CA-Zertifikaten

Hinweis: Die Umkehrsuche wird derzeit nur mit den Browsern (Vollversionen) Mozilla Firefox und Google Chrome unterstützt.

Telekom Security veröffentlicht in regelmäßigen Abständen Zertifikatssperrlisten (CRL), in der alle von der SBCA gesperrten Zertifikate mit Sperrdatum und -zeitpunkt enthalten sind. Es werden nur Zertifikate gesperrt, die zum Sperrzeitpunkt gültig sind.

In der Sperrliste für Zertifizierungsstellen (CARL) werden alle gesperrten CA-Zertifikate (jedoch keine Root-CA-Zertifikate) veröffentlicht.

Die Sperrlistenverteilpunkte sind in den ausgestellten Zertifikaten hinterlegt und über http und einen Verzeichnisdienst (LDAP) erreichbar.

Der Verzeichnisdienst hat die Aufgabe, an einem zentralen Ort alle zur Veröffentlichung anstehenden Zertifikate als auch die aktuellen Sperrinformationen per Standard-konformer Sperrlisten (CRL, CARL), für alle PKI-Beteiligten zur Verfügung zu stellen. Der Zugriff auf den Verzeichnisdienst erfolgt über das Protokoll LDAP (Lightweight Directory Access Protocol) und ist hinsichtlich Zugriffsschutz konfigurierbar (öffentlich oder Benutzername/Passwort-Schutz). Eine LDAP-Suchanfrage, die mehrere Ergebnisse zurück liefert, unterliegen einer Mengenbeschränkung (size limit).

Telekom Security veröffentlicht ausschließlich Benutzer- und Mail-Gateway-Zertifikate auf einem öffentlichen Verzeichnisdienst, sofern der Mandant dieser Veröffentlichung zugestimmt hat.

Über eine Benutzer-Webseite können Endteilnehmer Zertifikate anderer Mandanten suchen, sofern die Veröffentlichung von diesen gestattet ist.

Folgende Zertifikatstypen werden nicht veröffentlicht:

- Master-Registrator-Zertifikate
- Sub-Registrator-Zertifikate und deren Derivate
- Geräte-Zertifikate (Router-/Gateway-, Domain-Controller-Zertifikate, Server)

Server-Zertifikate, die eine CT-Log-Eintrag enthalten (Kapitel 4.4.2), werden über Log-Server von Dritten (z.B. Google) veröffentlicht.

Ferner stellt SBCA einen Validierungsdienst (OCSP-Responder) zur Verfügung, der über das Internetprotokoll „Online Certificate Status Protocol“ (OCSP) einem Anfragenden den Status von SBCA-Zertifikaten zurück liefert.

Die Adresse des OCSP-Responders ist im Zertifikat eingetragen und wird zusätzlich im Dokument „Zertifikats- und Konfigurationsdatenblatt der TeleSec Shared-Business-CA“ veröffentlicht. Die jeweiligen OCSP-Zertifikate stehen nicht zum Herunterladen per Webseite zur Verfügung.

Weitere Details zu CA-Zertifikaten finden sich in Tabelle 15.

Tabelle 15: Vorgaben für die Veröffentlichung von Zertifikaten (Produktion (SBCA-PU))

Zertifikatstyp:	**Vorgaben:**
Root-CA-Zertifikat „T-TeleSec GlobalRoot Class 2“	Dieses Zertifikat ist in den Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert bzw. wird online nachinstalliert und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.
Sub-CA-Zertifikat „TeleSec Business CA 1“	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „T-TeleSec GlobalRoot Class 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.
Root-CA-Zertifikat „Deutsche Telekom Internal Root CA 1“	Dieses Zertifikat ist nicht in den Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert, sondern muss zusätzlich nachinstalliert werden. Das Root-CA-Zertifikat unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.
Root-CA-Zertifikat „Deutsche Telekom Internal Root CA 2“	Dieses Zertifikat ist nicht in den Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert, sondern muss zusätzlich nachinstalliert werden. Das Root-CA-Zertifikat unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.
Sub-CA-Zertifikat „Business CA“	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 1“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.

Sub-CA-Zertifikat „Internal Business CA 2“	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 1“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.
Sub-CA-Zertifikat „Internal Business CA 3“	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.
Sub-CA-Zertifikat „Internal Business CA 5“	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und Vertrauenden Dritten. Ggf. kann das Zertifikat über den Verzeichnisdienst der SBCA oder per Internet abgerufen werden.

Zusätzlich werden Testseiten betrieben (z.B. für Software-Entwickler), die Auskunft über den Status (gültig, gesperrt und abgelaufen) eines Webserver-Zertifikats in Abhängigkeit von der Stamm-Zertifizierungsstelle (Root-CA) anzeigt.

Server-Zertifikate

https://active.tbca1.test.telesec.de

https://revoked.tbca1.test.telesec.de

https://expired.tbca1.test.telesec.de

Benutzer und Mail-Gateway-Zertifikate

https://www.telesec.de/de/service/downloads/produkte-und-loesungen

Änderungen der Informationssicherheitspolitik der TeleSec Shared-Business-CA werden den Bewertungsstellen/Auditoren (Kapitel 8 ff) und der Aufsichtsbehörde (Weiterleitung von Konzernlagezentrum der Deutschen Telekom AG an BSI, BNetzA) mitgeteilt.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Das vorliegende CPS wird, unabhängig von weiteren Änderungen, einer jährlichen Überprüfung (Review) unterzogen [CAB-BR]. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden.

Aktualisierungen des CPS werden wie in Kapitel 9.12 ff beschrieben veröffentlicht und in der Änderungshistorie vermerkt.

Aktuelle Entwicklungen, Änderungen und geänderte Anforderungen (zum Beispiel durch CABF-BR) werden verfolgt und in der Releaseplanung berücksichtigt.

Verantwortlich für die Durchführung bzw. die Koordination des Reviews ist die in Kapitel 1.5.1 benannte Stelle.

Zertifikate werden zum Zeitpunkt der Erzeugung veröffentlicht, sofern der Mandant nicht explizit einen Zugriffsschutz auf den Teilbaum (Ebene Master-Domäne) des Verzeichnisdienstes wünscht. Der Kunde teilt Telekom Security schriftlich mit, ob eine Veröffentlichung der Zertifikate auf Ebene der Master-Domäne gewünscht ist. Dem Kunden steht es frei, eine Zertifikatsveröffentlichung einzelner Sub-Domäne (Zuständigkeitsbereich) einzurichten.

Die Sperrlisten als auch OCSP-Antworten werden wie in Kapitel 4.9.7 beschrieben veröffentlicht.

2.4 Zugang zu den Ablagen und Verzeichnisdiensten

Der Abruf der Sperrlisten (CRL, CARL) und die Nutzung des OCSP-Dienstes für die Endteilnehmer (Kapitel 1.3.3), Vertrauende Dritte (Kapitel 1.3.4) oder Registrierungsstellen (Kapitel 1.3.2), unterliegen keiner Zugriffskontrolle.

Die Integrität und Authentizität der Sperrlisten und OCSP-Auskünfte wird durch die digitale Signatur mit vertrauenswürdigen Signern gewährleistet (Kapitel 4.10.1).

Das Suchen von Zertifikaten über den Verzeichnisdienst und Lesezugriff auf diese Informationen unterliegt grundsätzlich keiner Zugriffskontrolle. Der Mandant bestimmt jedoch, ob eine Zertifikatsveröffentlichung stattfinden soll oder nicht. Die Anzahl der Suchergebnisse wird jedoch beschränkt.

Das Suchen von Zertifikaten über die rollenspezifischen Webseiten ist erst nach erfolgreicher Authentifizierung mittels Zertifikat oder Benutzername/Passwort möglich. Das Suchergebnis ist jedoch abhängig von der vom Mandanten gewünschten Zertifikatsveröffentlichung.

Der lesende Zugriff durch Zertifikatsnehmer und -nutzer auf Informationen der Stamm- und Zwischenzertifizierungsstellen-Zertifikaten (Root- und Intermediate-CA) und der veröffentlichten CPS (siehe Kapitel 2.1 und 2.2) über einschlägige Webseiten unterliegt ebenfalls keiner Zugriffskontrolle.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

Ein Distinguished Name (DN) ist ein globaler, eindeutiger Name für Verzeichnisobjekte nach dem X.500-Standard. Mit dem Distinguished Name ist eine weltweite eindeutige Unterscheidbarkeit von Personen und Systemen gegeben. Der DN soll sicherstellen, dass kein digitales Zertifikat für verschiedene Personen mit dem gleichen Namen ausgestellt wird.

Innerhalb eines Zertifikates ist zu unterscheiden nach

- IssuerDistinguishedName (Issuer DN)
- SubjectDistinguishedName (Subject-DN)

Der Issuer DN repräsentiert den eindeutigen Namen der ausstellenden Zertifizierungsstelle (CA) und ist in den Kapiteln 1.3.1 ff beschrieben. Es gelten aber die Namensformen analog zum Subject-DN.

3.1.1 Namensformen

Für alle Zertifikatsanträge wird die Identität des Zertifikatnehmers geprüft. Abhängig vom Zertifikatstyp (Kapitel 1.3.3 und 7.1) werden die entsprechenden Informationen in unterschiedliche Pflichtfelder (mandatory fields) oder optionale Felder aufgenommen, die gemäß X.509v3-Standard vorgesehen sind.

Für alle Zertifikatstypen müssen zumindest die folgenden Felder ausgefüllt sein:

- Country Name (C)
- Organization Name (O)

Für Server-Zertifikate müssen zusätzlich die folgenden Felder ausgefüllt sein:

- Locality Name (L), oder
- State or Province Name (ST)

In optionalen Feldern (z.B. OU3, FQDN), die keine Informationen beinhalten (leere Felder) oder nicht relevant sind, ist die Verwendung von Füllzeichen (Metazeichen), wie beispielsweise "-", ".", „*“, " " (Zwischenraum, Space) oder „n/a“ verboten.

3.1.1.1 Konventionen für die Bestandteile des „Subject-DN“

In diesem Abschnitt werden Konventionen für Subject-DN (Antragsteller) festgelegt, die für alle Endteilnehmer-Zertifikate gelten. Im Folgenden werden die englischen Begriffe verwendet, die heute in diesem Umfeld gebräuchlich sind.

Innerhalb des Subject-DN sind folgende Zeichen erlaubt:

A – Z, a – z, ä, ö, ü 0 – 9, ( ) + - . / : = ? @ und Leerzeichen (Space, Blank)

Auf Grund der unterschiedlichen Kodierungsregeln der jeweiligen Zertifikatsfelder dürfen nicht alle o.g. Zeichen auch in diesen Eingabefeldern verwendbar werden (z.B. keine Umlaute (ä, ö, ü) in E-Mail-Adresse (Kapitel 3.1.1.1.8, 3.1.1.2.1) oder FQDN im Common Name (Kapitel 3.1.1.1.7) bzw. SubjectAlternativeName (Kapitel 3.1.1.2.3) eines Server-Zertifikats).

Es ist jedoch zu beachten, das, abhängig vom Zertifikatstyp (z.B. Benutzer, Server, Mail-Gateway), nicht alle Felder des Subject-DN (siehe Kapitel 3.1.1.1.1 bis 3.1.1.1.14) Verwendung finden und das die Feldlängen begrenzt sind.

3.1.1.1.1 Country Name (C)

Dieses Pflichtfeld enthält die weltweite Landeskennung. Festgelegt ist ein aus zwei Buchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist. Dieses Feld spezifiziert das Land, in welchem der Zertifikatsinhaber niedergelassen ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer gleichwertiger Verzeichnisse oder Dokumente verifiziert.

Beispiele: C = „DE“ für Deutschland. C = „US“ für Vereinigte Staaten von Amerika.

Weitere Details finden Sie hier:

http://www.unece.org/cefact/locode/subdivisions.html

http://www.nationsonline.org/oneworld/country_code_list.htm

Im Rahmen der Prüfung zur „Einrichtung einer Master-Domäne (Mandant)“ oder „erlaubten Internet-Domänen“ (Kapitel 3.2.2) werden die Attribute Country Name (C), Organization Name (O) (Kapitel 3.1.1.1.2), Locality Name (L) (Kapitel 3.1.1.1.9) und State or Province Name (ST) (Kapitel 3.1.1.1.10) als festes Wertepaar (Tupel) in die Konfiguration des Mandanten aufgenommen.

3.1.1.1.2 Organization Name (O)

Dieses Pflichtfeld enthält den Organisationsnamen (z.B. Firma, Institution, Behörde) des Zertifikatsinhabers. Der Organisationsname im Zertifikat soll die offizielle Schreibweise der Organisation aufweisen, also identisch mit dem jeweiligen Registereintrag (Handelsregister o.ä.) sein. Es darf auch die offizielle Abkürzung verwendet werden. Zudem darf von der offiziellen Schreibweise der Rechtsform abgewichen werden, sofern eine gebräuchliche Abkürzung verwendet wird. Die Rechtsform ist nicht verpflichtend anzugeben.

Bei Überschreitung der maximalen Feldlänge (64 Zeichen) behält sich die Zertifizierungsstelle eine sinnvolle Abkürzung vor.

Beispiel: O=Musterfirma Gesellschaft mit beschränkter Haftung, O=Musterfirma GmbH oder O=Musterfirma

Telekom Security prüft diese Angabe im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Leichte Abweichungen der Schreibweise des Organisationsnamens können akzeptiert werden, solange der Organisationsname weiterhin eindeutig ist (z.B. O=Alpha-Firma AG <-> O=Alpha Firma AG) und zusätzlich die Postleitzahl die Eindeutigkeit sicherstellt.

Telekom Security wird den Antragsteller über die Korrektur informieren und die akzeptierte Abweichung vom offiziellen Firmennamen dokumentieren.

Im Rahmen der Prüfung zur „Einrichtung einer Master-Domäne (Mandant)“ oder „erlaubten Internet-Domänen“ (Kapitel 3.2.2)) werden die Felder Organization Name (O), Country Name (C) (Kapitel 3.1.1.1.1), Locality Name (L) (Kapitel 3.1.1.1.9) und State or Province Name (ST) (Kapitel 3.1.1.1.10) als festes Wertepaar (Tupel) in die Konfiguration des Mandanten aufgenommen.

3.1.1.1.3 Organizational Unit Name 1 (OU1)

Dieses Pflichtfeld enthält den DNS-Bezeichner der Internet-Domäne des Mandanten, um eine globale Eindeutigkeit zu erreichen, oder einen anderen aussagekräftigen Namen. Der Organizational Unit Name 1 wird vor der Generierung des ersten Master-RA-Zertifikats für eine Master-Domäne festgelegt und kann danach nicht mehr geändert werden (siehe auch Kapitel 1.3.2.1 und 3.2.2 ff). Der Organizational Unit Name 1 ist im Zertifikats- und Konfigurationsdatenblatt aufgeführt.

Beispiele: OU1 = musterfirma.de, OU1 = t-systems.com

3.1.1.1.4 Organizational Unit Name 2 (OU2)

Dieses Pflichtfeld enthält bei Endanwender-, Gruppen-, Funktions-, Rollen- und Sub-RA-Zertifikate den Bezeichner eines Zuständigkeitsbereichs (Sub-Domäne). Ein Zuständigkeitsbereich muss eindeutig einer Master-Domäne zugeordnet sein.

Beispiele: OU2 = niederlassung-muenchen, OU2 = headquarter oder OU2 = ssl-vpn.

Hinweis: Der Zuständigkeitsbereich wird durch den Master-Registrator beantragt und steht erst nach Genehmigung durch Telekom Security zur Nutzung zur Verfügung.

3.1.1.1.5 Organizational Unit Name 3 (OU3)

Bei Endanwender- und Gruppen, Funktions-, Rollenzertifikaten kann mit diesem optionalen Feld (per Mandantenkonfiguration aktivierbar/deaktivierbar) eine weitere Zuordnung des Zertifikatsinhabers zu einer Organisationseinheit erfolgen.

Beispiele: OU3 = Vertrieb, OU3 = Niederlassung Duesseldorf, OU3 = <Vorname Nachname> (wenn CN (Kapitel 3.1.1.1.7) einer nicht aussagekräftigen Ziffern- bzw. Buchstabenkombination (z.B. Personalnummer) entspricht).

Folgende Einträge im OU3-Feld sind verboten:

- Einträge/Daten, die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt. Weiterhin sind Parolen oder Namen verboten, die auf rassistische, diskriminierende oder sexistische/pornografische Hintergründe verweisen oder Namen, die den Verdacht erzeugen, Identitäten von Organisationen zu täuschen oder zu verschleiern.
- Einträge/Daten, die keine Informationen beinhalten (leere Felder) oder die Verwendung von Füllzeichen (Metazeichen), wie beispielsweise "-", ".", „*“, " " (Zwischenraum, Space) oder „n/a“.
- Einträge, die üblicherweise in das O-Feld (Organization Name (O)) eingetragen werden (Kapitel 3.1.1.1.2) oder andere Organisationsdaten.
- Einträge/Daten, die Namenswahl von Warenzeichen, Markenname, Markenrechte darstellen.

Hinweis: Im Falle der Aktivierung des OU3-Feldes wird bei der Zertifikatsbeantragung der Inhalt per Positivliste (White List) geprüft. Im Falle fehlender Übereinstimmung wird die Antragsstellung unterbunden.

3.1.1.1.6 Vor- und Nachname

Abhängig vom Zertifikatstyp enthält das Pflichtfeld „Vorname“ und „Nachname“ den Namen einer natürlichen Person. Der Vor- und Nachname wird als eigene Subject-Inhalte auch für den Common Name (CN) (Kapitel 3.1.1.1.7) benötigt. Beide Namensteile sind mit einem Leerzeichen (Blank) getrennt.

Vorname und Nachname dürfen alle Zeichen der Zeichentabellen UTF-8 enthalten. Die folgenden Sonderzeichen sind jedoch verboten:

@ / \ [ ] | < > ? % $? ! ^ # ~ * ´ ` { } , ;

Griechisch oder kyrillische Zeichen in UTF-8-Kodierung werden derzeit nicht unterstützt.

Namensteile dürfen nicht mit Leer- oder Sonderzeichen beginnen und/oder enden. Die Länge des Common Name (gebildet aus Vornamen und Nachname) darf inkl. Leerzeichen maximal 64 Zeichen betragen (Leerzeichen zählt zu den 64 Zeichen und wird nachträglich eingefügt), max. 63 Zeichen).

3.1.1.1.7 Common Name (CN)

Abhängig vom Zertifikatstyp enthält das Pflichtfeld „Common Name“ den Namen des Endteilnehmers (siehe Kapitel 1.3.3). Dies sind für

- Benutzer-Zertifikate der Vor- und Nachname,
- Server-Zertifikate der Server-Name (FQDN),
- Router-Zertifikate die IP-Adresse,
- Mail-Gateway-Zertifikate das Präfix und der Server-Name (FQDN) und
- Domain-Controller-Zertifikate der Server-Name (FQDN).

Beispiele: CN = Peter Schmidt, CN = web1.musterfirma.de, CN = <IP-Adresse>

Für Benutzer-Zertifikate gilt: Zur Kennzeichnung von Zertifikaten für Gruppen-, Funktions-, Rollenzertifikate bzw. Verwendung von Pseudonymen sind dem Common Name folgende Kennungen voranzustellen (siehe auch Kapitel 3.1.3).

- Präfix „GRP:“ kennzeichnet Gruppen-, Funktions-, Rollenzertifikate
- Präfix „PN:“ kennzeichnet das Pseudonym-Zertifikat
- Präfix „SYS:“ kennzeichnet ein System oder Geräte-Zertifikat

Beispiele: CN = GRP: Funktionspostfach technischer Support, CN = PN: Max Mustermann (siehe auch Kapitel 3.1.3)

Bei Server-, Router-, Mail-Gateway und Domain-Controller-Zertifikaten wird der Common Name nach Zertifikatserzeugung in die Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name, Kapitel 3.1.1.2 ff) aufgenommen.

Für Server-Zertifikate gilt: Für alle Servernamen (DNS-Name, FQDN) steht ein eingeschränkter Zeichensatz zur Verfügung. Erlaubte Zeichen sind:

A – Z, a – z, 0 – 9, . (Punkt), - (Bindestrich), * (Sternchen), Umlaute (ä, ö, ü)

Für Server-Zertifikate gilt: Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur ganz links im FQDN akzeptiert. Wildcard-Zeichen in Verbindung mit Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

Für Server- und Router-Zertifikate gilt: Umlaute (ä, ö, ü) im FQDN müssen als IDN-Form in einen ACE-String konvertiert werden.

Beispiel:

IDN-Form: überall-ist.de
ACE-String: xn–berall-ist-8db.de

Einschränkungen: Zertifikate, die eine reservierte oder private IP-Adresse oder ein oder mehrere nicht öffentliche bzw. nicht auflösbaren DNS-Namen (insbesondere interne DNS-Namen) im Common Name –dies gilt insbesondere für die Zertifikatstypen Server, Router, Mail-Gateway und Domain-Controller- enthalten, dürfen nicht von einer öffentlichen Zwischenzertifizierungsstelle (siehe Kapitel 1.3.1.2.1) ausgestellt werden.

Alternativ können diese Zertifikatstypen von einer internen Zwischenzertifizierungsstelle ausgestellt werden (siehe Kapitel 1.3.1.2.2).

3.1.1.1.8 E-Mail-Address (E)

Das Pflichtfeld „E-Mail-Adresse“ (E) enthält bei

- Benutzer-Zertifikaten die E-Mail-Adresse des Zertifikatsinhabers (S/MIME) oder E-Mail-Adresse der Personenvereinigungen, Gruppen, Funktionen und Rollen, usw.,
- Geräte (Server, Router/Gateway, Mail-Gateway, Domain-Controller) die E-Mail-Adresse eines Administrators oder eines Funktionspostfachs,
- Master-Registrator-Zertifikaten die E-Mail-Adresse des Master-Registrators oder eines Funktionspostfachs,
- Sub-Registrator-Zertifikaten die E-Mail-Adresse des Sub-Registrators oder eines Funktionspostfachs.

Die Mail-Adresse wird zusätzlich benötigt für die Zustellung von Benachrichtigungsmails (z.B. Ausstellung, Sperrung und Erneuerung von Zertifikaten) und zur Zertifikatsbeantragung und -zustellung über die Mail-Schnittstelle.

Die E-Mail-Adresse (E) besteht aus einem Lokalteil (local part) und einem Domänenteil (domain part). Als Lokalteil wird der Teil einer E-Mail-Adresse bezeichnet, der sich vor dem @-Zeichen befindet und die Adresse innerhalb der Domain des E-Mail-Providers eindeutig bezeichnet. Der Domänenteil befindet sich nach dem @-Zeichen und es gelten die Syntaxregeln des DNS.

Beispiele: E = max.mustermann@musterfirma.de, E = pki-registrator@example.com

3.1.1.1.9 Locality Name (L)

Dieses Pflichtfeld enthält den Namen der Stadt, in dem die Organisation (z.B. Firma, Institution, Behörde) niedergelassen oder gemeldet ist, Zweigniederlassungen unterhält bzw. das Gerät (z.B. Server) betrieben wird. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer vergleichbarer Verzeichnisse oder Dokumente verifiziert.

Beispiele: locality = Berlin, locality = München, locality =Frankfurt/Main

Im Rahmen der Prüfung zur „Einrichtung einer Master-Domäne (Mandant)“ oder „erlaubten Internet-Domänen“ (Kapitel 3.2.2 ff) werden die Attribute Locality Name (L), Country Name (C) (Kapitel 3.1.1.1.1), Organization Name (O) (Kapitel 3.1.1.1.2) und State or Province Name (ST) (Kapitel 3.1.1.1.10) als festes Wertepaar (Tupel) in die Konfiguration des Mandanten aufgenommen.

3.1.1.1.10 State or Province Name (ST)

Dieses Pflichtfeld enthält den Namen des Gliedstaats oder die territoriale Verwaltungseinheit (z.B. Bundesland, Kanton, Departement), in dem die Organisation (z.B. Firma, Institution, Behörde) niedergelassen oder gemeldet ist, Zweigniederlassungen unterhält bzw. das Gerät (z.B. Server)

betrieben wird. Die Einträge und Schreibweisen sind spezifiziert nach ISO 3166-2 (International Organization for Standardization). Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer vergleichbarer Verzeichnisse oder Dokumente verifiziert.

Folgende Schreibweisen sind erlaubt:

- Vollschreibweise des „State or Province Name“ (Subdivision Name).
- Beispiele: state or province = “Berlin”, state or province = “Bayern”, state or province = “Hessen”
- Nach einer anerkannten Abkürzung des „State or Province Name“ (Subdivision Name).

Beispiele: state or province = “NW” für Nordrhein-Westfalen, state or province = “BRU“ für Région de Bruxelles-Capitale, state or province = “75“ für Paris

Offizielle englische Übersetzungen der jeweiligen landesspezifischen Schreibweise.

Weitere Details finden Sie hier:

http://www.unece.org/cefact/locode/subdivisions.html

Z.B.: https://www.iso.org/obp/ui/#iso:code:3166:DE (durch Änderung der Landeskennung gemäß ISO 3166-1 (im Beispiel „DE“) können andere länderspezifische „State or Province Name (Subdivision)“ selektiert werden).

Im Rahmen der Prüfung zur „Einrichtung einer Master-Domäne (Mandant)“ oder „erlaubten Internet-Domänen“ (Kapitel 3.2.2 ff) werden die Attribute State or Province Name (ST), Country Name (C) (Kapitel 3.1.1.1.1), Organization Name (O) (Kapitel 3.1.1.1.2) und Locality Name (L) (Kapitel 3.1.1.1.9) als festes Wertepaar (Tupel) n die Konfiguration des Mandanten aufgenommen.

3.1.1.1.11 Street Address

Dieses optionale Feld enthält den Straßennamen, an dem die Organisation (z.B. Firma, Institution, Behörde) gemeldet ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder vergleichbaren Verzeichnisses oder Dokumenten verifiziert.

Beispiele: street address = Musterstraße 17, street address = 5. Avenue

3.1.1.1.12 Postal Code

Dieses optionale Feld enthält die Postleitzahl der Stadt, in dem die Organisation (z.B. Firma, Institution, Behörde) gemeldet ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder vergleichbaren Verzeichnisses oder Dokumenten verifiziert.

Beispiele: postal code = 57250, postal code = AZ23G7

3.1.1.1.13 Subject-DN Serial Number (SN)

Innerhalb eines Zuständigkeitsbereiches (Sub-Domäne) kann es vorkommen, dass Zertifikate einen gleichlautenden Subject-DN aufweisen. Zur Unterscheidung wird dazu im Subject-DN eine numerische Seriennummer vergeben. Bei manueller Ausstellung von Benutzer-, Server- und Router/Gateway-Zertifikaten über die Sub-RA- und Benutzer-Webseiten wird dieses Attribut und dessen Wert automatisch vom CA-System (Zertifizierungsstelle) erzeugt und um den Wert eins (1) inkrementiert.

Dies gilt prinzipiell auch für Zertifikatsbeantragungen im Bulk-Prozess und via Mail-Schnittstelle. Optional kann der Sub-Registrator die Subject-DN-Seriennummer auch manuell vorgeben. Gleiche Regelung gilt auch für die Beantragung über die CMP-Schnittstelle.

Beispiele: SN = 1 für 1. Max Mustermann und SN = 2 für 2. Max Mustermann innerhalb des gleichen Zuständigkeitsbereichs.

Hinweis: Die Belegung der Subject-DN-Seriennummer mit einem alphanumerischen Wert, Namen, E-Mail-Adresse, FQDN, Organisationsname oder sonstigen Bezeichnung, ist verboten.

3.1.1.1.14 Unstructured Name

Weitere Informationen zum „unstructured name“ (Unstrukturierter Name) sind in Kapitel 3.1.1.2.3 dargestellt.

3.1.1.2 Konventionen für die Bestandteile „Subject Alternative Name“ (SAN)

Die Einträge im Feld „Alternativer Antragstellername“ (Subject Alternative Name (SAN)) sind abhängig von den jeweiligen Zertifikatstypen (Benutzer, Server, Router/Gateway, Domain-Controller und Mail-Gateway). Die Erweiterung „Subject Alternative Name“ muss mindestens einen Eintrag enthalten. Die Einträge im SAN stammen aus Pflichtfeldern wie

- Common Name (Kapitel 3.1.1.1.7)
- E-Mail-Adresse (Kapitel 3.1.1.1.8)
- User Principal Name (Kapitel 3.1.1.2.2)
- DNS-Name (Kapitel 3.1.1.2.3)
- IP-Adresse (Kapitel 3.1.1.2.4)

als auch optionalen Feldern wie

- E-Mail-Adresse (Kapitel 3.1.1.1.8), im Falle bei mehr als einer Adresse.
- DNS-Name (Kapitel 3.1.1.2.3)

Einschränkungen von Zertifikatsinhalten sind in Kapitel 3.1.1.1.7 beschrieben.

3.1.1.2.1 RFC822-Name

Der RFC822-Name entspricht der E-Mail-Adresse. Optional kann in einem Benutzer-Zertifikat bis zu drei (3) weiteren E-Mail-Adressen aufgenommen werden. Der bzw. die E-Mail-Adresse(n) werden automatisch in den Subject Alternative Name (SAN) übernommen.

3.1.1.2.2 User Principal Name (UPN)

Das Feld „User Principal Name“ (UPN) im Benutzer-Zertifikat ist optional, außer als Pflichteintrag im Smartcard-LogOn-Zertifikat (Triple-Key). Der „User Principal Name“ stellt einen benutzerfreundlichen (d.h. leicht zu merkenden) Name dar, der zur Windows-Anmeldung an der Domäne bzw. Active Directory dient. Dieser besteht aus einem Benutzerkontonamen (auch Anmeldenamen genannt) und der Domäne, in der das Benutzerkonto gespeichert ist („Benutzerkontonamen“@„Domänenname).

Der UPN kann, muss aber nicht der E-Mail-Adresse entsprechen.

Beispiele: UPN = max.mustermann@musterfirma.de, UPN = max.mustermann@local-server.com

Bei Benutzer-Zertifikaten wird der UPN in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name, Kapitel 7.1.2.3) als „Prinzipalname“ angezeigt.

3.1.1.2.3 DNS-Name

Der vollständige Name einer Domäne (auch absolute Adresse genannt) wird als Fully Qualified Domain Name (FQDN) bezeichnet und kennzeichnet eine exakte Position in der Baumstruktur der DNS-Hierarchie. Das Feld „FQDN“ besteht mindestens aus Top-Level und weiteren Sub-Domains.

Beispiele: FQDN = www.example.com, FQDN = s-server.pki.example.de

Bei Server-Zertifikaten wird der FQDN als Pflichtfeld im Subject-DN als „Common Name“ eingetragen und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „DNS-Name“ angezeigt.

Optional können in einem Server-Zertifikat bis zu vier (4) weiteren Server-Namen aufgenommen werden. Die Server-Namen werden automatisch als „DNS-Name“ in den Subject Alternative Name (SAN) übernommen.

Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur ganz links im FQDN akzeptiert. Wildcard-Zeichen in Verbindung mit Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

Bei Router-Zertifikaten wird das optionale Feld FQDN als „unstructured name“ im Subject-DN aufgenommen und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „DNS-Name“ angezeigt.

3.1.1.2.4 IP-Adresse

Bei Router-Zertifikaten wird die IP-Adresse als Bestandteil des „Common Name“ im Subject-DN und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „IP-Adresse“ angezeigt.

3.1.1.2.5 Anderer Name (Other Name)

Bei Domain-Controller-Zertifikaten wird das Pflichtfeldes „Microsoft-GUID“ (MSGuid) als Eintrag „DNS-Objekt-Guid“ unter „Other Name“ in die Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) angezeigt.

3.1.2 Aussagekraft von Namen

Der Name muss den Endteilnehmer bzw. Zertifikatsnehmer mit allgemein verständlicher Wortbedeutung enthalten, als auch eindeutig und nachprüfbar sein.

Im Falle von Zertifikaten für Personen- und Funktionsgruppen- und Pseudonymen kann Telekom Security vom Mandanten verlangen, die wahre Identität des Zertifikatsinhabers berechtigten Dritten offenzulegen.

3.1.3 Pseudonymität bzw. Anonymität der Zertifikatsinhaber

Benutzer-Zertifikate, die ein Pseudonym enthalten, werden mit dem Präfix „PN:“ im Common Name (CN) kenntlich gemacht (siehe auch Kapitel 3.1.1.1.7).

Benutzer-Zertifikate für Personen- und Funktionsgruppen Rolleninhaber, werden mit dem Präfix „GRP:“ im Common Name (CN) gekennzeichnet.

Beispiele: „PN: Novalis“ „PN: George Sand“, „GRP: Einkauf“, „GRP: Technischer Support“.

Die Nutzung von Gruppen- und Funktionszertifikaten oder Pseudonymen unterliegt verschiedenen Namenseinschränkungen. Ausgeschlossen werden Namen die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt, sowie politische Parolen, usw.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

Telekom Security stellt sicher, dass Benutzer-Zertifikate mit gleichem Subject-DN (siehe Kapitel 3.1.1.1 ff) nur einmal innerhalb des Zuständigkeitsbereiches (Sub-Domäne) vorkommen. Dies wird durch die Vergabe einer Seriennummer im Subject-DN (siehe Kapitel 3.1.1.1.13) gewährleistet.

Für Benutzer können ein, zwei oder drei Zertifikate mit demselben eindeutigen Subject-DN ausgestellt sein, die sich jedoch in der Schlüsselverwendung bzw. erweiterten Schlüsselverwendung (z.B. Signatur, Schlüsselverschlüsselung, Client-Authentifizierung, Smartcard-Anmeldung) und der Zertifikatsseriennummer unterscheiden. Durch die Erneuerungsfunktion können zeitlich begrenzt auch mehrere Zertifikate mit dem gleichen Subject-DN erstellt sein.

Zertifikate für Geräte mit gleichem Subject-DN (siehe Kapitel 3.1.1.1 ff) können mehrfach vorkommen.

3.1.6 Erkennung, Authentifizierung und Rolle von Warenzeichen

Für die Namenswahl von Warenzeichen, Markenname, Markenrechte usw. in Zertifikaten (z.B. Organization Name (O), Organizational Unit Name (OU)) gilt besondere Sorgfaltspflicht. Es liegt in der Verantwortung des Mandanten, dass die Namenswahl keine Warenzeichen, Markenrechte usw. oder die Rechte des geistigen Eigentums von Dritten verletzen. Die Zertifizierungsstelle SBCA als auch die interne Registrierungsstelle der Telekom Security ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Mandanten.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Methode zum Besitznachweis des privaten Schlüssels

Der Zertifikatsantragsteller muss bei einer Beantragung gegenüber der Zertifizierungsstelle in geeigneter Weise nachweisen, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist. Der Besitznachweis wird durch die Methode PKCS#10 erbracht.

Diese Anforderung gilt nicht, wenn die Schlüsselerzeugung in der Zertifizierungsstelle stattfindet (Bulk siehe Kapitel 3.2.3.4 und 3.2.3.5).

3.2.2 Authentifizierung der Organisations- und Domänenidentität

3.2.2.1 Einrichtung eines PKI-Mandanten

Grundvoraussetzung für die Nutzung der SBCA ist die Einrichtung eines PKI-Mandanten (auch Master-Domäne genannt) innerhalb des PKI-Dienstes TeleSec Shared-Business-CA. Die technische Einrichtung des PKI-Mandanten basiert auf dem ausgefüllten und unterzeichneten Formblatt „Auftrag zur Einrichtung einer Master-Domäne“. Zur ordentlichen Identifizierung und damit Nachweis der Organisation benötigt Telekom Security ein offizielles und aktuelles Dokument (z.B. beglaubigter Handelsregisterauszug oder vergleichbares Dokument), das nicht älter als 30 Kalendertage sein darf. Bei Behörden genügt das Dienstsiegel und die Unterschrift eines Bevollmächtigten der Behörde auf diesen Auftrag.

Während der Antragsprüfung zur Einrichtung der Master-Domäne wird die Identität des Auftraggebers (Mandant, beauftragte Drittpartei (Delegated Third Party)) überprüft.

Für die Überprüfung der Existenz oder der Adresse der Organisation können alternativ oder zusätzlich zum Handelsregister bzw. der vergleichbaren Verzeichnisse weitere Methoden herangezogen werden. Bei Bedarf kann ein Bisnode-Report (vormals Dun & Bradstreet) als vertrauenswürdige, verlässliche und unabhängige Datenquelle verwendet werden.

Als weitere Methode zur Überprüfung ist die Vorlage einer von einer entsprechend qualifizierten Person ausgestellten anwaltlichen Stellungnahmen zulässig. Ebenso kann ein Mitarbeiter der Zertifizierungsstelle oder ein von ihr beauftragten Drittpartei den angegebenen Standort persönlich aufsuchen und bestätigen.

Im Falle, dass ein Dritter im Namen des PKI-Mandanten (beauftragte Drittpartei (Delegated Third Party)) die Zertifikatsverwaltung (inkl. privaten Schlüssel) durchführen soll, bedarf es einer schriftlichen Vereinbarung zwischen diesen beiden Parteien hinsichtlich der Sorgfaltspflicht der übertragenen Arbeiten und zur Einhaltung der CPS der SBCA (Berechtigungsdokument „Übertragung von Rechte und Pflichten“).

T-System stellt bei der Authentifizierung sicher, dass keine Namen in den Feldern Organisation (O) und Organizational Unit Name (OU1 bis OU3) verwendet werden, die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt. Weiterhin sind Parolen oder Namen verboten, die auf rassistische, diskriminierende oder sexistische/pornografische Hintergründe verweisen oder Namen, die den Verdacht erzeugen, Identitäten von Organisationen zu täuschen oder zu verschleiern.

Telekom Security führt folgende Prüfungen durch:

- Feststellung der Existenz der Organisation durch einen Identitätsprüfungsservice oder Identitätsprüfungsdatenbank eines Dritten oder wahlweise durch entsprechende aktuelle Organisationsdokumente, die von einer zuständigen Stelle oder Behörde ausgestellt oder bei ihr eingereicht wurden, die die Existenz der Organisation bestätigen (z.B. Handelsregisterauszug oder vergleichbares Dokument, das nicht älter als 30 Tage sein darf, Dienstsiegel),
- Prüfung des/der Domänennamen gegen öffentlich zugängliche Datenbanken (z.B. WhoIs-Abfrage über Denic eG) oder einem Verfahren, wie unter Kapitel03.2.5.2 ff beschrieben,
- Feststellung der Existenz des im Dokument „Auftrag zur Einrichtung einer Master-Domäne“ angegebenen verantwortlichen Ansprechpartners, der als Master-Registrator bestimmt ist. Ferner ist zu prüfen, ob die genannte Person in der Organisation (Mandant) beschäftigt ist oder eine Vollmacht besitzt, im Namen der Organisation zu handeln,
- Zusätzliche Prüfungen nach Bedarf (z.B. zur Erfüllung der US-amerikanischen Exportbestimmungen und -lizenzen der Industrie- und Wissenschaftsbehörde (Bureau of Industry and Science, BIS) des amerikanischen Handelsministeriums).

Telekom Security stellt sicher, dass der Name der Master-Domäne nur einmal innerhalb der TeleSec Shared-Business-CA vorkommt. Die Master-Domäne wird in der Regel nach dem Domänennamen

(Top-Level-Domain und Second-Level-Domain, optional zusätzliche Sub-Level-Domains erlaubt) des PKI-Mandanten benannt. Die Domainprüfung ist in Kapitel 3.2.5.2 beschrieben. Der Name des PKI-Mandanten ist Attribut „Organizational Unit Name 1“ (OU1) (siehe Kapitel 3.1.1.1.3) im Subject-DN des Zertifikats fest eingetragen.

Sofern der Domänennamen nicht zur Namensbildung herangezogen werden kann, darf auch eine andere Namengebung erfolgen. Der Name muss eindeutig Rückschlüsse auf den Mandanten zulassen.

Bei der Einrichtung der Master-Domäne werden für alle angebotenen Zertifikatstypen (Benutzer, Server-, Mail-Gateway, Router/Gateway- und Domain-Controller) nur die Domänen eingerichtet, für die der Mandant einen entsprechenden Besitznachweis erbringen kann. Die Domänennamen gelten für die gesamte Master-Domäne und vererben sich auch auf Zuständigkeitsbereiche (Sub-Domänen).

Der Name der Master-Domäne(n) wird, sofern es sich um einen DNS-Namen handelt, auch in der Konfiguration der Master-Domäne (PKI-Mandant, externe Registrierungsstelle) als „erlaubte Internet-Domäne“ für den jeweiligen Zertifikatstyp (z.B. Benutzer, Server) aufgenommen.

Der Master-Registrator tritt als Verwalter des PKI-Mandanten (Master Domäne) auf und stellt innerhalb des Mandanten die oberste Registrierungsstelle (Kapitel 1.3.2.2.1) dar. Der Registrierungsprozess des Master-Registrators ist in Kapitel 3.2.3.2 beschrieben.

Organisationsänderungen (z.B. Umfirmierung) oder Personenänderung des Master-Registrators ist dem Herausgeber (siehe Kapitel 4.9.1.1) dieser CPS unverzüglich schriftlich anzuzeigen. Die Prüfung einer Organisationsänderung erfolgt nach gleichem Procedere wie oben beschrieben.

Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

Zur Erfüllung und Einhaltung der [CAB-BR] als auch diverser Root-Programme wird Telekom Security die Verwendungsrechte der Domäne(n) als auch Organisationen überprüfen.

Die „erlaubten Internet-Domänen“ als auch Organisationen werden, abhängig vom konfigurierten Zertifikatstyp, nach folgenden Zeiträumen geprüft:

- Öffentliche Server-Zertifikate
  - spätestens nach 13 Monaten bzw. 398 Tagen
- Alle anderen öffentlichen oder internen Zertifikate
  - spätestens nach 39 Monaten

Telekom Security behält sich vor, aktuelle Identifikationsdokumente des Inhabers der Master-Domäne und/oder Dritten zu dessen Lasten anzufordern.

Bei der Registrierung werden die folgenden Sachverhalte ausdrücklich nicht geprüft:

- Dass der im Zertifikat genannte Organisation einer aktiven Geschäftstätigkeit nachgeht.
- Dass der im Zertifikat genannte Organisation in ihrer Geschäftstätigkeit gesetzeskonform handelt.
- Dass der im Zertifikat genannte Organisation in ihrer Geschäftstätigkeit vertrauenswürdig, ehrlich oder seriös handelt.
- Dass es ungefährlich bzw. sicher ist, mit dem im Zertifikat genannten Organisation Geschäfte zu tätigen.

3.2.2.2 Zusätzliche Identitätsprüfungen

Die in den folgenden Kapiteln beschriebenen Identitätsprüfungen beziehen sich auf alle Zertifikatstypen (Kapitel 1.3.3) die unter einer öffentlichen Zertifizierungsstelle (Kapitel 1.3.1.2.1) ausgestellt werden.

Zertifikate, die einer dieser Identitätsprüfungen nicht entsprechen, dürfen nur von einer internen Zertifizierungsstelle (Kapitel 1.3.1.2.2) ausgestellt werden.

3.2.2.2.1 Identität

Die Informationen zur Subjektidentität werden durch mindestens eine der folgenden Methoden verifiziert:

1. eine staatliche Stelle in dem Hoheitsgebiet der rechtmäßigen Gründung, Existenz oder Anerkennung des Auftraggebers,
2. eine Drittdatenbank, die regelmäßig aktualisiert und als zuverlässige Datenquelle betrachtet wird,
3. einen Standortbesuch durch die CA oder eine Drittpartei, die als Agent für die CA tätig wird, oder
4. ein Bestätigungsschreiben.

3.2.2.2.2 Firmierung/Handelsname

Wenn die Informationen zur Subjektidentität eine Firmierung oder einen Handelsnamen enthalten, MUSS die CA das Recht des Auftraggebers zur Nutzung der Firmierung/des Handelsnamens durch mindestens eine der folgenden Methoden verifizieren:

1. Dokumentation, die durch eine staatliche Stelle in dem Hoheitsgebiet der rechtmäßigen Gründung, Existenz oder Anerkennung des Auftraggebers vorgelegt oder durch die Kommunikation mit einer solchen Stelle belegt wird,
2. eine zuverlässige Datenquelle,
3. Kommunikation mit einer staatlichen Stelle, die für die Verwaltung solcher Firmierungen oder Handelsnamen zuständig ist,
4. ein Bestätigungsschreiben, dem Nachweisdokumente beigefügt sind, oder
5. eine Rechnung eines Versorgungsunternehmens, eine Bankabrechnung, eine Kreditkartenabrechnung, ein vom Staat ausgegebenes Steuerdokument oder eine andere Form der Identifizierung, deren Zuverlässigkeit die CA feststellt.

3.2.2.2.3 Überprüfung der Länderkennung

Das zum Subjekt gehörende Land im Feld subject:countryName MUSS von der CA mithilfe einer der folgenden Methoden verifiziert werden:

1. die Zuweisung des IP-Adressenbereichs durch das Land für (i) die IP-Adresse der Webseite, wie durch den DNS-Eintrag für die Webseite angegeben, oder (ii) die IP-Adresse des Auftraggebers,
2. die ccTLD des beantragten Domain-Namens, oder
3. Informationen, die vom Domain-Name-Registrar vorgelegt werden.

3.2.2.2.4 Validierung der Berechtigung oder der Kontrolle der Domain

Für jeden vollqualifizierten Domain-Namen (FQDN), MUSS die CA bestätigen, dass der Auftraggeber (oder die Muttergesellschaft, die Tochtergesellschaft oder das verbundene Unternehmen des Auftraggebers, zum Zwecke dieses Abschnitts zusammen als „Auftraggeber“ bezeichnet) am Datum

der Zertifikatsausstellung entweder der Domain-Name-Registrant ist oder die Kontrolle über den FQDN besitzt.

Für die Prüfung der Domainkontrolle aller im Zertifikatsrequest enthaltenen Domain-Namen wird mindestens eine der folgenden Methoden eingesetzt.

3.2.2.2.4.1 Überprüfung des Antragstellers per Domain-Kontakt

Nicht anwendbar.

3.2.2.2.4.2 Überprüfung des Auftraggebers per Kontakt via E-Mail, Fax, SMS, oder Briefpost

Nicht anwendbar.

3.2.2.2.4.3 Überprüfung des Auftraggebers per Telefon

Nicht anwendbar.

3.2.2.2.4.4 Überprüfung des Auftraggebers per konstruierter E-Mail

Es wird bestätigt, dass der Auftraggeber die Kontrolle über die Domain hat, indem eine E-Mail an eine oder mehrere Adressen gesendet wird, die unter Verwendung von vorangestellten ‚admin', ‚administrator', ‚webmaster', ‚hostmaster' oder ‚postmaster', gefolgt von dem at-Zeichen („@"), gefolgt vom Domain-Namen des zu prüfenden FQDN. Die E-Mail-Nachricht MUSS einen Zufallswert enthalten, der in der Antwortmail enthalten sein MUSS. (Verfahren nach Kapitel 3.2.2.4.4 der [CAB-BR]). Es gilt:

- Jede E-Mail kann die Berechtigung für mehrere FQDN bestätigen, vorausgesetzt, dass der in der E-Mail verwendete Autorisierungs-Domain-Name ein Autorisierungs-Domain-Name für jeden FQDN ist, der bestätigt wird.
- Der Zufallswert ist in jeder E-Mail einmalig.
- Die E-Mail darf in ihrer Gesamtheit, einschließlich der Wiederverwendung des Zufallswertes, erneut versendet werden, vorausgesetzt, dass ihr gesamter Inhalt und Empfänger unverändert bleiben.
- Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.
- Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDNs ausgestellt werden, die mit allen Labels des validierten FQDN enden.
- Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

3.2.2.2.4.5 Domainvollmacht

Alternativ wird ein Domain-Autorisierungsschreiben für die Organisation angefordert, das vom Domäneninhaber (Domainholder), Registrant oder Admin-C ausgestellt worden ist.

Es wird geprüft, ob das Domain-Autorisierungsschreiben am oder nach dem Datum des Zertifizierungsauftrags ausgestellt wurde und dass der WHOIS-Eintrag seit der Ausstellung der Vollmacht nicht verändert wurde.

Diese Methode ist für Server-Zertifikate, die unter einer öffentlichen Zertifizierungsstelle ausgestellt werden sollen, zum 01.08.2018 entfallen.

3.2.2.2.4.6 Vereinbarte Änderung auf der Webseite

Es wird geprüft, dass der Auftraggeber für jeden im Zertifikat aufgelisteten FQDN die praktische Kontrolle nachzuweisen kann, indem er eine vereinbarte Änderung auf einer Webseite vornimmt.

Für den Nachweis ist eine bestimmte einmalige Textdatei unter einem vorgegebenen Pfad auf dem Server abzulegen (/.well-known/pki-validation/sbcadv.txt).

- Die Zertifizierungsstelle muss per HTTP/HTTPS darauf zugreifen können.
- Es wird ein einmaliger, konstruierter Zufallswert verwendet.
- Der Zufallswert ist maximal 30 Tage nach seiner Erstellung gültig.
- Der Empfänger fügt den Zufallswert an der definierten Stelle ein.

Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDNs ausgestellt werden, die mit allen Labels des validierten FQDN enden.

Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

3.2.2.2.4.7 Änderung im DNS

Bei diesem Validierungsverfahren wird für jeden im Zertifikat aufgelisteten FQDN die Domainkontrolle durch das gezielte Einfügen von eindeutigen Informationen im DNS nachgewiesen.

- Es wird ein einmaliger, konstruierter Zufallswert verwendet.
- Der Zufallswert ist maximal 30 Tage nach seiner Erstellung gültig.
- Der Empfänger fügt den Zufallswert im DNS des zu prüfenden FQDN ein.

Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDNs ausgestellt werden, die mit allen Labels des validierten FQDN enden.

Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

3.2.2.2.4.8 IP Adresse

Nicht anwendbar.

3.2.2.2.4.9 Testzertifikat

Nicht anwendbar.

3.2.2.2.4.10 TLS unter Verwendung einer Zufallszahl

Nicht anwendbar.

3.2.2.2.4.11 Jede andere Methode

Nicht anwendbar.

3.2.2.2.4.12 Validierung des Antragstellers als Domain-Kontakt

Durch Validierung des Antragstellers wird überprüft, ob der Antragsteller der Domain-Kontakt des beauftragten vollqualifizierte Domänenname (FQDN) ist. Diese Methode kann nur verwendet werden, wenn die Zertifizierungsstelle auch der Domain Name Registrar oder ein verbundenes Unternehmen des Registrars des Haupt-Domainnamen ist.

Hinweis: Sobald der vollqualifizierte Domänenname (FQDN) mit dieser Methode validiert wurde, kann die Zertifizierungsstelle (CA) auch Zertifikate für andere FQDN ausstellen, die mit allen

Bezeichnungen des validierten FQDN enden. Diese Methode eignet sich zur Validierung von Wildcard-Domainnamen.

Ein Vertrag mit dem Domain-Management der Deutschen Telekom AG (Registrar) enthält eine Liste mit festgelegten Domains, die im Besitz des Telekom Konzerns sind und von definierten Konzerneinheiten verwendet werden dürfen. Der beauftragte FQDN eines internen Auftraggebers wird gegen diese Liste geprüft.

Bei internen Bestellungen von anderen Konzerneinheiten lässt der Registrierungsmitarbeiter den Antragsteller vom Domain-Management als autorisierten Domain-Kontakt bestätigen.

3.2.2.2.4.13 E-Mail an DNS-CAA-Kontakt

Nicht anwendbar.

3.2.2.2.4.14 E-Mail an DNS TXT-Kontakt

Nicht anwendbar.

3.2.2.2.4.15 Telefonkontakt mit Domänenkontakt

Nicht anwendbar.

3.2.2.2.4.16 Telefonkontakt mit DNS TXT Telefonkontakt aufzeichnen

Nicht anwendbar.

3.2.2.2.4.17 Telefonkontakt mit DNS CAA Telefonkontakt

Nicht anwendbar.

3.2.2.2.4.18 Vereinbarte Änderung auf der Webseite - Version 2

Nicht anwendbar.

3.2.2.2.4.19 Vereinbarte Änderung auf der Webseite - ACME

Nicht anwendbar.

3.2.2.2.5 Authentifizierung für eine IP-Adresse

Nicht anwendbar.

3.2.2.2.5.1 Vereinbarte Änderung der Website

Nicht anwendbar.

3.2.2.2.5.2 E-Mail, Fax, SMS oder Post an IP-Kontakt senden

Nicht anwendbar.

3.2.2.2.5.3 Reverse Address Lookup

Nicht anwendbar.

3.2.2.2.5.4 Jede andere Methode

Nicht anwendbar.

3.2.2.2.5.5 Telefonkontakt an IP-Adresskontakt

Nicht anwendbar.

3.2.2.2.5.6 ACME-Methode "http-01" für IP-Adressen

Nicht anwendbar.

3.2.2.2.5.7 ACME-Methode "tls-alpn-01" für IP-Adressen

Nicht anwendbar.

3.2.2.2.6 Überprüfen einer Wildcard-Domain

Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur ganz links im FQDN akzeptiert. Wildcard-Zeichen in Verbindung mit Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

Wenn ein Wildcard-Zeichen in einem Label unmittelbar links von einem „registry-controlled“ oder „public suffix“ erscheint, MUSS die Ausstellung abgelehnt werden (z.B. „*.co.uk“ oder „*.de“), es sei denn, der Auftraggeber weist seine rechtmäßige Kontrolle über den gesamten Domain-Namensraum nach.

3.2.2.2.7 Zuverlässigkeit der Datenquelle

Es werden ausschließlich vertrauenswürdige Datenquellen als zuverlässige Datenquellen aber keine selbstgepflegten oder von verbundenen Unternehmen geführte Datenquellen verwendet.

3.2.2.2.8 CAA-Records

Siehe Kapitel 3.2.5.3 und 4.2.2 ff.

3.2.3 Authentifizierung der Endteilnehmer-Identität

3.2.3.1 Allgemeines

Die Authentifizierung der Identität bzw. Identifikation von Endteilnehmern (siehe Kapitel 1.3.3) wird von der beim Mandanten etablierten Registrierungsstelle (siehe Kapitel 1.3.2 ff) durchgeführt.

Standardmäßig stehen bei SBCA folgende Registrierungsmodelle zur Verfügung:

- zentrale Registrierung (zentrales Registrierungsmodell), d.h. nach erfolgreicher Registrierung des Endteilnehmers beantragt der Sub-Registrator über die Sub-RA-Webseite das Zertifikat (per Webformular oder Bulk) und erhält dieses bzw. das Schlüsselmaterial für den Endteilnehmer (außer Registrator-Zertifikat) direkt ausgestellt.
- dezentrale Registrierung (zentrales Registrierungsmodell), d.h. der Benutzer stellt den Zertifikatsantrag über die Benutzer-Webseite oder per Mail-Request, oder das Gerät stellt den Zertifikatsantrag über seine SCEP-Schnittstelle, den der Sub-Registrator bearbeitet (Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage)).

Auf eine detailliertere Beschreibung der beiden Registrierungsmodelle wird an dieser Stelle auf das Dokument „Leistungsbeschreibung TeleSec Shared-Business-CA“ verwiesen.

Daraus gelten folgende Regelungen:

- Grundsätzlich erfolgt die Registrierung eines Endteilnehmers über den zuständigen Sub-Registrator. Eine Ausnahme bildet die automatisierte Massengenerierung von Schlüsselmaterial (Bulk).
- Der Sub-Registrator entscheidet über Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage) des Zertifikatsantrags.
- Für Benutzer-Zertifikate steht eine Erneuerungsfunktion zur Verfügung, die beliebig häufig genutzt werden kann, sofern sich nicht die Zertifikatsdaten (z.B. Organisation) ändern. Die grundsätzliche Nutzung der Erneuerungsfunktion liegt im Ermessen des Mandanten. Für Geräte-Zertifikate steht keine Erneuerungsfunktion zur Verfügung.

Mit der initialen Einrichtung eines PKI-Mandanten wird die Kunden-Domain, wie unter Kapitel 3.2.2.1 ff beschrieben, als erlaubte Internet-Domain in die PKI-Konfiguration aufgenommen. Für die Ausstellung von Zertifikaten von einer öffentlichen Zertifizierungsstelle (siehe Kapitel 1.3.1.2.1) werden die geprüften Organisationsdaten (siehe 3.1.1.1.1, 3.1.1.1.2, 3.1.1.1.9 und 3.1.1.1.10) im PKI-Mandanten für eine definierte Zeit vorbelegt und der Kunden-Domain verknüpft.

Nach Bedarf können zusätzliche Domains als „erlaubte Internet-Domänen“ hinzugefügt und mit den jeweiligen Organisationsdaten verknüpft, in die PKI-Konfig aufgenommen werden. Basis bildet eins der in Kapitel 3.2.2.2.4 aufgeführten Prüfungsverfahren.

Bei der Registrierung werden die folgenden Sachverhalte ausdrücklich nicht geprüft:

- Dass die im Zertifikat genannte Endteilnehmer einer aktiven Geschäftstätigkeit nachgeht.
- Dass die im Zertifikat genannte Endteilnehmer in ihrer Geschäftstätigkeit gesetzeskonform handelt.
- Dass die im Zertifikat genannte Endteilnehmer in ihrer Geschäftstätigkeit vertrauenswürdig, ehrlich oder seriös handelt.
- Dass es ungefährlich bzw. sicher ist, mit der im Zertifikat genannten Endteilnehmer Geschäfte zu tätigen.

3.2.3.2 Registrierung eines Master-Registrators

Die Registrierung des Master-Registrators erfolgt durch Telekom Security im Rahmen der Identitätsprüfung einer Organisation (siehe Kapitel 3.2.2 ff).

Das zur Verwaltung der Master-Domäne (PKI-Mandant) erforderliche Master-Registrator-Zertifikat wird auf eine natürliche Person ausgestellt und enthält einen für das PKI-System eindeutigen Namen (Common Name). Die natürliche Person ist ein(e) Mitarbeiter(in) der Organisation (PKI-Mandant) oder einer beauftragten Drittpartei (Delegated Third Party). Als Identitätsnachweis wird eine Ausweiskopie (z.B. Personalausweis, Reisepass, Unternehmensausweis) und ein Kontrollanruf akzeptiert.

Für die Ausstellung zusätzlicher Master-Registrator-Zertifikate wird das oben genannte Verfahren durchgeführt.

Auf Grund dieser Berechtigungen werden Master-Registrator-Zertifikate grundsätzlich von Telekom Security auf Smartcard ausgestellt. Ungültige oder Master-Registrator-Zertifikate gesperrte können nicht mehr verwendet werden und bedürfen einer Neubeantragung mit entsprechender Identitätsprüfung.

3.2.3.3 Registrierung eines Sub-Registrators

Der Mandant kann ein oder mehrere Zuständigkeitsbereiche (Sub-Domänen) administrieren lassen, die durch Sub-Registratoren verwaltet werden. Dabei gelten folgende Regelungen:

Die Registrierung eines Sub-Registrators und die Ausstellung des Sub-Registrator-Zertifikats erfolgt durch einen Master-Registrator des Mandanten.

Die Registrierung erfolgt durch persönliches Erscheinen des Sub-Registrators oder auf Basis eines integeren Datenbestands des Mandanten.

Die gleiche Vorgehensweise gilt auch für die Sub-Registrator-Derivat (siehe Kapitel 1.3.2.2.2), die für das optionale Leistungsmerkmal „CMP-Schnittstelle“ benötigt wird.

3.2.3.4 Registrierung von Benutzer

Die Registrierung von Benutzern (natürlichen Person, Personen- und Funktionsgruppe, Pseudonym) erfolgt zentral oder dezentral durch den Sub-Registrator. Dabei gelten die Richtlinien wie unter Kapitel 4.2.1.2 beschrieben.

3.2.3.5 Registrierung von Geräten

Die Registrierung von Geräten (Server, Router/Gateway, Mail-Gateway und Domain-Controller) erfolgt zentral oder dezentral durch den Sub-Registrator. Dabei gelten die Richtlinien wie unter Kapitel 4.2.1.2 beschrieben.

3.2.4 Nicht verifizierte Teilnehmerangaben

Nicht verifizierte Informationen sind Informationen, die ohne Prüfung ins Zertifikat übernommen werden und umfassen:

- sonstige Informationen, die im Zertifikat als nicht verifiziert gekennzeichnet sind (z.B. Schlüsselverwendung, erweitere Schlüsselverwendung).

Zertifikate, die unter der Sub-CA “TeleSec Business CA 1” ausgestellt werden, enthalten von Telekom Security verifizierte Informationen.

Zertifikate, die unter der Sub-CA „Internal Business CA 1“ und „Business CA“ ausgestellt werden, können nicht verifizierte Informationen enthalten.

3.2.5 Berechtigungsprüfung

3.2.5.1 Sicherstellung der Authentizität des Zertifikatsantrags

Jeder Mandant bzw. beauftragte Drittpartei (Delegated Third Party) schließt mit Telekom Security einen Vertrag über die PKI-Dienstleistung „TeleSec Shared-Business-CA“ ab. Die beauftragte Drittpartei (Delegated Third Party) benennt der Telekom Security einen Mitarbeiter, der die Rolle des Master-Registrators wahrnimmt. Zur Feststellung der Authentizität des benannten Master-Registrators erfolgt ein Anruf bei der zentralen Telefonnummer der beauftragten Drittpartei, welche im Handelsregister oder einem vergleichbaren Verzeichnis hinterlegt ist. Der durchführende Registrierungsstellenmitarbeiter der Telekom Security (TC-Operator) lässt sich von der Zentrale mit dem oben genannten Vertreter des Kunden verbinden und bestätigt damit die Authentizität der genannten Person.

Ferner ernennt die beauftragte Drittpartei Mitarbeiter, die die Rolle des Sub-Registrators (ggf. Derivate des Sub-Registrators) wahrnehmen. Die Ernennungen müssen schriftlich in der Registrierungsstelle dokumentiert und archiviert (mindestens 7 Jahre) werden.

3.2.5.2 Prüfung von Domänen und IP-Adressen

Die beauftragte Drittpartei teilt der Telekom Security die Domäne(n) mit, auf die Zertifikate ausgestellt werden sollen, damit Telekom Security diese nach Prüfung als „erlaubte Internet-Domänen“ in die PKI-Konfiguration des Mandanten aufnehmen und pflegen kann.

Namensänderung(en) dieser Domäne(n) und/oder Besitzrechte dieser Domäne(n) sind unverzüglich schriftlich Telekom Security anzuzeigen.

Der Registrierungsstellenmitarbeiter der Telekom Security überprüft die relevanten Einträge, ob der Mandant die notwendigen Rechte an der entsprechenden Domäne besitzt. Dazu wird für geografische Top-Level-Domains (ccTLDs) die Online-Datenbank der landesspezifischen Stelle des NIC (z.B. Denic eG für Deutschland) bzw. für generische Top-Level-Domains (gTLDs) die des Whois abgefragt. Für die Überprüfung einer IP-Adresse werden adäquate Online-Datenbanken angefragt.

gTLDs dürfen nur für die Namensgebung von PKI-Mandanten und/oder zur Ausstellung von Zertifikaten verwendet werden, nachdem der gTLD-Betreiber den Besitz gegenüber dem TSP nachgewiesen hat und der ICANN-Vertrag (Registry Agreement) auf der ICANN-Webseite [www.ICANN.org] veröffentlicht wurde.

Der TSP prüft, ob der Antragsteller der Domain-Name-Registrant ist oder die Kontrolle über den Domain-Namen nachweisen kann, unter Verwendung der beschriebenen Validierungsmethoden (Kapitel 3.2.2.2.4 ff).

Führt dies nicht zum Erfolg, wird überprüft, ob der Mandant bzw. beauftragte Drittpartei über eine entsprechende Vollmacht des Antragstellers zur Nutzung der Domain oder der IP-Adresse verfügt. Der Antragsteller ist der Benutzer oder Vertreter einer Organisation, der über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt, auch wenn das Gerät den eigentlichen Antrag auf das Zertifikat sendet. Die Vollmacht ist vom Benutzer, Domäneninhaber oder Admin-C des Gerätes auszustellen.

Für Benutzer-Zertifikate, die für Mail-Security Verwendung finden (S/MIME-Zertifikate) und eine E-Mail-Adresse eines Internetdienstanbieters (Internet Service Providers (ISP)) enthalten, wird bei der Verwendung einer öffentlichen Zwischenzertifizierungsstelle (siehe Kapitel 1.3.1.2.1) von Telekom Security eine General-Vollmacht des jeweiligen Domain-Inhabers (z.B. t-online.de, gmx.de, 1und1.de) akzeptiert.

Im Falle, dass für diesen Zertifikatstyp ein Zertifikat von einer internen Zwischenzertifizierungsstelle ausgestellt wird (siehe Kapitel 1.3.1.2.2), reicht eine Kopie eines Identifikationsdokumentes (z.B. Unternehmensausweis, Personalausweis) aus. Hinweis: Die Zugangsnummer auf der Vorderseite des Personalausweises sollte aus Sicherheitsgründen geschwärzt werden, da sie bei Online-Funktionen verwendet werden kann.

Zur Erfüllung und Einhaltung der [CAB-BR] als auch diverser Root-Programme wird Telekom Security die Verwendungsrechte der Domäne(n) überprüfen.

Die „erlaubten Internet-Domänen“ werden, abhängig vom konfigurierten Zertifikatstyp, nach folgenden Zeiträumen geprüft:

- Öffentliche Server-Zertifikate
  - spätestens nach 13 Monaten bzw. 398 Tagen
- Alle anderen öffentlichen oder internen Zertifikate
  - spätestens nach 39 Monaten

Telekom Security behält sich vor, aktuelle Identifikationsdokumente des Inhabers der Master-Domäne und/oder Dritten zu dessen Lasten anzufordern.

3.2.5.3 Prüfung von CAA Einträgen im DNS

Für die Ausstellung von Server-Zertifikaten von einer öffentlichen Zertifizierungsstelle (siehe Kapitel 1.3.1.2.1) gilt:

Im Rahmen der Berechtigungsprüfung werden alle FQDN-Einträge gegen CAA-Einträge im DNS geprüft (Certification Authority Authorization; CAA Records for Fully Qualified Domain Names).

Wenn ein oder mehrere CAA Resource Records gefunden werden, dessen issue- bzw. issuewild-Property von „telesec.de“ abweicht, dann wird der Zertifikatsantrag abgelehnt. Enthält das issuewild-Property ein Semikolon „;“, dann wird ein Wildcard-Zertifikatsauftrag immer abgelehnt.

Wenn kein CAA Resource Record hinterlegt wurde oder dessen issue- bzw. issuewild-Property „telesec.de“ enthält, dann wird der Prüfprozess fortgesetzt.

TeleSec Shared-Business-CA verarbeitet 8 CNAME-Ketten-Einträge und begrenzt die Länge der Kette wie empfohlen auf maximal 10.

3.2.5.4 Zusätzliche Prüfungen des Mandanten

Sofern im Zertifikatsantrag der Name einer natürlichen Person dergestalt mit dem Namen einer Organisation verknüpft ist, dass daraus eine Berechtigung erkennbar wird, im Namen dieser Organisation handeln zu können, wird die Registrierungsstelle des Mandanten

- die Organisation auf ihre Existenz hin überprüfen. Dabei wird ein Identitätsprüfungsservice oder eine Identitätsprüfungsdatenbank eines Dritten genutzt oder wahlweise Dokumente bei der zuständigen Regierung oder Behörde abgefordert, die die Existenz der Organisation bestätigt, und
- Geschäftsinformationen einholen, die bestätigen, dass die Person, die den Zertifikatsantrag stellt, bei der Organisation beschäftigt ist und ob sie ggf. dazu autorisiert ist, im Namen der Organisation zu handeln.

3.2.6 Kriterien für Interoperabilität

Verwendet eine Sub-CA in einem von ihr signierten Zertifikat eine Policy-OID, welche die Erfüllung und Einhaltung der [CAB-BR] repräsentiert (siehe Kapitel 7.1.6.1), muss das jeweilige CP oder CPS der Sub-CA eine explizite Zusicherung enthalten, dass alle von der Sub-CA ausgestellten Zertifikate, welche diese Policy OID enthalten, in Übereinstimmung mit und Einhaltung von den [CAB-BR] ausgestellt und verwaltet werden.

Unter dem PKI-Service „TeleSec Shared-Business-CA“ werden keine weiteren Sub-CA Zertifikate ausgestellt.

Derzeit verwendet der PKI-Service „TeleSec Shared-Business-CA“ keine Cross-Zertifikate (siehe Abbildung 1).

3.3 Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung

Um durchgehend eine authentische und sichere Kommunikation anbieten zu können, muss sich der Endteilnehmer vor Ablauf eines gültigen Zertifikats ein neues Zertifikat beschaffen. Ob für die Folgebeauftragung ein neues Schlüsselpaar benötigt wird, ist abhängig von der eingesetzten Applikation und dem verwendeten Schlüsselspeicher (Smartcard, Soft-PSE).

Schlüsselerneuerung für Smartcard

Bei einer Folgebeantragung kann die aktuelle Smartcard mit den darauf befindlichen Schlüsselpaar verwendet werden, sofern technische Vorgaben (z.B. unsichere Krypto-Algorithmen) oder funktionale Beschränkungen (z.B. Ablauf des Fehlbedienungszählers) dies nicht verbieten oder verhindern. Andernfalls ist ein Folge-Zertifikat auf einer neuen Smartcard auszustellen. Es gelten die Regelungen der Registrierung wie im Kapitel 3.2.3 ff und 4.2.1 beschrieben. Sofern die Smartcard eine interne Schlüsselgenerierung unterstützt, können bei einer Folgebeauftragung neue Schlüsselpaare verwendet werden.

Schlüsselerneuerung für Soft-PSE

Bei Folgebeauftragungen als Soft-PSE werden im Allgemeinen neue Schlüsselpaare erzeugt, für bestimmte Geräte (z.B. Web-Server) kann aber auch der vorhandene Schlüssel erneut verwendet werden. Ob eine Schlüsselerneuerung stattfindet, liegt im Ermessen des Zertifikatsnehmers oder Mandanten. Die Regelungen in Kapitel 6.1 ff müssen beachtet werden.

Für die Ausstellung von Zertifikaten für Endteilnehmer (außer für Server) von einer öffentlichen Zertifizierungsstelle (siehe Kapitel 1.3.1.2.1) gilt:

- Telekom Security verwendet für die Validierung eines Erneuerungsauftrags ausschließlich Dokumente, Unterlagen oder sonstige Informationen, die bei der Ausstellung des Zertifikats nicht älter als 39 Monate sind.

Für die Ausstellung von Zertifikaten für Endteilnehmer (nur für Server) von einer öffentlichen Zertifizierungsstelle (siehe Kapitel 1.3.1.2.1) gilt:

- Telekom Security verwendet für die Validierung eines Erneuerungsauftrags ausschließlich Dokumente, Unterlagen oder sonstige Informationen, die bei der Ausstellung des Zertifikats
  - bis zum 31.08.2020: nicht älter als 825 Tage oder 27 Monate sind.
  - ab dem 01.09.2020: nicht älter als 398 Tage oder 13 Monate sind.

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Eine routinemäßige Schlüsselerneuerung obliegt unter Beachtung von Kapitel 6.1der Verantwortung des Mandanten. Die Identifizierung und Authentifizierung entspricht die einer Neubeauftragung (siehe Kapitel 3.2.2 ff und 3.2.3 ff).

3.3.2 Identitätsprüfung und Authentifizierung bei Schlüsselerneuerungen nach Zertifikatssperrung

Eine Zertifikatserneuerung eines gesperrten Zertifikats ist nicht möglich. Es steht nur die Option der Neubeauftragung und damit die beschriebene Identitätsprüfung zur Verfügung (siehe Kapitel 3.2.2 ff und 3.2.3 ff).

3.3.3 Identitätsprüfung nach Ablauf des Gültigkeitszeitraums

Nach Ablauf des Gültigkeitszeitraumes ist die Zertifikatserneuerung nicht möglich. Es steht nur die Option der Neubeauftragung und damit die beschriebene Identitätsprüfung zur Verfügung (siehe Kapitel 3.2.2 ff und 3.2.3 ff).

3.4 Identifizierung und Authentifizierung bei Sperranträgen

Die Authentifizierung von Sperranträgen erfolgt durch die Mitteilung von Zertifikatsinhalten (z.B. Common Name, Organisation/Firma, E-Mailadresse), um das zu sperrende Zertifikat suchen und selektieren zu können. Der Sperrantrag wird durch das dem Zertifikatsinhaber bekannte Sperrpasswort autorisiert. (siehe Kapitel 4.9.2)

4 BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

Die Zertifikatsbeantragung erfolgt, abhängig vom Registrierungsmodell (Kapitel 3.2.3), in elektronischer Form über eine Webseite (Sub-Registrator, Benutzer) oder technische Schnittstellen (SCEP- oder Mail-Schnittstelle).

Bedingt durch das Beantragungsverfahren bzw. die Schnittstelle wird ein Zertifikatsantrag bereits einem entsprechenden Zertifikatsprofil (z.B. Server, Router) zugeordnet.

4.1.1 Wer kann ein Zertifikat beantragen?

Für die Beantragung von Zertifikaten gelten folgende Voraussetzungen:

- Abschluss eines Vertragsverhältnisses über die Bereitstellung und Überlassung des PKI-Service TeleSec Shared-Business-CA zwischen dem Mandanten (externe Registrierungsstelle) oder Bevollmächtigten, und Telekom Security.
- Einrichtung einer Master-Domäne/PKI-Mandant (Kapitel 1.3.2.1),
- erfolgreiche Anmeldung der jeweiligen Rolle (Master-, Sub-Registrator, Benutzer) an der rollenspezifischen Webseite,
- optional: Zugangsdaten für die Mail-, SCEP- und CMP-Schnittstelle.

Folgende Personen können einen Zertifikatsantrag stellen:

- Autorisierte Personen einer externen Registrierungsstelle (Master-Registratoren, Kapitel 1.3.2.2.1),
- Autorisierte Personen einer externen Registrierungsstelle (Sub-Registratoren und deren Derivate, Kapitel 1.3.2.2.2),
- Autorisierte Personen, die als Subjekt des Zertifikats erscheinen,
- Autorisierte Personen, die als Vertreter des Antragstellers (Applicant Representative) auftreten,
- Autorisierte Personen von Personen- und Funktionsgruppen und Geräten,
- Autorisierte Personen der internen Registrierungsstelle der Telekom Security im Rahmen der Einrichtung und Verwaltung einer Master-Domäne (Kapitel 3.2.2 ff).

Als autorisierte Personen werden natürliche Personen verstanden, die entweder über ein gültiges Registrator-Zertifikat verfügen oder über geeignete Anmeldedaten verfügen.

4.1.2 Registrierungsprozess und Verantwortlichkeiten

4.1.2.1 Interne Registrierungsstelle

Die Einrichtung und weitere Pflege der Master-Domäne (PKI-Mandant), den „erlaubten Internet-Domänen“ und die Ausstellung des Master-Registrator-Zertifikats basieren auf einer erfolgreichen Authentifizierung der Identität von Organisationen, die in Kapitel 3.2.2 ff beschrieben ist.

PKI-Mandanten, die für den TSP eingerichtet und gepflegt werden, unterliegen den gleichen Anforderungen der Registrierungsprozesse.

4.1.2.2 Externe Registrierungsstelle

4.1.2.2.1 Einrichtung des Mandanten

Zur Einrichtung der Master-Domäne verpflichtet sich der Auftraggeber des Mandanten das Dokument „Auftrag zur Einrichtung einer Master-Domäne für die TeleSec Shared-Business-CA“ wahrheitsgemäß auszufüllen, von einem Berechtigten unterschreiben zu lassen und mit den erforderlichen Identifikationsdokumenten Telekom Security vorzulegen, damit Telekom Security wie in Kapitel 3.2.2 ff die Identifikationsprüfung durchführen kann. In diesem Dokument wird auch der Master-Registrator benannt. Nach der Ausstellung des Master-Registrator-Zertifikats wird dieses inkl. „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ zugesandt, die er schriftlich akzeptieren muss. Diese Einwilligung ist bei jeder Zertifikatserneuerung über das Web-Portal online zu wiederholen.

Der Mandant/externe Registrierungsstelle verpflichtet sich auch, die Bestätigung der Einhaltung der Regelungen dieses Dokuments CPS in seiner jeweils aktuellen Version auf seine Registrierungsstellenmitarbeiter (Master- und Sub-Registrator und deren Derivate, Kapitel 1.3.2.2.2) und Endteilnehmer zu übertragen. Neue Versionen werden von der Zertifizierungsstelle frühzeitig bekanntgegeben.

Der PKI-Service TeleSec Shared-Business-CA unterstützt zwei Registrierungsmodelle wie in Kapitel 3.2.3 ff beschrieben. Die Auswahl des Registrierungsmodells obliegt der Verantwortung der beauftragten Drittpartei (Delegated Third Party).

PKI-Mandanten, die für den TSP eingerichtet und gepflegt werden, unterliegen den gleichen Anforderungen der Registrierungsprozesse.

Bei Nutzung der SBCA mit Auslandsbezug sind zusätzlich die geltenden nationalen Export- und Importbestimmungen zu beachten.

4.1.2.2.2 Endteilnehmer inkl. Registrierungsstellenmitarbeiter

Alle Endteilnehmer inkl. Registrierungsstellenmitarbeiter (Master- und Sub-Registrator und deren Derivate, Kapitel 1.3.2.2 ff) erkennen das Dokument „Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS))“ in seiner aktuellen Version als auch die Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA inkl. Datenschutzerklärung an und verpflichten sich die dort beschriebenen Regelungen einzuhalten.

Ferner verpflichtet sich der Endteilnehmer und Registrierungsstellenmitarbeiter,

- dass die im Zertifikatsantrag gemachten Angaben wahr und korrekt sind, und zugleich den Bestimmungen der Namensgebung genügen (siehe Kapitel 3.1.1.1 ff),
- zu einer Übermittlung des öffentlichen Schlüssels und der Zertifikatsdaten an Telekom Security zur Zertifikatserzeugung,
- einen Nachweis über den Besitz des privaten Schlüssels zu führen, der in Verbindung mit dem zertifizierten öffentlichen Schlüssel steht.

Vor Ausstellung des Sub-Registrator-Zertifikats muss der Sub-Registrator die „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ schriftlich zu akzeptieren. Diese Einwilligung ist bei jeder Zertifikatserneuerung über das Web-Portal online zu wiederholen.

Vor Ausstellung des Endteilnehmer-Zertifikats muss der Antragsteller oder Vertreter des Antragstellers die „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ akzeptieren. Diese Einwilligung ist, abhängig vom Benatragungsverfahreb (z.B. Web-Formular, Bulk), bei jeder Zertifikatserneuerung online zu wiederholen.

Falls der Zertifikatsnehmer und die ausstellende CA einer gemeinsamen juristischen Person angehören (Verbundenes Unternehmen, Affiliate), muss der Repräsentant des Antragstellers vor der Ausstellung eines Zertifikates die „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ akzeptieren. Ist der Zertifikatsnehmer eine beauftragte Drittpartei (Delegated Third

Party), der Zertifikate für die „Eigennutzung“ verwendet (Enterprise RA) und nicht als Reseller (Wiederverkäufer) an Dritte veräußert, muss vor der Ausstellung eines Zertifikates die „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA" akzeptieren werden.

Im Falle, dass über eine beauftragte Drittpartei (Delegated Third Party) als Reseller (Wiederverkäufer) der Zertifikatsnehmer ein Zertifikat beauftragt/beantragt, muss dieser vor der Ausstellung eines Zertifikates den „Bezugsvertrag“ (Subscriber Agreement)" akzeptieren.

Im Falle, dass Antragsteller und Registrierungsstellenmitarbeiter die gleiche Person sind, ist der Zertifikatsantrag von einem Dritten (z.B. Vorgesetzte Person) schriftlich zu bestätigen.

Die o.g. Pflichten gelten ebenfalls für den TSP, der in seinem Namen Zertifikate ausstellt.

Die Telekom Security behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Endteilnehmer abzuschließen.

4.2 Bearbeitung von Zertifikatsanträgen

Die folgende Prozessbeschreibung gilt auch für den TSP selbst, wenn dieser in seinem Namen Zertifikate ausstellt.

Ein Zertifikatsantrag (Request), der aus einem Gerät oder einer Anwendung stammt, wird auf definierte Inhalte des Subject DN (siehe Kapitel 3.1.1 ff) und Verwendung unerlaubter Zeichen überprüft. Vorbelegte Inhalte der Attribute Organizational Unit Name 1 und 2 (Kapitel 3.1.1.1.3 und 3.1.1.1.4) werden immer mit der Zertifikatsgenehmigung bzw. –ausstellung durch die dem zuständigen Sub-Registrator zugeordneten Einträge überschrieben.

Inhalte, die über den Subject DN hinausgehen (z.B. Schlüsselverwendung, erweiterte Schlüsselverwendung), werden ohne Benachrichtigung oder Hinweis ignoriert. Es gilt die Ausprägung des jeweiligen Zertifikatsprofils wie in Kapitel 7.1 ff beschrieben.

Die Verwendung von unerlaubten Zeichen wird mit der Überprüfung angezeigt oder dem Antragsteller per E-Mail mitgeteilt.

4.2.1 Durchführung der Identifikation und Authentifizierung

4.2.1.1 Interne Registrierungsstelle

Die Ausstellung des Master-Registrator-Zertifikats basiert auf einer erfolgreichen Authentifizierung der Identität von Organisationen, die in Kapitel 3.2.3 ff beschrieben ist. Es sind die Namensformen gemäß Kapitel 3.1.1 ff einzuhalten.

Die Existenz des von Mandanten gemeldeten Master-Registrators wird durch den TSP jährlich in Schriftform überprüft (z.B. per Mail).

4.2.1.2 Externe Registrierungsstelle

Die Authentifizierung der Endteilnehmer erfolgt durch Sub-Registratoren (siehe Kapitel 1.3.2.2 ff) innerhalb der beim Mandanten etablierten zuständigen Registrierungsstelle.

Die externe Registrierungsstelle verpflichtet sich folgende Tätigkeiten durchzuführen:

- Die Registrierung erfolgt durch
  - persönliches Erscheinen des Endteilnehmers, seines Vertreters oder eines Schlüsselverantwortlichen, der sich durch Vorlage geeigneter Identifikationsdokumente ausweisen kann und für die ordnungsgemäße Erstellung des Zertifikatsantrages als auch für die Installation des Zertifikats verantwortlich ist, oder
  - einen anderen geeigneten Prozess (z.B. Beantragung über die Benutzer-Webseite, Mail-, SCEP- oder CMP-Schnittstelle), aus dem die Identität des Endteilnehmers eindeutig hervorgeht. Die Subjektdaten des Zertifikats dürfen auf einem integeren Datenbestands

des Mandanten basieren. Die Generierung des Datenbestands ist auf Anfrage der Zertifizierungsstelle darzulegen.

- Bei Zertifikatsanträgen für Geräte oder Personen- und Funktionsgruppen ist zusätzlich die natürliche Person (z.B. Administrator) als Schlüsselverantwortlichen zu authentisieren, die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt.
- Der Registrierungsstellenmitarbeiter nimmt den Zertifikatsantrag in elektronischer Form oder Papierform entgegen, prüft diesen auf Integrität und Authentizität und die im Antrag enthaltenen Angaben gegenüber vom Antragsteller vorgelegten eindeutigen Identifikationsdokumenten (z.B. Unternehmensausweis, Personalausweis (Hinweis: Die Zugangsnummer auf der Vorderseite sollte aus Sicherheitsgründen geschwärzt werden, da sie bei Online-Funktionen verwendet werden kann), ERP-System) auf Authentizität (Echtheit, Glaubwürdigkeit), Integrität (Unversehrtheit), Korrektheit, Wahrheit und Vollständigkeit. Zur Authentifizierung der Antragsdaten dürfen zuverlässige interne oder öffentliche Datenquellen verwendet werden.
- Es sind die Namensformen gemäß Kapitel 3.1.1 ff einzuhalten.
- Für Benutzer-Zertifikate, die für Mail-Security Verwendung finden (S/MIME-Zertifikate) und die von der Sub-CA „TeleSec Business CA 1“ ausgestellt werden, muss die externe Registrierungsstelle eine elektronische Überprüfung der E-Mail-Adresse durchführen. Die erfolgt auf Basis eines „Challenge-Response-Verfahrens“, indem der Endteilnehmer aufgefordert wird, die Existenz der E-Mail-Adresse nachzuweisen.
- Bei der elektronischen Beantragung des Zertifikats über die jeweilige Webseite bzw. Mail-Schnittstelle werden der Domänenteil (domain-part) der E-Mail-Adresse (optional auch der UPN) auf die in der PKI-Konfiguration eingetragenen „erlaubten Internet-Domänen“ geprüft.
- Für Geräte-Zertifikate ist, abhängig vom Zertifikatstyp, der Domänenteil (domain-part) der E-Mail-Adresse oder DNS-Name (Top-Level-Domain und weiteren Sub-Domains des FQDN), auf die in der PKI-Konfiguration eingetragenen „erlaubten Internet-Domänen“ zu prüfen.
- Im Falle, dass der Mandant über weitere Domänen verfügt, auf die Zertifikate ausgestellt werden sollen, ist Telekom Security über die zusätzliche Domäne zu informieren. Nach erfolgreicher Domänenprüfung werden diese in die PKI-Konfiguration der Master-Domäne (PKI-Mandant) aufgenommen (siehe auch Kapitel 3.2.2 ff und 4.2.1.1).
- Irreführende Antragsdaten sind gegenüber dem Antragsteller abzulehnen.
- Im Falle gleiche Namensgebung muss die Registrierungsstelle eine Eindeutigkeit herstellen.
- Im Falle, dass die Antragsdaten nicht mit den Daten des Mandanten (Country Name (C), Organization Name (O), Organizational Unit Name, Domänenteil der E-Mail-Adresse und ggf. User Principal Name (UPN), Top-Level- und weitere Sub-Domains des Fully Qualified Domain Name (FQDN), siehe auch Kapitel 3.1.1 ff) übereinstimmen, ist eine Vollmacht oder ein Berechtigungsdokument des Antragstellers erforderlich.
- Für Zertifikate für Gruppen- und Funktionszertifikate oder Pseudonym gelten die Ausführung des Kapitels 3.1.3.
  - Bei Gruppen- und Funktionszertifikaten ist die Identität des verantwortlichen Antragstellers oder Vertreter durch den Sub-Registrator zu prüfen, bewerten und nach Freigabe zu dokumentieren.
  - Bei der Verwendung eines Pseudonyms ist die amtliche Identität des Endteilnehmers bzw. Zertifikatnehmers durch den Sub-Registrator festzustellen und zu dokumentieren.
  - Die Verantwortung obliegt dem Mandanten.
- Die vom Antragsteller vorgelegten eindeutigen Identifikationsdokumenten sind als Kopie revisionssicher mindestens 7 Jahre zu Lasten des Mandanten/externe Registrierungsstelle zu archivieren. Dieses Archiv ist vor unbefugtem Zugriff zu schützen.
- Im Falle von Audits oder anderen Prüfungen (z.B. Stichprobenprüfungen) sind die Registrierungsdokumente Telekom Security oder einer von Telekom Security bestimmten qualifizierten Auditor offen zu legen.
- Abhängig vom Registrierungsmodell (Kapitel 3.2.3) ist zu prüfen, ob der Antragsteller oder Vertreter den „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“

akzeptiert. Im Falle der Ablehnung eines dieser Dokumente ist der gesamte Zertifikatsantrag abzulehnen.

- Bei der Ausstellung von Server-Zertifikaten durch die Sub-CA „TeleSec Business CA 1“ müssen die Registrierungsstellenmitarbeiter die Anforderungen der jeweils aktuellen Version der [CAB-BR] Kapitel 7.1.4.2 ff (Subject Information) und 3.2.2 ff (Authentication of Organization and Domain Identity) der jeweils aktuellen Version der [CAB-BR] erfüllen.
- Die Registrierungsstellenmitarbeiter sind verpflichtet, verdächtige Schlüsselkompromittierungen, Zertifikatsmissbrauch oder andere zertifikatsbetreffende Betrugsfälle oder -versuche unverzüglich gegenüber der Telekom Security zu melden.
- Zertifikatsanträge, deren Einträgen mit der „High Risk List“ (Kapitel 4.2.2.2) übereinstimmen, sind besonders sorgsam durch den Registrierungsstellenmitarbeiter zu prüfen.
- Zertifikatsanträge, deren Einträgen mit der „Denied List“ (Kapitel 4.2.2.2) übereinstimmen, sind zusätzlich durch das Trust Center der Telekom Security zu genehmigen.
- Elektronische Einstellung von Registrierungsdaten durch den Sub-Registrator (optionale Funktion). Diese „Vorregistrierungsdaten“ (Pre Authentication Data) unterstützen eine automatische Zertifikatsausstellung, sofern die Antragsdaten, die über Benutzer-Webseite, SCEP- oder CMP-Schnittstelle gestellt werden, mit den Vorregistrierungsdaten übereinstimmen.

Mit der Beantragung über die Webseiten wird der Zertifikatsantrag durch die Zertifizierungsstelle auf erhöhtes Risiko auf folgende Listeneinträge hin überprüft:

- **Denied List**: Telekom Security unterhält eine interne Datenbasis, in die gesperrte Zertifikate eingehen, die in Zusammenhang mit Phishing-, Missbrauchs- oder Betrugsversuchen stehen. Diese Informationen werden verwendet, um zukünftige verdächtige Zertifikatsaufträge identifizieren zu können.
- **High Risk List**: Bei Telekom Security werden sowohl Organisationen, als auch Domainnamen bzw. IP-Adressen in einer Datenbank gepflegt, die möglicherweise aufgrund ihrer Attraktivität Ziel von Phishing-, Missbrauchs- oder Betrugsattacken sein könnten. Diese Zertifikatsaufträge werden automatisch kenntlich gemacht, um die Registrierungsstellenmitarbeiter auf die besondere Sorgfaltspflicht hinzuweisen. Dabei wird einem dokumentierten Prozess gefolgt. Dadurch soll zusätzliche Wachsamkeit und Aufmerksamkeit bei der Überprüfung der Auftragsdaten erzeugt werden. Die Prüfung kann im Einzelfall dazu führen, dass ein beauftragtes Zertifikat nicht ausgestellt wird.

Im Falle, dass der Zertifikatsantrag mit den Einträgen der „High Risk List“ übereinstimmen, bedarf es einer zusätzlichen Genehmigung durch die interne Registrierungsstelle der Telekom Security.

Im Falle, dass der Zertifikatsantrag mit den Einträgen der „High Risk List“ übereinstimmen, wird der Antragsteller informiert, dass er gerade ein Zertifikat beantragt, das die „High-Risk-Kriterien“ erfüllt und dass die Sicherheitsanforderungen an den Registrierungsprozess in diesem Fall und damit auch den Registrierungsstellenmitarbeiter besonders erhöht sind. Zusätzlich ist diese Prüfung schriftlich in dem elektronischen Antrag zu bestätigen.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Durch die Vergabe einer Referenznummer bei der Zertifikatsbeauftragung wird die eindeutige Zuordnung von einem ausgestellten Zertifikat zu den entsprechenden Auftragsunterlagen und Zusatzdokumenten (z.B. Vollmachten) hergestellt.

4.2.2.1 Interne Registrierungsstelle

4.2.2.1.1 Master-Registrator-Zertifikat

Wenn die Authentifizierung der erforderlichen Endteilnehmer-Informationen nach Kapitel 3.2.2 und 4.2.1.1 erfolgreich war, wird der Zertifikatsauftrag genehmigt und das Master-Registrator-Zertifikat zur Verwaltung des Mandanten ausgestellt.

Telekom Security verwendet für die Validierung eines Auftrags, der zur Ausstellung des Master-Registrator-Zertifikats führt, ausschließlich aktuelle und gültige Dokumente, Unterlagen oder sonstige Informationen (z.B. Ausweiskopie, Telefonanruf zum Master-Registrator).

Im Falle, dass die Identifikationsdaten nicht mit den Prüfungsdaten übereinstimmen, ist der Zertifikatsantrag abzulehnen.

4.2.2.1.2 Prüfung von Domänen- und Organisationsdaten

Die Interne Registrierungsstelle führte folgende Prüfungen durch:

- Existenz und Zugehörigkeit der Domäne zu einem Mandanten (Kapitel 3.2.2 ff, 3.2.3 ff, 3.2.5 ff).
  - Für gTLD gilt: Telekom Security überprüft regelmäßig (maximal alle 30 Tage) auf der ICANN-Website (https://newgtlds.icann.org), ob neue gTLD freigegeben oder gekündigt wurden. Im Falle von Änderungen erfolgt eine Überprüfung, ob Zertifikate bereits Domainnamen mit dieser gTLD enthalten. Ferner wird eine weitere Zertifikatsausstellung für diese gTLD unterbunden, bis die Kontrolle über den Domainnamen oder das ausschließliche Recht des Antragstellers zur Verwendung des Domain-Namens nachgewiesen wurde. Im Falle, dass ein Nachweis nicht erbracht werden kann oder die gTLD gekündigt wurde, sind alle ausgestellten Zertifikate mit dieser TLD im Domainnamen innerhalb von 120 Tage zu sperren (siehe Kapitel 4.9.1.1).
- Prüfung der Organisationsdaten (Organisationsname (Kapitel 3.1.1.1.2) und Lokation (Land, Bundesland, Ort siehe Kapitel 3.1.1.1.1, 3.1.1.1.10 und 3.1.1.1.9)).

Nach erfolgreicher Domänen-Prüfung wird diese in die zugehörige Mandanten-Konfiguration als „erlaubte Domain“ dem jeweiligen Zertifikatstyp (z.B. Benutzer, Server) hinzugefügt.

Optional besteht die Möglichkeit, die Organisationsdaten mit der Domäne als Vorbelegung in die Mandanten-Konfiguration aufzunehmen (Vorbelegung von Organisationsdaten).

Die Bearbeitung dieser Aufträge erfolgt innerhalb eines angemessenen Zeitraums nach Erhalt der vollständigen Unterlagen.

4.2.2.2 Externe Registrierungsstelle

Nur nach erfolgreicher Registrierung des Zertifikatsnehmers wird ein Zertifikatsantrag weiterbearbeitet (siehe Kapitel 3.2.3 und 4.2.1.2). Abhängig vom Registrierungsmodell (Kapitel 3.2.3) stellt der Sub-Registrator über seine Webseite den Zertifikatsantrag in elektronischer Form ein oder genehmigt den bereits in elektronischer Form vorliegenden Antrag.

Ein Zertifikatsauftrag muss abgelehnt werden, wenn

der Zertifikatsantrag und die Identifikationsdokumente nicht vollständig, wahr oder korrekt sind,

- der Zertifikatsantrag und die Identifikationsdokumente aus einer nicht integren Quelle stammen,
- der Zertifikatsantrag und die Identifikationsdokumente zu keinem eindeutigen positiven Registrierungsergebnis führen,
- der öffentliche Schlüssel die Mindestschlüssellänge von 2048 Bit unterschreitet (Ausnahme sind möglich bei Verwendung der Sub-CA „Business CA“),
- der Public Exponent nicht den Vorgaben der [CAB-BR] entspricht,
- die Untersuchung auf Debian-Schwäche (Debian weak key) positiv ausfällt,

- wenn Antragsdaten mit High-Risk-Kriterien übereinstellen,
- bei Server-Zertifikaten, ausgestellt von den Sub-CA „TeleSec Business CA 1“, ein CAA Resource Record des Typs 257 gefunden wird, der nicht den Eintrag (tag=issue bzw. issuewild-Property, value=telesec.de) enthält.

Der Registrierungsstellenmitarbeiter kann bei unvollständigen Identifikationsdokumenten den Antrag auf Wiedervorlage stellen.

Im Falle einer Zurückstellung oder Ablehnung des Auftrags wird der Beauftragte (Techn. Ansprechpartner) des Zertifikatsnehmers unter Angabe von Gründen per E-Mail benachrichtigt.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

4.2.3.1 Interne Registrierungsstelle

Die Bearbeitung des Zertifikatantrags für Master-Registratoren auf Basis des Dokuments „Einrichtung einer Master-Domäne für TeleSec Shared-Business-CA“ oder „Nachbeauftragung von weiteren Master-Registrator-Zertifikaten“ erfolgt innerhalb eines angemessenen Zeitraums nach Erhalt eines der vollständigen Unterlagen.

4.2.3.2 Externe Registrierungsstelle

Die Bearbeitungsdauer von Zertifikatsanträgen für Endteilnehmer-Zertifikate (außer Master-Registrator-Zertifikat) obliegt der Zuständigkeit und Verantwortung des Mandanten.

4.3 Zertifikatsausstellung

Die folgende Prozessbeschreibung gilt auch für den TSP selbst, wenn dieser in seinem Namen Zertifikate ausstellt.

4.3.1 Maßnahmen der Zertifizierungsstelle während der Ausstellung von Zertifikaten

4.3.1.1 Interne Registrierungsstelle

Nach der Genehmigung des Zertifikatsantrags durch die interne Registrierungsstelle wird das Master-Registrator-Zertifikat unmittelbar von der Zertifizierungsstelle (CA-System) ausgestellt.

Umstände können dazu führen, dass eine Zertifikatsausstellung zurückgestellt wird, wenn

- die Identifizierung und Authentifizierung der erforderlichen Informationen für den Master-Registrator gemäß Abschnitt 3.2 ff erfordert die Einholung weiterer Informationen,
- das Vorlegen eventuell erforderlicher und angeforderten Zusatzdokumente verzögert sich,
- der Master-Registrator antwortet bei Rückfragen oder Kontaktaufnahme nicht.

Die Zurückstellung eines Zertifikats wird dem Endteilnehmer per E-Mail mitgeteilt.

4.3.1.2 Externe Registrierungsstelle

Nach der Genehmigung durch die externe Registrierungsstelle prüft das CA-System den Zertifikatsantrag auf die in der PKI-Konfiguration des Mandanten (Master-Domäne) eingetragenen „erlaubten Internet-Domänen“ und, sofern zutreffend, die „vorbelegten Organisationsdaten“ (Kapitel 4.2.2.1.2). Im Falle einer Gutprüfung wird das Zertifikat unmittelbar ausgestellt.

Im Falle der Beantragung über die CMP-Schnittstelle kann von diesem Prozess abgewichen werden. Optional kann das Zertifikat auch ohne Genehmigung durch den zuständigen Sub-Registrator ausgestellt werden.

Im Falle, dass im Zertifikatsantrag Informationen enthalten sind, die nicht mit den „erlaubten Internet-Domänen“ übereinstimmen, wird die Zertifikatsaustellung nicht durchgeführt und der der zuständige Sub-Registrator per Hinweismeldung informiert.

Zertifikatsanträge, die mit den Vorregistrierungsdaten übereinstimmen, werden ohne Genehmigung des Sub-Registrators freigegeben und die Zertifikate direkt ausgestellt.

Im Falle, dass für den Mandanten die optionale Funktion der Vorregistrierung eingerichtet ist und Vorregistrierungsdaten durch den Sub-Registrator eingestellt wurden, werden alle Zertifikatsanträge, die über die Benutzer-Webseite, SCEP- oder CPM-Schnittstelle gestellt werden direkt ausgestellt.

4.3.2 Benachrichtigung von Endteilnehmern über die Ausstellung von Zertifikaten

Abhängig vom Zertifikatstyp wird der Zertifikatsnehmer, Antragsteller oder Vertreter über die Ausstellung des Zertifikats per E-Mail benachrichtigt (approval notification). In dieser E-Mail befinden sich die relevanten Zertifikats-Informationen.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme durch den Zertifikatsinhaber

Das folgende Verhalten stellt die Annahme eines Zertifikats dar:

- Das Herunterladen und Installieren eines Zertifikats auf Basis einer Mitteilung oder deren Anhang durch den Endteilnehmer.
- Die Annahme des Schlüsselmaterials inkl. PIN bzw. Passwort (Smardcard oder Soft-PSE), dass für den Endteilnehmer oder Registrator ausgestellt wurde.
- Falls der Endteilnehmer nicht innerhalb einer vom Mandanten definierten Frist nach Erhalt des Zertifikats Einwände gegen das Zertifikat oder seinen Inhalt gegenüber der zuständigen Registrierungsstelle erhebt.
- Kein Widerspruch gegenüber der zuständigen Registrierungsstelle innerhalb einer vom Mandanten definierten Frist nach Erhalt des Zertifikats bzw. Inhalt des Zertifikats.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Die Veröffentlichung von Zertifikaten erfolgt über einen Verzeichnisdienst oder Web-basierenden Zugriff auf eine Datenbank. Dabei gelten folgende Regelungen:

- Die Veröffentlichung der Zertifikate ist abhängig vom Zertifikatstyp und den Regelungen gemäß Tabelle 15.
- Es können zusätzlich bestimmte Zertifikatstyp (siehe Tabelle 15) nach Absprache mit dem Mandanten veröffentlicht werden.
- Ob der Verzeichnisdienst öffentlich oder geschützt ist, liegt im Ermessen des Mandanten und wird bei Einrichtung der Master-Domäne konfiguriert. Evtl. datenschutzrechtliche Vereinbarungen liegen in der Zuständigkeit des Mandanten. Der Master-Registrator kann in den darunterliegenden Zuständigkeitsbereichen (Sub-Domänen) ebenfalls einen Zugriffsschutz konfigurieren.

Für die Veröffentlichung von Server-Zertifikaten durch eine öffentliche Zertifizierungsstelle (Kapitel 1.3.1.2.1) kann innerhalb Mandantenkonfiguration die CT-Funktion (Certificate Transparency) aktiviert werden. In diesem Falle wird das Server-Zertifikat mit einem SCT-Eintrag versehen und auf mehreren CT-Logservern veröffentlicht.

Wichtiger Hinweis: Die Nichtveröffentlichung via CT-Logserver zieht eine Einschränkung des Leistungsumfangs nach sich und kann dazu führen, dass eine Applikation das Server-Zertifikat nicht akzeptiert oder ablehnt.

4.4.3 Benachrichtigung über die Zertifikatsausstellung durch die Zertifizierungsstelle an weitere Instanzen

Die Benachrichtigung per E-Mail (approval notification) an weitere Instanzen (z.B. Registratoren, Administratoren, Funktionsgruppen) ist in der Master-Domäne konfigurierbar.

4.4.4 Certificate Transparency

TeleSec Shared-Business-CA unterstützt Certificate Transparency (CT). Weitere Informationen finden Sie unter: https://www.certificate-transparency.org und [RFC6962].

Alle von einer öffentlichen Zertifizierungsstelle (CA) (Kapitel 1.3.1.2.1) ausgestellten Server-Zertifikate enthalten per Voreinstellung (default) die Erweiterung „Certificate Transparency (CT)“ (Kapitel 7.1.11). Diese Erweiterung kann auf Kundenwunsch auch deaktiviert werden.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Das Zertifikat und der zugehörige private Schlüssel darf nur entsprechend den einzelvertraglichen Regelungen, dieser CPS, die „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ verwendet werden.

Die Verwendung des privaten Schlüssels, mit dem dazu gehörigen zertifizierten öffentlichen Schlüssel, ist erst gestattet, nachdem der Endteilnehmer das Zertifikat angenommen hat (Kapitel 4.4.1). Die Zertifikatsnutzung wird durch die Vorgaben und Verwendungszweck des Mandanten bestimmt. Die technische Zertifikatsverwendung ist im Zertifikat als Attribut „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ definiert.

Alle Endteilnehmer und Registratoren sind verpflichtet,

- ihre privaten Schlüssel vor unbefugtem Gebrauch schützen,
- ihre privaten Schlüssel keinem Dritten, auch nicht als Vertreter(in), zu übereignen oder offen zu legen,
- den privaten Schlüssel nach Ablauf des Gültigkeitszeitraums oder der Sperrung des Zertifikats nicht mehr benutzen, außer zur Einsichtnahme verschlüsselter Daten (z.B. Entschlüsselung von E-Mails).

Für Zertifikate von Personen- und Funktionsgruppen und Geräten gelten darüber hinaus folgenden Anforderungen:

- Der Schlüsselverantwortliche (Kapitel 1.3.3) ist für das Kopieren bzw. Weitergeben der Schlüssel an den/die Endteilnehmer verantwortlich.
- Der Schlüsselverantwortliche muss den/alle Endteilnehmer zur Einhaltung dieser CPS im Umgang mit dem privaten Schlüssel verpflichten.

- Zertifikatssperrungen können auf Personen aus dem Kreise der Endteilnehmer übertragen werden. Der Schlüsselverantwortliche muss dem/den Sperrberechtigten die Details zu Sperranlässen und das Sperrpasswort mitteilen.
- Nach dem Ausscheiden einer Person aus dem Kreise der Endteilnehmer (z.B. Kündigung des Vertragsverhältnisses) muss ein Missbrauch des privaten Schlüssels durch den Benutzer oder Schlüsselverantwortlichen verhindern werden, indem das Zertifikat gesperrt wird.
- Eine Übertragung der Verantwortung an einen neuen oder zusätzlichen Schlüsselverantwortlichen ist bei der zuständigen Registrierungsstelle zu beantragen und dort zu dokumentieren. Der neue Schlüsselverantwortliche ist gemäß dieser CPS zu identifizieren und zu registrieren, seine Autorisierung als Schlüsselverantwortlicher muss nachgewiesen werden.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Vertrauende Dritte

Jeder Vertrauende Dritte, der ein Zertifikat einsetzt, das von der TeleSec Shared-Business-CA ausgestellt wurde, sollte

- vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen,
- vor der Nutzung des Zertifikats dessen Gültigkeit überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie), den Gültigkeitszeitraum und die Sperrinformationen (CRL, OCSP) des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit der vorliegenden CPS einsetzen. Telekom Security ist nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich,
- den technischen Verwendungszweck prüfen, der durch das im Zertifikat angezeigte Attribut „Schlüsselverwendung“ und ggf. „erweiterte Schlüsselverwendung“ festgelegt ist.

Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Abhängig vom Zertifikatstyp wird der Zertifikatsnehmer, Antragsteller, Vertreter oder weitere Instanzen über die Erneuerung des Zertifikats per E-Mail benachrichtigt (renewal notification), dort sind die relevanten Zertifikats-Informationen enthalten.

Der Versand dieser Benachrichtigung erfolgt 30 Kalendertage vor Ablauf des Zertifikats und wird mehrfach wiederholt, bis das Zertifikat erneuert wurde oder abgelaufen ist.

Bei einer Zertifikatserneuerung wird dem Zertifikatsnehmer ein neues Zertifikat mit neuer Seriennummer, neuem Gültigkeitszeitraum und gleichen Subject-DN (Kapitel 3.1.1.1) ein neues Zertifikat ausgestellt.

Eine Zertifikatserneuerungsfunktion ist nur für Benutzer-Zertifikate implementiert.

Für andere Zertifikatstyp bedarf es einer Zertifikatsneubeantragung, auch wenn dazu auf den ursprünglichen technischen Antragsdaten zurückgegriffen werden kann.

Eine Zertifikatserneuerung ist grundsätzlich nur mit gültigem Zertifikat und Vorhandensein des privaten Schlüssels möglich. Eine Erneuerung eines gesperrten oder abgelaufenen Zertifikats ist nicht möglich. Eine Zertifikatserneuerung kann, abhängig vom Schlüsselmaterial Smartcard oder Soft-PSE, mit oder ohne neuer Schlüsselgenerierung erfolgen. Bei der Verwendung des gleichen Schlüsselpaares wird jedoch vorausgesetzt, dass die eindeutige Zuordnung von Zertifikatsnehmer und Schlüssel erhalten bleibt, keine Kompromittierung des Schlüssels vorliegt und die

kryptographischen Parameter (z.B. Schlüssellänge) für die Gültigkeitsdauer des neuen Zertifikats noch ausreichend sind.

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, muss der Endteilnehmer die Akzeptanz dieser neuen Nutzungsbedingungen vor der Ausstellung eines neuen Zertifikats immer bestätigen.

4.6.1 Umstände für eine Zertifikatserneuerung

Sofern keine Gründe (z.B. Vertragskündigung, Namensänderung) dagegensprechen, muss sich der Zertifikatnehmer vor Ablauf seines gültigen Zertifikats ein neues Zertifikat beschaffen, um die Kontinuität der Zertifikatsnutzung gewährleisten zu können.

Eine Zertifikatserneuerung ist nur für Benutzer- und Registrator-Zertifikate vorgesehen und nur innerhalb von 30 Kalendertagen vor Ablauf der Gültigkeit des vorhandenen Zertifikats möglich. Zur Zertifikatserneuerung muss das Zertifikat inkl. privatem Schlüssel vorliegen.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Grundsätzlich liegt die Zertifikatserneuerung im Ermessen des Mandanten und sollte unbedingt vorab im Rahmen eines „Schlüsselsicherungskonzeptes (Key-Back-Up)“ definiert sein.

Die Zertifikatserneuerung wird ausschließlich von registrierten Personen (bei Vorliegen des privaten Schlüssels) oder autorisierten Personen (Schlüsselverantwortlicher, Geräte-Administrator) beauftragt. Die autorisierte Person verfügt sowohl über die erforderlichen Login-Daten als auch über das Zertifikat-Service-Passwort.

4.6.3 Bearbeitung von Zertifikatserneuerungen

Das Erneuerungsverfahren muss gewährleisten, dass nur berechtigte Zertifikatsnehmer (Benutzer, Schlüsselbeauftragte) diesen Prozess durchführen können.

Als Authentifizierungsmerkmal wird bei der Erneuerung von Endteilnehmer-Zertifikaten der Besitz des vollständigen Schlüsselmaterials (Zertifikat und privater Schlüssel) vorausgesetzt.

Die Erneuerung von Registrator-Zertifikaten (Master-RA- und Sub-RA-Zertifikate und deren Derivate, Kapitel 1.3.2.2.2) erfolgt durch den Zertifikatsinhaber selbst. Es ist zu beachten, dass nach dem Erneuerungsprozess das zu erneuernde Zertifikat nicht automatisch gesperrt wird. Der Registrator verfügt für eine Übergangsfrist (Erneuerungszeitraum bis Ablauf des Zertifikats) über zwei gültige Zertifikate. Das zu erneuernde Zertifikat kann während dieser Frist von dem hierarchisch übergeordneten Registrator gesperrt werden (Kapitel 4.9.3.3 ff).

Mit der Einrichtung des Zuständigkeitsbereiches (Sub-Domäne) erfolgt eine Konfiguration, ob mit der Erneuerung das zu erneuernde Endteilnehmer-Zertifikat automatisch gesperrt wird oder nicht. Damit kann der Endteilnehmer für eine Übergangsfrist (Erneuerungszeitraum bis Ablauf des Zertifikats) über zwei gültige Zertifikate verfügen. Es obliegt dem Mandanten oder autorisierten Person (Registrator, Benutzer) das zu erneuernde Zertifikat anschließend zu sperren (Kapitel 4.9.3.2 ff).

Sofern eine Schlüsselsicherung (Key-Back-Up, siehe auch Kapitel 1.3.2.2.2) definiert ist, sollte an Stelle der Zertifikatserneuerung eine Zertifikatsneuausstellung durch den zuständigen Sub-Registrator erfolgen.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

Die Schlüsselerneuerung von Zertifikaten stellt eine weitere Antragsform zur Ausstellung eines neuen Zertifikats unter Verwendung eines neuen Schlüsselpaares dar. Zertifikatsinhalt und Identifikationsdaten bleiben unverändert.

Ob eine Schlüsselerneuerung unterstützt wird, hängt von den technischen Vorgaben der Anwendung ab (z.B. Web-Server) ab und obliegt der Verantwortung des Kunden.

4.7.1 Umstände für eine Schlüsselerneuerung

Zur Erhöhung des Sicherheitsniveaus ist eine Schlüsselerneuerung sinnvoll. Die Maßnahme liegt im Ermessen des Mandanten.

Die Zertifikatserneuerung mit Schlüsselerneuerung kann nur im Zeitraum 30 Kalendertage vor Ablauf des Zertifikats und ausschließlich vom autorisierten Kunden durchgeführt werden. Das zu verlängernde Zertifikat darf nicht gesperrt und nicht ungültig/abgelaufen sein.

4.7.2 Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beauftragen?

Es gelten die Regelungen gemäß Kapitel 4.6.2.

4.7.3 Bearbeitung von Schlüsselerneuerungsanträgen

Bei Zertifikaten für Benutzer, Master- und Sub-Registratoren, die den Vorgaben aus Kapitel 4.7.1 entsprechen, erfolgt eine direkte Ausstellung nach Erneuerung. Eine Erneuerung ist so lange möglich, bis sich die Zertifikatsdaten des Antragstellers sich ändern (Kapitel 4.8 ff), ein Sperrgrund eintritt oder eine Zertifikatsnutzung (Kapitel 4.9 ff) nicht mehr gewünscht ist.

Für andere Zertifikatstypen (Server, Router, Mail-Gateway, Domain-Controller) erfolgt die Bearbeitung der Zertifikatserneuerung (Schlüsselerneuerung) durch den zuständigen Sub-Registrator (Kapitel 4.2.2.2 und 4.3).

4.7.4 Benachrichtigung des Zertifikatsinhabers über die Ausstellung mit neuem Schlüsselmaterial

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.7.5 Annahme einer Zertifikatserneuerung mit neuem Schlüsselmaterial

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.7.6 Veröffentlichung eines Zertifikats mit neuem Schlüsselmaterial durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.7.7 Benachrichtigung weiterer Stellen über eine Zertifikaterstellung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Zertifikatsänderung

Das Ausstellen eines neuen Zertifikats ist zwingend erforderlich, wenn sich die Zertifikatsinhalte (mit Ausnahme des öffentlichen Schlüssels) gegenüber dem bisherigen ausgestellten Zertifikat ändern bzw. geändert haben (z.B. C, O, OU1, OU2, OU3, CN, E-Mail, siehe auch Kapitel 3.1.1.1.1 bis 3.1.1.1.10).

4.8.2 Wer darf eine Zertifikatsänderung beauftragen?

Es gelten die Regelungen gemäß Kapitel 4.6.2.

4.8.3 Bearbeitung von Zertifikatsänderungen

Wenn sich Zertifikatsinhalte ändern (siehe Kapitel 3.1 ff), ist eine erneute Authentifizierung wie im Falle der Erst-Beauftragung erforderlich (siehe Kapitel 3.2.3.3 bis 3.2.3.5). Das vorhergehende Zertifikat ist umgehend zu sperren.

4.8.4 Benachrichtigung des Zertifikatsinhabers über die Ausstellung eines Zertifikats

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.8.5 Annahme einer Zertifikatserneuerung mit geänderten Zertifikatsdaten

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.8.6 Veröffentlichung eines Zertifikats mit geänderten Daten durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.8.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserstellung durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Umstände für eine Sperrung

4.9.1.1 Gründe für eine Sperrung eines Endteilnehmer- und Registrator-Zertifikats

Die folgenden Gründe erfordern die Zertifikatssperrung durch den Zertifikatsnehmer oder die Zertifizierungsstelle:

- Die Zertifizierungsstelle erhält angemessene Beweise dafür, dass der private Schlüssel kompromittiert, verloren, gestohlen oder offengelegt wurde (dies gilt nicht im Zusammenhang mit einer Schlüsselsicherung) oder es besteht ein dringender Verdacht, dass dies geschehen ist.
- Die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr aktuell, ungültig, falsch oder entsprechen nicht den Bestimmungen der Namensgebung (siehe Kapitel 3.1 ff). Dies gilt auch für Domänennamen, die nicht mehr im Besitz des Domäneninhabers sind oder die von befugten Instanzen (z.B. ICANN) zurückgezogen wurden (z.B. generische Top-Level-Domains (gTLD).
- Die vormals interne Top-Level-Domain wird zu einer öffentlichen Top-Level-Domain (Kollision der Domänennamen).
- Der zertifizierte Schlüssel (öffentliche Schlüssel) oder die damit verwendeten kryptografischen Algorithmen und Parameter entsprechen nicht mehr den aktuellen Anforderungen.
- Es liegt ein Missbrauch oder Missbrauchsverdacht durch zur Nutzung des Schlüssels berechtigte Personen vor.
- Verwendung und Handhabung des Zertifikats steht im Widerspruch zu vertraglichen Regelungen oder dieser CPS (insbesondere Kapitel 1.4.2).
- Das Zertifikat wurde nicht gemäß dieser CPS ausgestellt.
- Das Zertifikat wurde unter Verstoß gegen die aktuelle Version dieser CPS ausgestellt.
- Die Zertifizierungsstelle erhält angemessene Nachweise dafür, dass das Zertifikat für einen Zweck verwendet wurde, der außerhalb des im Zertifikat oder in der Leistungs- und Nutzungsbedingungen der der Zertifizierungsstelle angegebenen Zwecks liegt.
- Die Zertifizierungsstelle erhält eine Benachrichtigung oder wird auf andere Weise darauf aufmerksam, dass ein Zertifikatsnehmer eine oder mehrere seiner wesentlichen Verpflichtungen aus dem Abonnentenvertrag verletzt hat.
- Sperrung des zu erneuernden Zertifikats nach dem Zertifikatserneuerungsprozess.
- Bei Vertragsbeendigung bzw. -kündigung zwischen dem Mandanten und Endteilnehmer, sofern nichts anderes vereinbart ist.
- Gesetzliche Vorschriften oder richterliche Urteile.
- Das Zertifikat wird nicht mehr benötigt bzw. der Zertifikatnehmer verlangt ausdrücklich die Sperrung des Zertifikats.

Die Zertifizierungsstelle sperrt Endteilnehmer- und Registrator-Zertifikate innerhalb von 24 Stunden, wenn mindestens einer der Gründe vorliegt:

- Der Zertifikatnehmer, Schlüsselbeauftragte oder eine sonstige verantwortliche Person reicht den Auftrag zur Sperrung schriftlich ein.
- Der Auftraggeber oder eine verantwortliche Kontaktperson informiert darüber, dass der zugrundeliegende Zertifikatsrequest nicht autorisiert war und die Autorisierung auch nachträglich nicht gegeben wird.
- Der Zertifizierungsstelle liegen Beweise vor, dass der private Schlüssel des Zertifikatsnehmers kompromittiert wurde.
- Die Zertifizierungsstelle erlangt Kenntnis darüber, die Validierung der Domänenautorisierung oder -kontrolle für einen vollständig qualifizierten Domänennamen oder eine IP-Adresse im Zertifikat nicht verlässlich sein sollte.

Die Zertifizierungsstelle sperrt Endteilnehmer- und Registrator-Zertifikate innerhalb von 5 Tagen, wenn mindestens einer der folgenden Gründe vorliegt:

- Das Zertifikat entspricht nicht mehr den Anforderungen in Kapitel 6.1.5 oder 6.1.6.
- Der Zertifizierungsstelle liegen Beweise vor, dass das Zertifikat missbräuchlich eingesetzt wurde,
- Die Zertifizierungsstelle erlangt Kenntnis von einer oder mehreren schwerwiegenden Vertragsverletzungen des Zertifikatsnehmers.
- Die Zertifizierungsstelle erlangt Kenntnis darüber, dass das Nutzungsrecht für einen FQDN oder eine IP-Adresse erloschen ist. (Z.B. ein Gericht untersagt die Nutzung, eine Vollmacht läuft aus usw.)
- Die Zertifizierungsstelle erlangt Kenntnis, dass ein Wildcard-Zertifikat für die Authentisierung eines missverständlichen untergeordneten FQDN, der betrügerisch verwendet wird.
- Die Zertifizierungsstelle erlangt Kenntnis von einer relevanten Änderung in den Zertifikatseinträgen.
- Die Zertifizierungsstelle erhält Kenntnis davon, dass das Zertifikat nicht regelkonform herausgegeben wurde, wie es in den Anforderungen des CA-Browserforums oder der anzuwendenden CP oder CPS beschrieben ist.
- Die Zertifizierungsstelle stellt fest, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist.
- Die Zertifizierungsstelle stellt den Betrieb ein und hat keine Regelungen getroffen, dass im Falle einer Betriebseinstellung der Sperrsupport durch eine andere CA weitergeführt wird.
- Der Nachweis der CA-Browserforum-Konformität der CA hat seine Gültigkeit verloren. Ein Sperrgebot gilt nicht, wenn die Zertifizierungsstelle Vorsorge getroffen hat, dass die CRL und der OCSP-Dienst weiter gepflegt und bereitgestellt werden.
- Die CA erlangt Kenntnis von einer möglichen Kompromittierung des privaten Schlüssels einer Sub-CA, der zur Zertifikatsausstellung genutzt wird (es werden alle von dieser Sub-CA ausgestellten Zertifikate gesperrt).
- Die CP und/oder CPS der herausgebenden Zertifizierungsstelle sieht eine Sperrung vor.
- Die Inhalte oder das Format des Zertifikats stellt aus technischer Sicht ein inakzeptables Risiko für Anwendungssoftware-Hersteller oder vertrauende Dritte dar, z.B. wenn das CA-Browserforum ein solches Risiko aufzeigt und deshalb das Zertifikat gesperrt und ersetzt werden sollte.
- Die Zertifizierungsstelle erlangt Kenntnis davon, dass es eine Methode gibt, mit der der man den zu einem öffentlichen Schlüssel korrespondierenden privaten Schlüssel einfach berechnen kann. (vergleichbar mit der Debian-Schwäche (Debian weak key, http://wiki.debian.org).
- Gesetzliche Vorschriften oder richterliche Urteile oder eine Weisung einer aufsichtsführenden Behörde liegt vor.

Die Zertifizierungsstelle sperrt Endteilnehmer- und Registrator-Zertifikate innerhalb von 120 Tagen,

- wenn das Zertifikat einen Domainnamen mit einer gTLD enthält, der von befugten Instanzen (z.B. ICANN) zurückgezogen wurde.

4.9.1.2 Gründe für die Sperrung eines Sub-CA-Zertifikats

Das Telekom Security Trust Center sperrt ein Sub-CA-Zertifikat innerhalb von 7 Tagen, wenn mindestens einer der folgenden Gründe vorliegt:

- Die Sub-CA beantragt den Widerruf in schriftlicher Form.
- Die Sub-CA benachrichtigt die ausstellende Zertifizierungsstelle (Root-CA), dass die ursprüngliche Zertifikatsantrag nicht autorisiert wurde und auch keine rückwirkende Autorisierung erteilt wird.

- Die ausstellende Zertifizierungsstelle erhält den Nachweis, dass der private Schlüssel der Sub-CA, der dem öffentlichen Schlüssel im Zertifikat entspricht, kompromittiert wurde oder nicht mehr den Anforderungen der Abschnitte 6.1.5 und 6.1.6 entspricht.
- Die ausstellende Zertifizierungsstelle erhält den Nachweis, dass das Sub-CA-Zertifikat missbräuchlich verwendet wurde.
- Der ausstellenden Zertifizierungsstelle wird mitgeteilt, dass das Sub-CA-Zertifikat nicht in Übereinstimmung mit diesem Dokument oder den geltenden Zertifikatsrichtlinien oder der Erklärung zum Zertifizierungsbetrieb ausgestellt wurde oder dass die untergeordnete Zertifizierungsstelle dieses Dokument nicht eingehalten hat.
- Die ausstellende Zertifizierungsstelle stellt fest, dass alle im Zertifikat enthaltenen Informationen ungenau oder irreführend sind.
- Die ausstellende Zertifizierungsstelle oder die Sub-CA stellt den Betrieb aus irgendeinem Grund ein und hat keine Vorkehrungen getroffen, damit eine andere Zertifizierungsstelle das Sub-CA-Zertifikat sperren kann.
- Das Recht der ausstellenden Zertifizierungsstelle oder der Sub-CA, Zertifikate gemäß diesen Anforderungen auszustellen, erlischt oder wird widerrufen oder beendet, es sei denn, die Sub-CA hat Vorkehrungen getroffen, um das CRL / OCSP-Repository weiter zu pflegen.
- Die Sperrung ist gemäß den Zertifikatsrichtlinien und / oder der Erklärung zur Zertifizierungsbetrieb der Sub-CA erforderlich, oder
- Der technische Inhalt oder das Format des Zertifikats stellt ein inakzeptables Risiko für Anbieter von Anwendungssoftware oder vertrauende Parteien dar (z. B. kann das CA/Browser-Forum feststellen, dass ein veralteter Kryptografie- /Signaturalgorithmus oder eine Schlüsselgröße ein inakzeptables Risiko darstellt und dass solche Zertifikate gesperrt werden sollten und innerhalb eines bestimmten Zeitraums durch Zertifizierungsstellen ersetzt werden).
- Die Sub-CA sollte ein Zertifikat nach der Bewertung oder einer Frist sperren, wenn eine oder mehrere der folgenden Situationen eintreten.

Die Sub-CA sollte ein Zertifikat nach der Bewertung oder einer Frist sperren, wenn eine oder mehrere der folgende Ereignisse eintreten:

- Es gibt gesetzliche Regelungen oder Entscheidungen oder Anweisungen einer Aufsichtsbehörde.

4.9.2 Wer kann eine Sperrung beauftragen?

Die folgenden Personen sind in der Regel berechtigt, die Sperrung eines Endteilnehmer- oder Registrator-Zertifikates zu initiieren:

- Autorisierte Personen einer externen Registrierungsstelle (Master-Registratoren, Kapitel 1.3.2.2.1),
- Autorisierte Personen einer externen Registrierungsstelle (Sub-Registratoren und deren Derivate, Kapitel 1.3.2.2.2),
- Autorisierte Personen, die als Subjekt im Zertifikat aufgeführt sind,
- Autorisierte Personen von Personen- und Funktionsgruppen und Geräten,
- Autorisierte Personen die als Schlüsselverantwortliche oder Sperrberechtigte auftreten,
- Autorisierte Personen der internen Registrierungsstelle der Telekom Security im Rahmen der Einrichtung und Verwaltung einer Master-Domäne (Kapitel 3.2.2 ff),
- Autorisierte Personen der internen Registrierungsstelle der Telekom Security, wenn die Telekom Security über das Vorliegen eines der in Kapitel 4.9.1 genannten Sperrgründe in Kenntnis gesetzt wird.

Die folgenden Personen sind in der Regel berechtigt, die Sperrung eines Sub-CA-Zertifikates zu initiieren:

- Autorisierte Person(en) des PKI-Service TeleSec Shared-Business-CA (z.B. Change Advisory Board der Telekom Security).

4.9.3 Ablauf einer Sperrung

4.9.3.1 Sperrvarianten

Je nach Rolle und Berechtigung stehen den Teilnehmern dieser PKI (Kapitel 1.3.2 ff, 1.3.3, 1.3.4 und 1.3.5) unterschiedliche Sperrvarianten 7x24h zur Verfügung. Zertifikatssperrungen sind möglich über

- die Benutzer-Webseite für alle Benutzer (außer Master- und Sub-RA und deren Derivate (Kapitel 1.3.2.2.2),
- die Sub-RA-Webseite für alle Benutzer und Geräte (außer Master und Sub-RA und deren Derivate),
- die Master-RA-Webseite für alle Benutzer, Geräte und Sub-Registratoren (inkl. Derivate, außer Master-RA),
- die Sperrservice-Webseite des Telekom Security Service Desk nur für Master-RA, und
- optional: CMP-Schnittstelle.

Tabelle 16 bis Tabelle 19 stellt die Sperrvarianten in Abhängigkeit zu den Zertifikatstypen (Kapitel 1.3.2.2 ff und 1.3.3) dar.

Tabelle 16: Sperrvarianten Master-Registrator-Zertifikat

Zertifikatstyp:	Master-Registrator-Zertifikat
Sperrung über:	Sperrservice-Webseite des Service Desk

Tabelle 17: Sperrvarianten Sub-Registrator-Zertifikat und Derivate

Zertifikatstyp:	Sub-Registrator-Zertifikat und Derivate
Sperrung über:	Master-Registrator-Webseite

Tabelle 18: Sperrvarianten Benutzer-Zertifikate

Zertifikatstyp:	Benutzer-Zertifikate
Sperrung über:	Sub-Registrator-Webseite, Master-Registrator-Webseite, Benutzer-Webseite, CMP-Schnittstelle

Tabelle 19: Sperrvarianten Geräte-Zertifikate

Zertifikatstyp:	Geräte-Zertifikate (z.B. Server, Router/Gateway)
Sperrung über:	Sub-Registrator-Webseite, Master-Registrator-Webseite, CMP-Schnittstelle

Unabhängig von o.g. Sperrvarianten behält sich das Trust Center der Telekom Security vor, Zertifikate bei Vorliegen von mindestens einem, der in Kapitel 4.9.1.1 aufgeführten Sperrgründe, zu sperren.

4.9.3.2 Sperrung von Endteilnehmer-Zertifikaten

Eine Zertifikatssperrung kann 7x24h durch eine in Kapitel 4.9.2 aufgeführte Sperrvariante initiiert werden. Dabei reicht das Vorliegen von mindestens einem in Kapitel 4.9.1.1 aufgeführten Sperrgrund.

In jedem Fall sind Inhalte des Subject-DN des Zertifikatsinhabers (z.B. Common Name) erforderlich, um das zu sperrende Zertifikat selektieren zu können. Die Authentifizierung der Sperrung erfolgt über das dem Zertifikatsinhaber bekannte Sperrpasswort.

Die Sperrung ist endgültig. Anschließend ist manuell vom Master- oder Sub-Registrator bzw. Sperrservice-Operator eine neue Zertifikatssperrliste (CRL) zu generieren. Andernfalls wird die Sperrung erst mit dem täglichen Zyklus des CA-Systems (Kapitel 4.9.7) in der Zertifikatssperrliste (CRL) veröffentlicht. Nach der Zertifikatssperrung stehen die Sperrinformationen per OCSP unmittelbar zur Verfügung.

Die Zertifizierungsstelle sperrt Zertifikate bei Vorliegen von mindestens einem der in Kapitel 4.9.1.1 aufgeführten Sperrgründe zu sperren.

Telekom Security bietet Endteilnehmern, Vertrauenden Dritten (z.B. Software-Hersteller) und anderen Teilnehmern die Möglichkeit an, verdächtige Schlüsselkompromittierungen, Zertifikatsmissbrauch oder andere zertifikatsbetreffende Betrugsfälle oder -versuche zu melden.

Innerhalb von 24 Stunden nach Eingang eines Missbrauchsverdachts beginnt Telekom Security mit den Nachforschungen, um entscheiden zu können, ob weitere Maßnahmen (z.B. Sperrung) eingeleitet werden. Innerhalb dieser 24 Stunden werden ein erster Bericht des Sachverhalts und der Analyseergebnisse erstellt und dem Zertifikatsinhaber sowie der Person, die das Problem gemeldet hat, als Rückmeldung gegeben. Nach Ansicht der Fakten und Umgebungsparameter wird die Zertifizierungsstelle mit dem Zertifikatsnehmer/Beauftragten oder der meldenden Person die Analyseergebnisse besprechen und entscheiden, inwiefern eine Zertifikatssperrung notwendig wird. In diesem Zusammenhang wird das Datum der Sperrung festgelegt. Der Zeitraum zwischen Erhalt des Zertifikatsproblemreports bzw. Sperrwunsches bis zur veröffentlichten Sperrung darf die in Kapitel 4.9.1.1 geforderten Fristen für eine Sperrung nicht überschreiten.

Das weitere Vorgehen wird anhand folgender Kriterien bestimmt:

- Die Ursache oder Art des Problems (Kontext, Schwere, Auswirkungen, Risiko oder Schaden)
- Die Auswirkungen einer Sperrung (direkte oder gemeinsame Auswirkungen auf Zertifikatsinhaber und vertrauende Dritte)
- Die Anzahl der Meldungen zu diesem Zertifikatsproblem oder von diesem Zertifikatsinhaber
- Die Person, welche die Meldung eingestellt hat (z.B. eine Meldung durch eine Strafverfolgungsbehörde wird mit erhöhter Priorität eingestuft) und
- Die bezugnehmende Gesetzgebung

Telekom Security verfügt bei einer hoch priorisierten Zertifikats-Problemmeldung jederzeit über die Möglichkeit intern zu reagieren und zu entscheiden, ob eine Weiterleitung an eine Strafverfolgungsbehörde erforderlich ist oder ein Zertifikat, das Gegenstand einer solchen Meldung ist, zu sperren.

4.9.3.2.1 Sperrungen von Benutzer-Zertifikaten

Die Sperrung von Benutzer-Zertifikaten erfolgt über folgende Rolleninhaber und Webseiten bzw. Schnittstelle (Kapitel 4.9.3.1):

- Durch den Benutzer über die Benutzer-Webseite.
- Durch den zuständigen Sub-Registrator (oder deren Derivate).
- Durch den zuständigen Master-Registrator über Master-Registrator-Webseite.
- Optional: CMP-Schnittstelle.

4.9.3.2.2 Sperrungen von Geräte-Zertifikaten

Die Sperrung von Geräte-Zertifikaten erfolgt über folgende Rolleninhaber und Webseiten bzw. Schnittstelle (Kapitel 4.9.3.1):

- Durch den Benutzer über die Benutzer-Webseite.
- Durch den zuständigen Sub-Registrator (oder deren Derivate).
- Durch den zuständigen Master-Registrator über Master-Registrator-Webseite.
- Optional: CMP-Schnittstelle.

4.9.3.3 Sperrung von Registrator-Zertifikaten

4.9.3.3.1 Sperrung eines Master-Registrator-Zertifikats

Die Sperrung von Master-Registrator-Zertifikaten erfolgt über folgende Rolleninhaber und Webseiten (Kapitel 4.9.3.1):

- Durch das Telekom Security Service Desk über die Sperrservice Webseite.

4.9.3.3.2 Sperrung eines Sub-Registrator-Zertifikats oder deren Derivate

Die Sperrung von Master-Registrator-Zertifikaten erfolgt über folgende Rolleninhaber und Webseiten (Kapitel 4.9.3.1):

- Durch den zuständigen Master-Registrator über Master-Registrator-Webseite.

4.9.3.4 Sperrung von Zertifikaten zur Unterstützung des PKI-Betriebs

Zur Unterstützung des PKI-Betriebs TeleSec Shared-Business-CA werden die in Kapitel 1.3.1.3.1 und 1.3.1.3.2 beschriebenen Web-Server- und OCSP-Zertifikate eingesetzt.

Aufforderungen für diese Zertifikatssperrungen werden dem Telekom Security Service Desk gemeldet. Die aktuellen Kontaktdaten des Service Desk sind im Dokument „Service Level Agreement“ (SLA) aufgeführt.

4.9.3.4.1 Sperrung von externen Web-Server-Zertifikaten

Telekom Security verpflichtet sich zu einer Sperrung des Web-Server-Zertifikats der SBCA-Webseiten (Kapitel 1.3.1.3.1), sobald der Verdacht einer Schlüsselkompromittierung besteht. Telekom Security behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. Die Sperrung wird über eine Zertifikatssperrliste (CRL) bekannt gegeben. Ein gesperrtes Web-Server-Zertifikat wird unverzüglich durch ein neues ersetzt.

Telekom Security sperrt den Zugang zum Web-Server, wenn dessen Sicherheit durch eine Sperrung dieses Zertifikats gefährdet ist.

4.9.3.4.2 Sperrung des OCSP-Responder-Zertifikats

Telekom Security verpflichtet sich zu einer Sperrung des OCSP-Responder-Zertifikats (Kapitel 7.3 ff), sobald der Verdacht einer Schlüsselkompromittierung besteht. Telekom Security behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. Die Sperrung wird über eine Zertifikatssperrliste (CRL) bekannt gegeben. Ein gesperrtes OCSP-Zertifikat wird unverzüglich durch ein Neues ersetzt.

4.9.3.5 Sperrung von Sub-CA-Zertifikaten

Telekom Security verpflichtet sich zu einer Sperrung des Sub-CA-Zertifikats (Kapitel 1.3.1.2 ff), sobald der Verdacht einer Schlüsselkompromittierung besteht oder Vorgaben dies erfordern.

Es besteht ein interner Geschäftsprozess der Telekom Security zur Sperrung von Sub-CA-Zertifikaten.

4.9.4 Fristen für einen Sperrauftrag

4.9.4.1 Service Desk der Telekom Security

Nach Eingang eines vollständigen Sperrauftrags (nur Master-Registrator-Zertifikate oder bei Zertifikats-Missbrauchsfällen) beim Telekom Security Service Desk sperrt Telekom Security das Endteilnehmer- und Registrator-Zertifikate innerhalb von 24 Stunden und veröffentlicht diese in der Zertifikatssperrliste (CRL) und OCSP-Datenbank.

4.9.4.2 Externe Registrierungsstelle

Die Einhaltung von Fristen für Sperraufträgen liegt in der Verantwortung der beauftragten Drittpartei (Delegated Third Party). Sobald für Endteilnehmer-Zertifikate ein Sperrgrund gemäß Kapitel 4.9.1.1 vorliegt, muss der Sperrauftrag so schnell als möglich innerhalb einer wirtschaftlich angemessenen Frist vom Endteilnehmer, Schlüsselverantwortlichen oder Sperrberechtigten gestellt werden.

4.9.5 Bearbeitungsfristen der Zertifizierungsstelle für Sperranträge

Die Sperrung durch den Endteilnehmer, Registrator, Schlüsselverantwortlichen, Sperrberechtigten des Service Desk der Telekom Security über die jeweiligen Webseiten steht 7x24h zur Verfügung und wird unmittelbar nach dem Sperrvorgang an die angeschlossenen Systeme weitergegeben. Der OCSP-Dienst, der auf diese Systeme zugreift, verfügt damit über den aktuellen Zertifikatsstatus.

4.9.6 Überprüfungsvorgaben für Vertrauende Dritter

Vertrauende Dritte müssen die Möglichkeiten erhalten, den Status von Zertifikaten überprüfen zu können. Zu diesem Zweck kann der OCSP-Responder genutzt werden, der den aktuellen Status eines Endteilnehmer-, Registrator- oder OCSP-Responder-Zertifikat übermittelt.

Eine weitere Methode, wie ein Vertrauender Dritter überprüfen kann, ob ein Zertifikat gesperrt ist, ist die Prüfung der aktuellen Zertifikatssperrliste (CRL), die auf dem Verzeichnisdienst der SBCA veröffentlicht wird.

Gesperrte CA-Zertifikate (außer Root-CA-Zertifikate) werden in der standardisierten Zertifikatssperrliste (CARL) veröffentlicht und können daher mit Standard-konformen Anwendungen geprüft werden.

Telekom Security stellt sicher, dass das gesperrte Zertifikat auch nach dessen Ablauf mindestens in der nächsten CRL enthalten ist.

4.9.7 Veröffentlichungsfrequenz von Sperrinformationen

Die Zertifikatssperrliste (CRL) als auch Zertifizierungsstellen-Sperrliste (CARL) wird, wie im Kapitel 2.3 beschrieben, über den Verzeichnisdienst publiziert.

Die Zertifikatssperrliste (CRL), in der Zertifikats-Sperrungen von Endteilnehmern aufgeführt sind, wird mindestens einmal pro Tag automatisch vom CA-System aktualisiert und über den Verzeichnisdienst veröffentlicht. Innerhalb dieses automatischen Zyklus kann der Mandant/externe Registrierungsstelle durch die Rolleninhaber Master- und Sub-Registrator die Zertifikatssperrliste (CRL) manuell generieren.

In den Sperrlisten für Zertifizierungsstellen (CARL) werden alle gesperrten CA-Zertifikate (keine Root-CA-Zertifikate) veröffentlicht, die von der jeweiligen Stammzertifizierungsstelle (Root-CA) ausgestellt wird. In Abbildung 1 sind die jeweiligen Stamm- und untergeordneten Zertifizierungsstellen (Sub-CA) grafisch dargestellt. Die Aktualisierung aller CARLs erfolgt innerhalb von drei (3) Monaten oder ereignisbezogen innerhalb von 24 Stunden nach Widerruf eines untergeordneten CA-Zertifikats.

4.9.8 Maximale Latenzzeit von Sperrlisten

Die Latenzzeit der Zertifikatssperrliste (CRL) nach automatischer Generierung beträgt wenige Minuten.

Die Latenzzeit für Zertifizierungsstellen-Sperrliste (CARL) nach manueller Veröffentlichung beträgt wenige Minuten.

4.9.9 Online-Verfügbarkeit von Sperr-/Statusinformationen

Zusätzlich, zu den Sperrinformationen über CRL und CARL (Kapitel 2.3, 4.9.7), stellt Telekom Security Online-Informationen zum Zertifikatsstatus via OCSP bereit. Die URL des OCSP-Responders ist im Zertifikat in der Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)“ (siehe Kapitel 7.1.2.9) aufgeführt. Die von SBCA ausgegebenen OCSP-Antworten von Endteilnehmer-Zertifikaten entsprechen den Vorgaben des RFC6960.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

Vertrauende Dritte müssen den Status eines Zertifikats überprüfen, dem sie vertrauen möchten. Für den Abruf aktueller Statusinformationen steht der OCSP-Dienst (OCSP-Responder) zur Verfügung. Eine weitere Möglichkeit der Statusabfrage liefert die aktuelle Zertifikatssperrliste (CRL).

Der OSCP-Responder unterstützt die GET-Methode.

Die OCSP-Datenquelle (repository) für Endteilnehmer-Zertifikate wird spätestens nach zehn (10) Minuten aktualisiert. Die OCSP-Antworten haben eine maximale Gültigkeit von fünf (5) Tagen.

Die OCSP-Datenquelle (repository) für Sub-CA-Zertifikate wird spätestens nach sechs (6) Monaten aktualisiert. Nach der Sperrung eines CA-Zertifikats erfolgt die Aktualisierung innerhalb von vierundzwanzig (24) Stunden.

Der OCSP-Responder antwortet auf Anfragen von Zertifikats-Seriennummern mit „unknown“, wenn diese nicht dem PKI-Service „TeleSec Shared-Business-CA” zugeordnet werden können.

Der TSP überwacht den OCSP-Responder im Rahmen seiner Sicherheitsverantwortung auf Anfragen nach "nicht verwendeten" Seriennummern.

4.9.11 Andere verfügbare Formen der Veröffentlichung von Sperrinformationen

Abhängig vom Zertifikatstyp wird der Zertifikatsnehmer, Antragsteller, Vertreter oder weitere Instanz über die Sperrung des Zertifikats per E-Mail benachrichtigt (revoke notification), in der die relevanten Zertifikats-Informationen enthalten sind.

4.9.12 Besondere Anforderungen bezüglich der Kompromittierung privater Schlüssel

Dritte, die eine Schlüsselkompromittierung melden wollen, werden gebeten, die in Abschnitt 1.5.2 beschriebenen Kontaktmöglichkeiten zu nutzen. Es müssen ausreichende Informationen oder Verweise auf Informationen angegeben werden, die das Vorliegen einer Schlüsselkompromittierung beweisen, z. B. ein mit dem kompromittierten privaten Schlüssel signierter CSR mit commonName "Compromised Key". Das betroffene Zertifikat selbst sollte ebenfalls referenziert werden.

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu sperren (Kapitel 4.9.1.1).

4.9.13 Umstände einer Suspendierung

Die Suspendierung (temporäre Sperrung) von Zertifikaten wird nicht unterstützt.

4.9.14 Wer kann eine Suspendierung beantragen?

Nicht anwendbar.

4.9.15 Verfahren der Suspendierung

Nicht anwendbar.

4.9.16 Beschränkung des Suspendierungszeitraums

Nicht anwendbar.

4.10 Statusauskunftsdienste von Zertifikaten

Der Status von Endteilnehmer- und Registrator-Zertifikaten ist ermittelbar via OCSP-Dienst (Kapitel 2.1 und 2.2) und per Zertifikatssperrliste (CRL).

4.10.1 Betriebseigenschaften

Die OCSP-Antworten werden von einem OCSP-Responder signiert, dessen Zertifikat seinerseits von der Zwischenzertifizierungsstelle (Sub-CA) signiert wurde, welche das betreffende Endteilnehmer-Zertifikat ausgestellt hat. In Abbildung 1 sind die jeweiligen Zuordnungen der Endteilnehmer zu den ausstellenden Stamm- und untergeordneten Zertifizierungsstellen (Sub-CA) grafisch dargestellt.

Die OCSP-Antwort enthält einen der folgenden Stati:

- gut (good) bedeutet:
  - es ist ein Aussteller (Issuer) des PKI-Services und
  - das Zertifikat ist gültig (innerhalb der Zertifikatslaufzeit) und
  - das Zertifikat ist nicht gesperrt.
- gesperrt (revoked) bedeutet:
  - es ist ein Aussteller (Issuer) des PKI-Services und
  - das Zertifikat ist gültig (innerhalb der Zertifikatslaufzeit) und
  - das Zertifikat wurde gesperrt.
- unbekannt (unknown) bedeutet:
  - das Zertifikat ist ungültig (außerhalb der Zertifikatslaufzeit) oder
  - das Zertifikat ist gültig, wurde aber nicht von dem angefragten Aussteller (Issuer) des PKI-Services ausgestellt oder

- das Zertifikat ist gültig, wurde aber nicht von dem Aussteller (Issuer) des PKI-Services ausgestellt.

Das Zertifikat des OCSP-Responders enthält die in Kapitel 7.3.2 beschriebene Erweiterung.

Die von SBCA ausgegebene Zertifikatssperrliste (CRL) entspricht den Vorgaben des RFC5280. Die Zertifikatssperrlisten (CRL) werden von der jeweiligen Sub-CA, die Sperrlisten für Zertifizierungsstellen (CARL) werden von der jeweiligen Root-CA ausgestellt, signiert und auf dem LDAP-Verzeichnisdienst veröffentlicht. In Abbildung 1 sind die jeweiligen Zuordnungen der ausstellenden Stamm- und untergeordneten Zertifizierungsstellen (Sub-CA) grafisch dargestellt.

Telekom Security hat Mechanismen zum Schutz des Sperrstatus-Dienstes (CRL, CARL, OCSP) gegen unbefugte Versuche implementiert, um Manipulationen an Sperrstatusinformationen (hinzufügen, löschen, ändern) zu verhindern.

Der TSP bietet kein OCSP-Stapling an.

4.10.2 Verfügbarkeit des Dienstes

Es sind Maßnahmen getroffen, die in der Regel einen Betrieb des OCSP-Dienstes oder der CLR/CARL ohne Downtime für 7x24 h gewährleisten (Redundanzen, Caching). In Notfallszenarien sind Downtimes von bis zu einem Tag möglich.

Die Antwortzeit des OCSP-Responders und LDAP-Verzeichnisdienst beträgt unter normalen Betriebsbedingungen weniger als 10 Sekunden.

4.10.3 Optionale Funktionen

Nicht anwendbar.

4.11 Beendigung des Vertragsverhältnisses

Im Falle einer Vertragskündigung durch den Mandanten oder der Telekom Security erfolgt zunächst unmittelbar die Deaktivierung der zur Verfügung gestellten Zertifikatstypen. Dies hat zur Folge, dass eine Neubeantragung als auch Erneuerung von Endteilnehmer-Zertifikaten nicht mehr möglich ist. Eine Anmeldung an der Webseite, um bestehende Zertifikate sperren zu können, besteht weiterhin. Mit der Deaktivierung der Master-Domäne werden sämtliche Funktionen zur Anmeldung an der jeweiligen Webseite, Neuausstellung, Erneuerung und Sperrung von Zertifikaten unterbunden; eine Zertifikats-Validierung über die Zertifikatssperrliste und OCSP wird aber weiterhin unterstützt.

Zertifikate, die nach dem Tarifmodell Classic und Classic Pro entgeltpflichtig wurden, behalten ihre Gültigkeit bis Ablauf des Zertifikats, eine Erneuerung ist nicht möglich.

Zertifikate, die nach dem Tarifmodell Advanced entgeltpflichtig wurden, werden nach dem Kündigungsdatum gesperrt und verlieren die Gültigkeit. Einzelvertraglich kann eine gesonderte Übergangsregelung getroffen werden.

Bei einer ordentlichen Vertragskündigung muss der Kunde seinen Archivierungsverpflichtung nachkommen (Kapitel 5.5 ff). Auf Anfrage des TSP muss der Kunde Zugriffsrechte auf diese Daten unentgeltlich einräumen.

Im Falle einer Zahlungsunfähigkeit (Insolvenz) muss der Kunde rechtzeitig den TSP informieren und unmittelbar Zugriffsrechte auf diese Daten unentgeltlich einräumen.

4.12 Schlüsselhinterlegung und Wiederherstellung

Die im Rahmen des PKI-Service „TeleSec Shared-Business-CA“ verwendeten Schlüsselpaare der untergeordneten Zertifizierungsstellen (Sub-CA) (siehe Abbildung 1) werden auf einem

sicherheitsüberprüften Hardware Security Module (HSM) gespeichert und in sicherer Umgebung betrieben. Die Speicherung des Schlüsselmaterials auf weiteren HSMs erfolgt ausschließlich zur Schlüsselsicherung (Key-Back-Up) und dient zur Wiederherstellung und Aufrechterhaltung des Dienstes durch qualifiziertes und sicherheitsgeprüftes Personal (Trusted Role) des Trust Centers. Eine Schlüsselhinterlegung (Escrow) bei Dritten (z.B. Treuhänder, Notar) ist nicht vorgesehen.

4.12.1 Richtlinien für Schlüsselhinterlegung und –wiederherstellung

Nicht anwendbar.

4.12.2 Sitzungsschlüsselkapselung und Richtlinien für die Wiederherstellung

Nicht anwendbar.

5 GEBÄUDE-, VERWALTUNGS- UND BETRIEBSKONTROLLEN

Das Telekom Security Trust Center ist in einem speziell geschützten Gebäude untergebracht und wird von fachkundigem Personal betrieben. Alle Prozesse für die Generierung und Verwaltung von Zertifikaten der dort betriebenen Zertifizierungsstellen sind genau definiert. Alle technischen Sicherheitsmaßnahmen sind dokumentiert.

Die folgenden Aussagen gelten für die vom Telekom Security Trust Center betriebenen Zertifizierungsstellen.

Die angewendeten physikalischen, organisatorischen und personellen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept [SBCA Siko] festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen.

Die für den operativen Betrieb notwendigen Sicherheitsmaßnahmen sind in dem Service- und Organisations-Handbuch, Systems-Handbuch sowie den Betriebsleitfaden des Trust Centers beschrieben.

Die Anforderungen aus [ETSI EN TSP] Kapitel 5, 6.3 und 7.3 sind umgesetzt, d.h. es sind Festlegungen

- zur Risikobewertung im Rahmen des ISMS,
- zu den Richtlinien zur Informationssicherheit,
- zum Asset-Management

beschrieben.

Das Management genehmigt die Risikobewertung und akzeptiert das identifizierte Restrisiko.

5.1 Physikalische Kontrollen

5.1.1 Standort und bauliche Maßnahmen

Der Betrieb von Telekom Security-eigenen Services (Diensten) erfolgt in Rechenzentren, die den Konzernvorgaben hinsichtlich technischer und physikalischer Sicherheit entsprechen.

Das Trust Center der Telekom Security befindet sich in Rechenzentren, deren Lokalitäten sich an zwei georedundanten Standorten in Deutschland befinden und mit einem Mindestabstand von größer 10 km einander getrennt sind.

Das Trust Center der Telekom Security ist im jeweiligen Rechenzentrum in einem separaten Bereich (Cage) aufgebaut und mittels Zutrittskontrollanlage abgesichert.

Die Errichtung und der Betrieb des Trust Centers bzw. Rechenzentrums erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Verbandes der Schadenversicherer e.V. (VdS) / neu: Gesamtverband der Deutschen Versicherungswirtschaft (GDV), der einschlägigen DIN-Normen zu Brandschutz, Rauchschutz und Angriffshemmung. Das Trust Center ist sicherheitstechnisch vom VdS / GDV abgenommen.

Die technischen Maßnahmen werden durch organisatorische Elemente ergänzt, die die Handhabung der sicherheitsrelevanten Techniken und Regelungen über den Zutritt zu Sicherheitszonen für Mitarbeiter und Dritte (Besucher, Fremd- und Reinigungspersonal), die Anlieferung von Material (Hardware, Zubehör, Betriebsmittel) und Ordnung am Arbeitsplatz sowie in Rechnerräumen beinhalten.

5.1.2 Räumlicher Zutritt

Im Trust Center gilt eine Zutrittsregelung die die Zutrittsrechte für Mitarbeiter, Mitarbeiter von Fremdfirmen und Gästen in den einzelnen Sicherheitszonen regelt. Der Zutritt ist zwischen den Sicherheitsbereichen nur über Personenvereinzelungsanlagen möglich. Der kontrollierte Zutritt zu den verschiedenen Sicherheitsbereichen ist weiter mit einem rechnergesteuerten Zutrittskontrollsystem geschützt. Gäste werden nur in Ausnahmefälle und nach vorheriger Anmeldung empfangen. Hier gelten besondere Sicherheitsvorschriften.

5.1.3 Stromversorgung und Klimatisierung

Die Ansaugöffnungen für die Außenluft sind so angeordnet, dass keine Schadstoffe wie Staub und Schmutz, ätzende, giftige oder leicht brennbare Gase eindringen können. Die Systeme werden mit einem sehr geringen Außenluftanteil betrieben. Die erforderlichen Zuluftöffnungen sind zugangsgeschützt. Zum Schutz gegen Luftverunreinigung durch schwebende Partikel sind Filter installiert. Die Frischluftansaugung wird ständig auf aggressive Gase überwacht. Im Notfall (z.B. Brand in der Umgebung) wird die Außenluftansaugung automatisch durch Luftklappen verschlossen.

Zum Ausfallschutz der Energieversorgung ist eine unabhängige Wechselspannungsversorgung entsprechend VDE-Vorschriften installiert. Sie bietet Schutz gegen Spannungsschwankungen, unterbrechungsfreie Kurzzeitüberbrückung, eine Langzeitüberbrückung mit zwei getrennten, ortsfesten Notstromaggregaten mit einer Leistung, die der Volllast des Rechenzentrums entspricht.

5.1.4 Wassergefährdung

Das Trust Centers liegt in einer geschützten Lage, d.h. es liegt nicht in der Nähe von Gewässern und Niederungen (Hochwassergefahr).

5.1.5 Brandschutz

Die geltenden Brandschutzbestimmungen (z.B. DIN 4102, Auflagen der örtlichen Feuerwehr, Vorschriften über Feuerresistenz, VDE-gerechte Elektroinstallation) werden eingehalten. Alle Brandschutztüren besitzen automatische Schließeinrichtungen. In Absprache mit der Feuerwehr wird nur in äußersten Notfällen mit Wasser gelöscht.

Brandabschnitte sind durch feuerbeständige Bauteile gesichert. Durchgänge durch Brandschutzwände sind mit selbsttätig schließenden Brandschutztüren ausgestattet.

In Bereichen mit Doppelböden sowie abgehängten Decken sind Brandschutzwände durchgehend bis zum Geschoßboden bzw. zur Geschoßdecke ausgeführt.

In alle Systemräume, Systemoperatorräume, Archivräume, USV-Räume, sowie weitere ausgewählte Räume, sind Brandfrühesterkennungssysteme (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut. Die Brandbekämpfung erfolgt mit inertem Gas.

5.1.6 Aufbewahrung von Datenträgern

Alle Datenträger, die Produktions-Software und -daten, Audit-, Archiv- oder Sicherungs-Informationen enthalten, werden in Räumen gelagert, die mit den entsprechenden physischen und logischen Zutrittskontrollen versehen sind und Schutz vor Unfallschäden (z.B. Wasser-, Brand- und elektromagnetische Schäden) bieten.

5.1.7 Entsorgung

Vertrauliche Dokumente und Materialien werden vor ihrer Entsorgung physisch zerstört. Datenträger, die vertraulichen Informationen enthalten, werden vor ihrer Entsorgung derart behandelt, dass diese Daten nicht auslesbar oder wieder herstellbar sind. Kryptographische Geräte werden vor ihrer Entsorgung gemäß den Richtlinien des Herstellers physisch vernichtet. Andere Abfälle werden gemäß den regulären Entsorgungsrichtlinien von Telekom Security entsorgt.

5.1.8 Externe Sicherung

Telekom Security führt routinemäßige Sicherungskopien von kritischen Systemdaten, Audit-Protokolldaten und anderen vertraulichen Informationen durch. Sicherungskopien werden räumlich getrennt von den Ursprungsdaten gelagert.

5.2 Organisatorische Maßnahmen

Die organisatorischen Maßnahmen sind im Sicherheitsrahmenkonzept [SRK TC] und Sicherheitskonzept der SBCA [SBCA Siko] dokumentiert und werden durch das Betriebskonzept des Trust Centers umgesetzt. Die relevanten Anforderungen aus [ETSI EN TSP] Kapitel 7.4 b, c, d, e sind umgesetzt.

5.2.1 Vertrauenswürdige Rollen

Vertrauenswürdige Personen sind alle Personen (Mitarbeiter der Telekom Security, Mitarbeiter des Mandanten, Auftragnehmer, und Berater) mit Zugang zu oder Kontrolle über Authentifizierungs- oder kryptographische Abläufen, die erhebliche Auswirkungen auf Folgendes haben können:

- die Validierung von Informationen in Zertifikatsanträgen,
- die Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatsanträgen, Sperranträgen oder Erneuerungsanträgen,
- die Vergabe oder den Widerruf von Zertifikaten, einschließlich Personal, das Zugang und Zugriff auf die Datenbanksysteme hat,
- den Umgang mit Informationen oder Anträgen von Endteilnehmern.

Vertrauenswürdige Personen sind insbesondere:

- Mitarbeiter des Trust Centers (z.B. Systemadministration, interne Registrierungsstellenmitarbeiter),
- Registrierungsstellenmitarbeiter des Mandanten (externe Registrierungsstellenmitarbeiter),
- Mitarbeiter kryptographischer Abteilungen,
- Sicherheitspersonal,
- zuständiges technisches Personal und
- für die Verwaltung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

Die o.g. vertrauenswürdigen Personen müssen die in dieser CPS festgelegten Anforderungen (Kapitel 5.3.1) erfüllen und die jeweilige(n) Rolle(n) zugewiesen werden. Durch eine schriftliche Bestätigung (z.B. per e-Mail) akzeptieren diese Personen ihre zugewiesene(n) Rolle(n). Diese Nachweise müssen mindestens 7 (Sieben) Jahre archiviert werden.

Ebenfalls müssen diese vertrauenswürdigen Personen frei von Interessenskonflikten gestellt werden, damit die ausgeübten Rollen unbefangen und vorurteilsfrei ausgeübt werden können. Die Mitarbeiter verpflichten sich zur Anerkenntnis und Einhaltung des vom Konzern vorgegebenen „Code of Conduct“.

Das Telekom Security Advisory Board ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten und CPS der von Telekom Security Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.2.2 Anzahl involvierter Personen pro Aufgabe

Die Aufrechterhaltung des Betriebs der Zertifizierungsinstanz und Verzeichnisdienstes wird von fachkundigen und vertrauenswürdigen Personen wahrgenommen.

Arbeiten an hochsensitiven Komponenten (z.B. Schlüsselerstellungssysteme, HSM) sind durch besondere interne Kontrollverfahren geregelt und werden von mindestens zwei Mitarbeitern durchgeführt.

Den Systemadministratoren des Trust Centers stehen im Störungsfalle zusätzlich Master- und Sub-Registrator- oder Trust-Center-Operatorrechte zum Zwecke der Störungsbeseitigung zur Verfügung.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

5.2.3.1 Mitarbeiter des Trust Centers

Mitarbeiter der internen Registrierungsstelle der Telekom Security, die als besonders vertrauenswürdige Personen eingestuft sind und besonders vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer Telekom Security -internen Sicherheitsüberprüfung (siehe Kapitel 5.3.2).

Telekom Security stellt sicher, dass Mitarbeiter einen vertrauenswürdigen Status erlangt haben und die Zustimmung der Abteilung erteilt wurde, bevor diese Mitarbeiter

- Zugangsgeräte und Zugang zu den erforderlichen Einrichtungen erhalten,
- die elektronische Berechtigung zum Zugriff auf die SBCA und andere IT-Systeme erhalten,
- zur Durchführung bestimmter Aufgaben im Zusammenhang mit diesen Systemen zugelassen werden.

Die Mitarbeiter des Trust Centers werden nach positiver Prüfung formell vom Leiter des Trust Centers ernannt.

5.2.3.2 Mitarbeiter einer externen Registrierungsstelle

Der Mandant/externe Registrierungsstelle muss gewährleisten, dass nur vertrauenswürdige Personen (Master- bzw. Sub-Registratoren) die die Tätigkeiten der Registrierungsstellen wahrnehmen.

5.2.4 Rollen, die eine Funktionstrennung erfordern

Folgende Rollen unterliegen einer Funktionstrennung:

- Die Erstellung, Installation oder Vernichtung von Sub-CA- und Root-CA-Zertifikaten,
- Sicherung und Rücksicherungen von Datenbanken und HSMs.

5.3 Personelle Maßnahmen

Telekom Security setzt umfassende personelle Sicherheitsmaßnahmen um, die einen hohen Schutz ihrer Einrichtungen und der Zertifizierungsdienste gewährleisten. Im Trust Center ist der Einsatz von qualifiziertem geschultem Personal obligatorisch die personellen Maßnahmen sind im Sicherheitskonzept [SBCA Siko] dokumentiert.

Das Personal unterliegt keinem Kostendruck oder Mengengerüst oder sonstigen Zwängen deren Einhaltung möglicherweise mit den Qualitätsanforderungen bei der Prüfung von Antragsunterlagen konkurrieren würde.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

5.3.1.1 Mitarbeiter der Telekom Security

Für den Betrieb der in Kapitel 1 beschriebenen PKI-Dienstleistungen verlangt Telekom Security von seinen Mitarbeitern, die eine vertrauenswürdige Rolle einnehmen sollen, entsprechende Nachweise über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.

In regelmäßigen Abständen ist dem Personalvorgesetzten ein neues polizeiliches Führungszeugnis vorzulegen.

5.3.1.2 Mitarbeiter einer externen Registrierungsstelle

Der Mandant muss gewährleisten, dass das eingesetzte Personal (Master- bzw. Sub-Registratoren) die Tätigkeiten einer Registrierungsstelle in Bezug auf Fachkunde und Zuverlässigkeit durchführen kann. Die Qualifikation und Maßnahmen zur Zuverlässigkeitsprüfung müssen auch gegenüber Auditoren nachweisbar sein.

Vor Ausstellung eines Master-Registrator-Zertifikats ist die Identität des Master-Registrators nachzuweisen. Der Mandant oder sein Vertreter stellt dazu die Kopie eines Ausweisdokuments des Master-Registrators zur Verfügung.

5.3.2 Sicherheitsüberprüfung

5.3.2.1 Mitarbeiter der Telekom Security

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt Telekom Security eine Sicherheitsüberprüfung durch mit folgendem Inhalt durch:

- Überprüfung und Bestätigung der bisherigen Beschäftigungsverhältnisse,
- Überprüfung von Arbeitszeugnissen,
- Bestätigung des höchsten oder maßgebenden Schul-/Berufsabschlusses,
- polizeiliches Führungszeugnis.

Sofern die in diesem Abschnitt festgelegten Anforderungen nicht erfüllt werden können, macht Telekom Security ersatzweise Gebrauch von einer gesetzlich zulässigen Ermittlungsmethode, die im Wesentlichen die gleichen Informationen liefert.

Ergebnisse einer Sicherheitsüberprüfung, die zu einer Ablehnung eines Anwärters für eine vertrauenswürdige Person führt, können beispielsweise sein

- falsche Angaben seitens des Anwärters oder der vertrauenswürdigen Person,
- besonders negative oder unzuverlässige berufliche Referenzen, und
- gewisse Vorstrafen.

Berichte, die solche Informationen enthalten, werden durch Mitarbeiter der Personalabteilung und Sicherheitspersonal bewertet, die das weitere angemessene Vorgehen festlegen. Das weitere Vorgehen kann Maßnahmen bis einschließlich zur Rücknahme des Einstellungsangebots an Anwärter für vertrauenswürdige Positionen führen oder der Kündigung von vertrauenswürdigen Personen beinhalten.

Die Verwendung von in einer Sicherheitsüberprüfung ermittelten Informationen zur Ergreifung solcher Maßnahmen unterliegt geltendem Recht.

5.3.2.2 Mitarbeiter einer externen Registrierungsstelle

Nicht anwendbar.

5.3.3 Schulungs- und Fortbildungsanforderungen

5.3.3.1 Mitarbeiter der Telekom Security

Das Personal des Telekom Security Trust Centers besucht Fortbildungsmaßnahmen, die zur kompetenten und zufriedenstellenden Erfüllung ihrer beruflichen Pflichten erforderlich sind. Telekom Security führt Unterlagen über diese Schulungsmaßnahmen.

Die Schulungsprogramme sind auf die individuellen Tätigkeitsbereiche abgestimmt und beinhalten u.a.:

- fortgeschrittene PKI-Kenntnisse,
- Verfahrensweisen nach ITIL,
- Daten- und Fernmeldegeheimnis,
- Informationsschutz,
- Zutrittsschutz,
- Antikorruption,
- Datenschutz,
- Sicherheits- und Betriebsrichtlinien und –verfahren von Telekom Security,
- Verwendung und Betrieb eingesetzter Hardware und Software,
- Meldung von und Umgang mit Störungen und Kompromittierungen und
- Verfahren für die Schadensbehebung im Notfall (Disaster Recovery) und Geschäftskontinuität (Business Continuity).

Mitarbeiter, welche mit der Validierung von Zertifikatsaufträgen befasst sind, erhalten zusätzlich Schulungen in den folgenden Bereichen:

- Richtlinien, Verfahren und aktuelle Entwicklungen zu Validierungsmethoden
- Inhalte und insbesondere relevante Änderungen des vorliegenden CPS und der zugehörigen CP
- relevante Anforderungen und Vorgaben aus den Zertifizierungsnormen [CAB-BR]
- Allgemeine Bedrohungs- und Angriffsszenarien bzgl. der Validierungsmethoden (z.B. Social Engineering)

Die Schulungen sind schriftlich zu dokumentieren und die Lerninhalte jährlich mit einer Prüfung (examination) zu bestätigen.

5.3.3.2 Mitarbeiter einer externen Registrierungsstelle

Telekom Security stellt dem Mandanten bzw. Master-Registrator entsprechende Schulungsunterlagen zur Verfügung, aus der die Funktionen, Prozesse und begleitende Dokumentation ersichtlich sind.

Der Master-Registrator ist verpflichtet, neue Registrierungsstellenmitarbeiter vor Übernahme der Registrierungstätigkeit entsprechend den Anforderungen zu schulen. Diese Schulung ist schriftlich zu dokumentieren und auf Anfrage der Telekom Security oder einem beauftragten Dritten nachzuweisen.

Der Master-Registrator führt im Rahmen von Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) jährlich eine Schulung für die zuständigen Sub-Registratoren inkl. Derivaten durch. Diese Schulung ist schriftlich zu dokumentieren und auf Anfrage der Telekom Security oder einem beauftragten Dritten nachzuweisen.

5.3.4 Nachschulungsintervalle und -anforderungen

5.3.4.1 Mitarbeiter der Telekom Security

Das Personal des Trust Centers erhält im erforderlichen Umfang und den erforderlichen Abständen Auffrischungsschulungen und Fortbildungslehrgänge. Die Erfordernisse werden jährlich überprüft und im Schulungsprogramm eingepflegt.

5.3.4.2 Mitarbeiter einer externen Registrierungsstelle

Im Falle, dass Telekom Security neue Schulungsunterlagen bereitstellt, die relevante Schulungsthemen beinhalten, ist der Master-Registrator verpflichtet, eine gesonderte Schulung gemeinsam mit den zuständigen Sub-Registratoren (und Derivaten) durchzuführen. Diese Schulung ist schriftlich zu dokumentieren und auf Anfrage der Telekom Security oder einem beauftragten Dritten nachzuweisen.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

5.3.6 Sanktionen bei unbefugten Handlungen

5.3.6.1 Mitarbeiter der Telekom Security

Die Telekom Security behält sich vor, unbefugter Handlungen oder anderer Verstöße gegen dieser CPS und Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA der daraus abgeleiteten Verfahren zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen und können Maßnahmen bis einschließlich der Kündigung beinhalten.

5.3.6.2 Mitarbeiter einer externen Registrierungsstelle

Die Ahndung etwaige Verstöße obliegt der Verantwortung des Mandanten/Externe Registrierungsstelle.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Telekom Security behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter der Telekom Security in vergleichbarer Position.

Obiger Personenkreis, der die in Kapitel 5.3.2.1 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von Telekom Security nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.3.8 Dokumentation für das Personal

5.3.8.1 Mitarbeiter der Telekom Security

Um die beruflichen Pflichten angemessen erfüllen zu können, stellt Telekom Security seinen Mitarbeitern alle dafür erforderlichen Dokumente (Schulungsunterlagen, Verfahrensanweisungen) und Hilfsmittel zur Verfügung.

5.3.8.2 Mitarbeiter einer externen Registrierungsstelle

Telekom Security stellt entsprechende Dokumentation zur Verfügung, aus denen die Funktionen und der Betrieb der Registrierungsstellen hervorgehen.

5.4 Protokollereignisse

Es ist im Loggingkonzept sowie im Installationshandbuch festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden.

Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden (derzeit 6 Wochen) und wie sie vor Verlust und unbefugtem Zugriff geschützt werden.

Es werden dabei die Anforderungen aus [ETSI EN TSP] Kap. 7.10 umgesetzt.

5.4.1 Art der aufgezeichneten Ereignisse

Generell enthalten alle Protokolleinträge mindestens das Datum und die Uhrzeit des Eintrags, einen Verweis auf die Person oder das System, welches den Eintrag generiert hat, sowie eine Beschreibung des Ereignisses.

5.4.1.1 CA-Schlüsselpaare und CA-Systeme

Für das Lifecycle–Management für CA-Schlüsselpaare bzw. von CA-Systemen protokolliert das Telekom Security Trust Center für TeleSec Shared-Business-CA mindestens die folgenden Ereignisse:

- Erzeugung, Vernichtung, Speicherung, Sicherung und Wiederherstellung, sowie Archivierung des Schlüsselpaares oder Teile des Schlüsselpaares
- Ereignisse im Lebenszyklus-Management von kryptografischen Geräten (z.B. HSM), sowie der eingesetzten CA-Software

5.4.1.2 EE- und CA-Zertifikate

Für das Lifecycle-Management von EE- als auch CA-Zertifikaten und deren Validierung protokolliert das Trust Center der Telekom Security für TeleSec Shared-Business-CA mindestens die folgenden Ereignisse:

- Auftrag und Sperrung von Zertifikaten
- Auftrag zur Erneuerung mit und ohne Schlüsselwechsel (renewal und rekey)
- Alle Tätigkeiten im Zusammenhang mit der Verifikation von Informationen
- Das Ergebnis, sowie Datum/Uhrzeit und Rufnummer von Telefonaten im Zusammenhang mit der Verifikation und Name des Gesprächspartners
- Annahme oder Ablehnung von Zertifikatsaufträgen
- Ausstellung eines Zertifikates
- Erzeugung von Sperrlisten (CRL) und OCSP-Einträgen

5.4.1.3 Sonstige sicherheitsrelevante Ereignisse

Zusätzlich werden vom Trust Center der Telekom Security für den Betrieb der Infrastruktur TeleSec Shared-Business-CA alle sicherheitsrelevanten Ereignisse protokolliert. Das beinhaltet mindestens die folgenden Ereignisse:

- Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI
- Durchgeführte Aktionen an und durch PKI- und sonstigen sicherheitsrelevanter Systeme
- Änderungen an Sicherheitsprofil
- Systemabstürze, Hardware-Ausfälle und andere Anomalien
- Firewall- und Router-Aktivitäten
- Zutritt und Verlassen von Einrichtungen des Trust Centers
- Ergebnisse von Netzwerkprüfungen (Schwachstellenüberprüfungen)
- Start und Beendigung des Protokollierungsprozesses

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

5.4.2 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/History-Daten/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft Telekom Security ihre Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen der SBCA.

Eingeleitete Maßnahmen, die als Reaktion aus der Auswertung von Audit-Protokollen/Logging-Dateien stammen, werden ebenfalls protokolliert.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Audit-Protokolle/History-Daten/Logging-Dateien werden nach Bearbeitung gemäß Kapitel 5.5.2 archiviert.

5.4.4 Schutz der Audit-Protokolle

Audit-Protokolle/History-Daten/Logging-Dateien werden mit Betriebssystemmechanismen gegen unbefugten Zugriff geschützt.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Eine inkrementelle Sicherung von Audit-Protokollen/History-Daten/Logging-Dateien wird täglich durchgeführt.

5.4.6 Audit-Erfassungssystem (intern vs. extern)

Audit-Daten/History-Daten/Logging-Dateien von Anwendungs-, Netzwerk- und Betriebssystemebene werden automatisch erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von Telekom Security -Mitarbeitern aufgezeichnet.

5.4.7 Benachrichtigung des ereignisauslösenden Subjekts

Ereignisse, die das Audit-Monitoringsystem erfasst, werden bewertet an das zuständige Trust-Center-Personal weitergeleitet. Ereignisse mit hoher Priorität werden unverzüglich -auch außerhalb der Regelarbeitszeit- an das Trust-Center-Personal weitergeleitet.

5.4.8 Schwachstellenbewertung

Nach jeder signifikanten System- oder Netzwerkänderung oder einer Aufforderung des CA/Browserforums erfolgt innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan). Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen festgelegt und in einem definierten Plan umgesetzt. Die Schwachstellenüberprüfungen, ihre Ergebnisse und Aktionen (Behebungen, Austausch) werden dokumentiert.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen, die dem TSP mitgeteilt wurden, werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Im Falle, dass eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

5.5 Datenarchivierung

5.5.1 Art der archivierten Datensätze

Telekom Security archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener Form (z.B. Angebote, Aufträge),
- Informationen in Zertifikatsanträgen und zum Zertifikatslebenszyklus (z.B. Sperr- und Erneuerungsanträge),
- Soft-PSE, die über Bulk beantragt wurden,
- alle Audit-Daten/History-Daten/Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden,

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommener Sperrungen, werden sieben (7) Jahre nach Ablauf der Zertifikatsgültigkeit vorgehalten,
- Soft-PSE, die über Bulk beantragt wurden, werden max. dreißig (30) Tage archiviert,
- Audit-, History- und Event-Logging Daten werden bis zu zweiundvierzig (42) Tage archiviert.

5.5.3 Schutz von Archiven

Telekom Security stellt sicher, dass nur autorisierte und vertrauenswürdige Personen Zutritt zu Datenträgerarchiven erhalten. Archivdaten sind gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt.

5.5.4 Sicherungsverfahren für Archive

Eine inkrementelle Sicherung der elektronischen Archive wird täglich durchgeführt.

Telekom Security bewahrt die Datenträger auf, die die Archivdaten und die zur Verarbeitung der Archivdaten erforderliche Anwendungen enthalten, um die Archivdaten für den in dieser CPS festgelegten Archivierungszeitraum zu gewährleisten.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Datensätze wie beispielsweise Zertifikate, Zertifikatssperrlisten, OSCP-Antworten, Loging-Dateien enthalten Informationen über Datum und Uhrzeit. Als Zeitquelle dient eine NTP-Appliance (mit GPS- und DCF77-Antenne), aus dem die UTC abgeleitet wird. Die einzelnen Systeme gleichen die Systemzeit mit der Zeitquelle mehrmals am Tag ab.

5.5.6 Archiverfassungssystem (intern oder extern)

Telekom Security verwendet ausschließlich interne Archivierungssysteme.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Nur autorisiertes und vertrauenswürdiges Personal erhält Zutritt zu Archiven und damit Zugang und Zugriff auf Archivdaten. Bei der Wiederherstellung der Archivdaten werden diese auf Authentizität verifiziert.

5.6 Schlüsselwechsel

Zertifikate verlieren ihre Gültigkeit nach Überschreitung des Gültigkeitszeitraums.

Innerhalb des Gültigkeitszeitraums kann ein Schlüsselwechsel bzw. Zertifikatswechsel in folgenden Fällen erforderlich werden:

- Kompromittierung des Schlüsselmaterials,
- zwingende Änderung des Kryptoalgorithmus,
- zwingende Änderung der Schlüssellänge,
- Änderung des Zertifikatsinhalts.

Ein Schlüsselwechsel von Registrator- und Endteilnehmer-Zertifikaten liegt in der Verantwortung des Mandanten. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3).

Die Generierung neuer CA- und Root-CA-Schlüssel als auch OCSP-Responder-Zertifikate wird dokumentiert und gemäß den Regelungen des Schlüsselgenerierungsverfahren (Key Generation Ceremony) überwacht. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3).

Telekom Security informiert unverzüglich alle Mandanten vor Integration der neuen CA- und Root-CA-Zertifikate in die entsprechenden Dienste, damit ein reibungsloser Übergang von altem auf ein neues Schlüsselpaar möglich wird.

Abgelaufene oder gesperrte CA- und Root-CA-Zertifikate stehen solange zur Validierung auf einer Webseite zur Verfügung, bis das letzte Endteilnehmer-Zertifikat abgelaufen ist und nach der gesetzlich vorgeschriebenen Archivierungszeit gelöscht wurde.

5.7 Kompromittierung und Wiederherstellung (Disaster Recovery)

5.7.1 Umgang mit Störungen und Kompromittierungen

Die Notfalldokumentation des Trust Centers berücksichtigt die Anforderungen der Telekom Security CP.

Telekom Security hat ein IT-Servicemanagement gemäß ITIL sowie ISMS Prozesse etabliert, über die Störungen und Sicherheitsvorfälle nach definierten Standard-Prozessen bearbeitet werden.

Durch die Festlegung aller erforderlichen Ansprechpartner und entsprechend eingerichteter Gruppen in den IT-Servicemanagement-System sowie der Etablierung einer Rufbereitschaft und des MoD (Manager on Duty) ist sichergestellt, dass die Bearbeitung von Störungen und

Sicherheitsvorfälle kurzfristig beginnt, damit der Schaden möglichst gering bleibt und schnell beseitigt werden kann.

Die TeleSec Shared-Business-CA verfügt über ein Service Level Agreement (SLA), indem der Störungsprozess ausführlich beschrieben ist.

Störungen werden vom Endteilnehmer über die im Service Level Agreement (SLA) definierten Kontakte des Service Desk eingereicht und im Rahmen des Service Managements bearbeitet.

Das Personal des Service Desk bewertet zunächst die Störung auf Basis der im Service Level Agreement (SLA) definierten Störungsklassen, bevor die Störung in die Störungsbearbeitungsanwendung der Telekom Security eingegeben, priorisiert und an den/die Fachbereich(e) zwecks Störungsbeseitigung weitergeleitet wird. In der EDV-Anwendung werden transparent alle Informationen revisionssicher gespeichert, um jederzeit den Bearbeitungsstand der Störung bis zur Beseitigung nachvollziehen zu können.

Das Service Desk wird, entsprechend der Störungsklasse, von dem Fachbereich über den Bearbeitungszustand in Kenntnis gesetzt, um der beauftragten Drittpartei (Delegated Third Party) entsprechende Informationen bereitstellen zu können.

Betroffene Kunden werden, sofern erforderlich, schnellstmöglich – spätestens aber innerhalb von 24 Stunden - informiert und in den Prozess eingebunden.

5.7.2 Beschädigung von EDV-Geräten, Software und/oder Daten

Bei einer Beschädigung der EDV-Komponenten, Software und/oder Daten wird der Vorfall unmittelbar untersucht und der Sicherheitsabteilung (dem Informationssicherheitsbeauftragten) gemeldet. Das Ereignis initiiert eine entsprechende Eskalation, Störfalluntersuchung, Störfallreaktion bis hin zur finalen Störungsbeseitigung. Abhängig von der Störungsklassifizierung erfolgt die Wiederherstellung (Disaster Recovery).

Jegliche Hard- und Software, die zur Bereitstellung des PKI-Service TeleSec Shared-Business-CA erforderlich ist, wird als Vermögensgegenstand (Asset) und Anwendung im Konfigurationsmanagement der Telekom Security geführt.

Diese Anwendung bildet auch die Basis für ein Problem-Management.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme auf eine Kompromittierung privater Schlüssel von CA- oder Root-CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.

Der Mandant wird über die mögliche Kompromittierung schriftlich informiert (siehe hierzu Kapitel 2.3). Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechende Zertifizierungsstellen-Sperrliste (CARL) zu generieren und zu veröffentlichen. Die Generierung neuer Schlüssel und Zertifikate ist gemäß den Arbeitsanweisungen zu dokumentieren und gemäß den Auflagen des jeweiligen Sicherheitskonzepts zu überwachen. Neue Zertifikate und ihre Fingerprints sind zu veröffentlichen (siehe hierzu Kapitel 2.3).

5.7.4 Geschäftskontinuität nach einem Notfall

Telekom Security hat für den Rechenzentrumsbetrieb einen Notfallplan entwickelt, implementiert und getestet, um die Auswirkungen von Katastrophen jeder Art (Naturkatastrophen oder Katastrophen menschlichen Ursprungs) zu mildern und die Verfügbarkeit kritischer Geschäftsprozesse schnellstmöglich wiederherzustellen. Dieser umfasst auch alle Prozesse, Komponenten, Systeme und Dienste des Trust Centers. Dieser Plan wird mindestens jährlich überprüft, getestet und entsprechend aktualisiert, um im Falle einer Katastrophe gezielt und strukturiert reagieren zu können.

Der Notfallplan enthält mindestens die folgenden Informationen:

- Die notwendigen Kriterien für die Aktivierung des Planes,
- Mögliche Notfallmaßnahmen (je nach Situation),
- Ausweichverfahren,
- Wiederanlauf-Verfahren,
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung,
- Sensibilisierungsmaßnahmen,
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals,
- Die Verantwortung der Individuen (Rollenbeschreibung und -zuweisung),
- Wiederanlaufzeit (RTO),
- Regelmäßige Durchführung der Notfallpläne zu Testzwecken,
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der SBCA Geschäftstätigkeit nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse,
- Eine Verpflichtung kritische kryptographische Geräte und Informationen an einem anderen Standort zu sichern bzw. vorzuhalten,
- Festlegung der maximal tolerierbaren Ausfallzeit (MTO) und entsprechende Zeiten zur Wiederherstellung,
- Häufigkeit, in der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden,
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur SBCA Hauptgeschäftsstelle bzw. zum Rechenzentrum des Trust Centers,
- Verfahren zur bestmöglichen Sicherung der Betriebsstätten und –Einrichtungen nach einer Katastrophe (Notbetrieb) bis zur Wiederherstellung eines den Anforderungen entsprechend gesicherten Normalbetriebs.

Im Rahmen eines Compliance-Audits (siehe Kapitel 8 ff) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

5.8 Betriebsbeendigung einer Zertifizierungs- oder Registrierungsstelle

5.8.1 Beendigung der Zertifizierungsstelle

Eine Betriebsbeendigung der Zertifizierungsstelle (Kapitel 1.3.1 ff) oder internen Registrierungsstelle der Telekom Security (Kapitel 1.3.2.1) kann nur durch Telekom Security ausgesprochen werden.

Im Falle der Einstellung des Zertifizierungsdienstes geht die Zertifizierungsstelle entsprechend den Vorgaben aus [ETSI EN TSP] Kap. 7.12 vor und hat dafür einen Beendigungsplan erstellt, der folgende Maßnahmen beschreibt:

- Benachrichtigung der Mandanten, Endteilnehmer und Vertrauende Dritte über die geplante Einstellung des Dienstes,
- Fortführung der Sperrfunktionalitäten einschließlich der regelmäßigen Erstellung von Sperrlisten, Abruf der Zertifikatsstatusinformationen und Service-Desk-Funktionen,
- Sperrung von involvierten Sub-CA-Zertifikaten,
- eventuell erforderliche Übergangsregelungen auf eine Nachfolge-CA,
- je nach Ausgestaltung bestehender Einzelverträge entstehende Kostenerstattung,
- Aufbewahrung der Unterlagen und Archive der Zertifizierungsinstanz (CA).

Vor der Einstellung des Dienstes werden alle möglichen Maßnahmen getroffen, um den potentiellen Schaden für alle Beteiligten möglichst gering zu halten. Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen, betroffene nachgeordnete Stellen

(Endteilnehmer, vertrauende Dritte, Registrierungsstellen des Mandanten und Telekom Security) so früh als möglich vorab über diese Betriebsbeendigung zu informieren.

Anschließend sind alle noch gültigen Zertifikate zu sperren. Anschließend werden alle Rechte der Mitarbeiter der Zertifizierungsstelle und der Registrierungsstellen entzogen, die privaten Schlüssel der CAs werden vernichtet.

Alle elektronisch erfassten Daten mit Ausnahme der Zertifikate und Sperrlisten werden gelöscht. Die Zertifikate und Sperrlisten sowie Papierdokumente werden archiviert, um ggf. zur Beweissicherung in Gerichtsprozessen darauf zugreifen zu können.

5.8.2 Beendigung der externen Registrierungsstelle

Eine Betriebsbeendigung der Registrierungsstelle eines Mandanten (externe Registrierungsstelle) (Kapitel 1.3.2.2) erfolgt nach Kündigung durch den Mandanten selbst oder durch Telekom Security. Außerdem kann Telekom Security einen PKI-Mandanten deaktivieren im Falle, dass eine gravierende Pflichtverletzung (z.B. Missbrauch, mehrmalige geahndete Verletzungen dieser CPS) vorliegt verursacht durch den Inhaber, einem seiner Mitarbeiter oder beauftragten Dritten.

Die interne Registrierungsstelle deaktiviert zunächst die Ausstellung und Erneuerung von Endteilnehmer-Zertifikaten. In Abstimmung mit dem Kunden werden die Endteilnehmer-Zertifikate gesperrt. Im Falle einer gravierenden Pflichtverletzung (z.B. Missbrauch, mehrmalige geahndete Verletzungen dieser CPS) ist Telekom Security berechtigt alle Endteilnehmer-Zertifikate des Mandanten unmittelbar zu sperren.

Bei einer Beendigung bzw. Auflösung einer externen Registrierungsstelle (z.B. Vertragskündigung, Umfirmierung, Insolvenz) muss der Kunde seinen Archivierungsverpflichtung nachkommen (Kapitel 5.5 ff). Auf Anfrage des TSP muss der Kunde Zugriffsrechte auf diese Daten unentgeltlich einräumen. Im Falle einer Zahlungsunfähigkeit (Insolvenz) muss der Kunde rechtzeitig den TSP informieren und unmittelbar Zugriffsrechte auf diese Daten unentgeltlich einräumen.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

Die technischen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept [SBCA Siko] festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen. Es werden die Vorgaben aus [ETSI EN TSP] Kap. 7.5 umgesetzt.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Alle Schlüsselpaare für CA-Zertifikate werden von geschultem und vertrauenswürdigem Fachpersonal (Trusted Roles) in einem abstrahlarmen Raum auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140-2/ Level 3 evaluiert) in der sogenannten “Key Ceremony” (Schlüsselgenerierungsverfahren) erzeugt und abgelegt.

Im Fall von CA- und Root-CA-Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem evaluierten HSM (FIPS 140-1/ Level 3 evaluiert) erzeugt und abgelegt.

Alle Aktivitäten während der “Key Ceremony“ werden protokolliert und von allen beteiligten Personen unterzeichnet. Diese Aufzeichnungen werden zu Audit- und Nachverfolgungszwecken für einen von Telekom Security als angemessen erachteten Zeitraum aufbewahrt.

Die Generierung des Schlüsselpaars für ein Zertifikat für eine öffentliche Stammzertifizierungsstelle (Public Root) und dem zugehörigen Zertifikat für eine Zwischenzertifizierungsstelle (Sub-CA) erfolgt auf der Offline-CA und dem zugeordneten kryptografischen Hardware-Security-Moduls (HSM) unter Aufsicht eines unabhängigen und qualifizierten Auditors.

Die Generierung des Schlüsselpaars für eine Zwischenzertifizierungsstelle (Sub-CA) erfolgt auf dem für die TeleSec Shared-Business-CA zugeordneten kryptografischen Hardware-Security-Moduls (HSM) im Online-Betrieb. Das zugehörige Zertifikat der Zwischenzertifizierungsstelle wird auf der Offline-CA generiert.

Alle Schlüsselgenerierungen und Zertifikatsausstellungen an der Offline-CA werden mittels Prüfprotokoll und Video-Aufzeichnung protokolliert und revisionssicher dokumentiert.

Die Systeme der Offline-CA, bestehend aus Zertifizierungsinstanz, kryptografischen Hardware-Security-Moduls (HSM) (inkl. Back-Up-Token) und Browser, werden „offline“, d.h. ohne Anbindung an irgendeine eine Netzstruktur, betrieben. Die Systeme der Offline-CA sind in einem verschließbaren Computer-Rack untergebracht und gehen Öffnung und Austausch versiegelt. Die Unversehrtheit der Versiegelung wird bei jeder Nutzung der Offline-CA geprüft und dokumentiert.

Die Generierung von Master-Registrator-Zertifikaten erfolgt in der Regel von der internen Registrierungsstelle Telekom Security und unter Verwendung des auf der Smartcard befindlichen Schlüssels.

Für die Ausstellung des Sub-Registrator-Zertifikats gilt folgender Regeung:

- Im Falle, dass Endteilnehmer-Zertifikate von einer öffentlichen Zertifizierungsstelle (Kapitel 1.3.1.2.1) ausgestellt werden sollen, muss das Sub-Registrator-Zertifikat auf einer Smartcard ausgestellt sein. Diese Regelung trifft nicht auf das Derivate des Sub-Registrator-Zertifikat zu (Kapitel 1.3.2.2.2).
- Für Endteilnehmer-Zertifikate, die von einer internen Zertifizierungsstelle (Kapitel 1.3.1.2.2) ausgestellt werden sollen, darf das Sub-Registrator-Zertifikat auch als Soft-PSE ausgestellt sein.

Die Generierung der Endteilnehmer-Schlüsselpaare liegt in der Verantwortung des Mandanten. Es können die Schlüssel einer Smartcard, die im Betriebssystem, Browser oder einer Anwendung (z.B. Server, OpenSSL) generierten Schlüssel, verwendet werden.

Eine Ausnahme bildet die Bulk-Funktion der TeleSec Shared-Business-CA. Hier wird das Schlüsselpaar über einen Schlüsselgenerator in der CA erzeugt.

6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Die Zustellung von privaten Schlüsseln an Endteilnehmer erfolgt durch den Mandanten bzw. davon autorisierten Personen (Master-, Sub-Registrator) über sicherem Wege (z.B. persönliche Zustellung). Vorpersonalisierte Smartcards sind mit einem PIN-Brief zu versehen und über getrenntem und sicherem Wege an den Endteilnehmer zu versenden. Zum Schutz des privaten Schlüssels ist die Soft-PSE mit einem sicheren Passwort zu versehen.

Die Versandart obliegt der Verantwortung des Mandanten. Der Eingang der Smartcard oder Soft-PSE des Endteilnehmers ist zu protokollieren. Zur Erhöhung der Sicherheit wird ein zeitversetzter Versand über einen kommerziellen Postdienst empfohlen.

Im Falle, dass der Endteilnehmer selbst Schlüsselpaare über das Betriebssystem oder Applikation generiert, oder ein anderes Schlüsselmedium (vorbeschlüsselte Smartcard) nutzt, entfällt die Zustellung von privaten Schlüsseln an den Endteilnehmer.

6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller

Alle Endteilnehmer und Registratoren reichen, nach erfolgreicher Authentifizierung, den zu zertifizierenden öffentlichen Schlüssel in elektronischer Form (PKCS#10-Request) über eine durch TLS/SSL gesicherten Verbindung bei der Zertifizierungsinstanz TeleSec Shared-Business-CA ein.

6.1.4 Zustellung öffentlicher Zertifizierungsstellenschlüssel an Vertrauende Dritte

Das Stammzertifikat „T-TeleSec GlobalRoot Class 2“, dass für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich ist, wird für alle Endteilnehmer und Vertrauende Dritte durch die Einbettung in die gängigen Zertifikatsspeicher der Betriebssysteme und Anwendungen zur Verfügung gestellt.

Das Stammzertifikat „Deutsche Telekom Internal Root CA 1“ und „Deutsche Telekom Internal Root CA 2“, dass für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich ist, muss in den Zertifikatsspeicher nachinstalliert werden.

Das dem jeweiligen Stammzertifikat untergeordnete Sub-CA-Zertifikat wird im Rahmen einer Signatur oder Authentifikation durch die Applikation zur Zertifikatsvalidierung vom Absender (Quelle) mit versandt oder ist in den jeweiligen Zertifikatsspeicher nachträglich zu installieren.

Alle Stammzertifikate und Sub-CA-Zertifikate stehen auf der öffentlichen Webseite www.telesec.de, auf den rollenspezifischen Webseiten der TeleSec Shared-Business-CA (Master-, Sub-Registrator, Benutzer) und auf dem Verzeichnisdienst zum Herunterladen bereit.

6.1.5 Schlüssellängen

Um nicht mit Hilfe der Kryptoanalyse private Schlüssel ermitteln zu können, müssen die Schlüssellängen innerhalb des definierten Verwendungszeitraums über eine ausreichende Länge verfügen.

Alle Zertifikate (Zwischenzertifizierungsstelle, Endteilnehmer), die von einer öffentlichen Stamm-zertifizierungsstelle ausgestellt werden, als auch dieses Zertifikat selbst, erfüllten die Anforderungen der Baseline Requirements [CAB-BR] in der aktuellen Fassung zum Zeitpunkt der Freigabe und Veröffentlichung.

Die Zertifikate der internen Stamm- und Zwischenzertifizierungsstellen verfügen über eine RSA-Schlüssellängen von mindestens 2.048 Bit (siehe Kapitel 1.3.1.1.1 und 1.3.1.2.1).

Alle Endteilnehmer-Zertifikate, die von einer internen Zwischenzertifizierungsstelle (siehe Kapitel 1.3.1.2.2) ausgestellt werden, müssen über eine RSA-Schlüssellängen von mindestens 1.024 Bit verfügen.

Telekom Security empfiehlt für Registratoren eine ausreichende Schüssellänge von mindestens 2.048 Bit zu verwenden.

Die Schlüssellänge auf Basis Elliptischer Kurven (Elliptic Curve Cryptography, ECC) beträgt, abhängig von den Kurvenparametern, 256 oder 384 Bit.

6.1.6 Generierung der Parameter von öffentlichen Schlüssel und Qualitätskontrolle

Der während der Antragstellung eingereichte Zertifikatsrequest (PKCS#10) wird auf die folgenden Qualitätsparameter geprüft:

- Für die Schlüsselgenerierung wird das Kryptoverfahren RSA oder ECC verwendet.
- Für die Zertifikatsgenerierung wird der Signaturalgorithmus RSA mit SHA256, RSASSA-PSS mit SHA-256 oder ECDSA mit SHA-256 verwendet.
- Als Algorithmus-Parameter des öffentlichen Schlüssels wird verwendet:
  - RSA 05 00
  - ECC prime256v1 (auch secp256r1, NIST P-256) oder ECC secp384r1 (auch NIST P-384)
- Als Signatur-Hash-Algorithmus zulässig ist SHA-256, SHA-1 nur bei der Nutzung einer interne Zertifizierungsstelle.
- Die Mindestschlüssellänge für RSA-Schlüssel beträgt 2.048 Bit (Einschränkungen siehe Kapitel 6.1.5), die Schlüssellänge für ECC-Schlüssel beträgt 256 oder 384 Bit.
- Die Prüfung des Public Exponent entspricht den Vorgaben der aktuellen Baseline Requirements [CAB-BR].
- Der öffentliche Schlüssel ist kein Debian Weak Key.
- für Server-Zertifikate, die unter einer öffentlichen Zertifizierungsstelle ausgestellt werden sollen, konnte erfolgreich die zLint- und crt.sh-Prüfung durchgeführt werden

Schlägt eine der Parameterüberprüfungen fehl, wird der entsprechende Zertifikatsauftrag mit einem Hinweistext abgelehnt.

6.1.7 Schlüsselverwendungen (gemäß X.509v3-Erweiterung „key usage“)

Siehe Kapitel 7.1.2.1.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptographischer Module

Das Trust Center der Telekom Security hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA- und Root-CA-Schlüsseln gewährleisten zu können.

Endteilnehmer und Registratoren sind verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um den Verlust, Offenlegung und unberechtigte Nutzung von privaten Schlüsseln zu verhindern.

6.2.1 Standards und Kontrollen für kryptographische Module

Die privaten Schlüssel der CAs werden auf einem FIPS 140-2/Level 3 evaluiertem Hardware Security Modul (HSM) abgelegt. Die Sicherung der Schlüssel wird unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken (siehe auch Kapitel 6.2.2) durchgeführt.

Zum Schutz der kryptographischen Geräte während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet, die während der FIPS- und CC-Zertifizierungen geprüft wurden. Die Geräte werden hierbei getrennt von den zum Betrieb und zur Nutzung benötigten PED-Keys aufbewahrt, so dass die Kompromittierung einer einzelnen Lokation nicht ausreicht, um die Geräte missbräuchlich zu verwenden.

6.2.2 Mehrpersonenkontrolle (m von n) bei privaten Schlüsseln

Telekom Security hat technische, organisatorische und prozessuale Mechanismen implementiert, die die Teilnahme mehrerer vertrauenswürdiger und geschulter Personen des Telekom Security Trust Centers (Trusted Roles) erfordern, um vertrauliche kryptografische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentification mit Key) geschützt, der nur hierfür zuständigen Personen bekannt ist. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

6.2.3 Hinterlegung von privaten Schlüsseln

Eine Hinterlegung von privaten Schlüsseln (CA- und Root-CA-Schlüssel) bei Treuhändern außerhalb von Telekom Security wird nicht durchgeführt (Kapitel 4.12 ff).

6.2.4 Sicherung von privaten Schlüsseln

Das Trust Center der Telekom Security behält für Wiederherstellungs- und Notfallzwecke Sicherungskopien (Back-Up) des Schlüsselmaterials jedes CA-Zertifikates im erzeugenden HSM. Diese Schlüssel werden in verschlüsselter Form innerhalb des kryptografischen Hardware-Security-Moduls (HSM) und zugehörigen Schlüsselspeichergeräten im Trust Center der Telekom Security gespeichert.

Weiterhin gibt es Sicherungen der privaten CA-Schlüssel der jeweiligen Sub-CAs der TeleSec Shared-Business-CA in gesicherter Umgebung. Der Zugriff auf diese Schlüssel ist nur vertrauenswürdigen Personen des Trust Centers (Trusted Role) gestattet.

Der jeweilige private Schlüssel wird dabei in verschlüsselter Form auf speziellen Security-Tokens gespeichert.

Zur Wiederherstellung eines privaten Schlüssels einer CA, d.h. Installieren des Schlüssels in die CA-Software, werden ebenfalls mehrere vertrauenswürdige Personen des Trust Centers (Trusted Role) benötigt. Eine Wiederherstellung darf nur innerhalb der Hoch-Sicherheitszone des Trust Centers der Telekom Security erfolgen.

Telekom Security speichert keine Kopien von privaten Schlüsseln des Master- und Sub-Registrator-Zertifikats.

Der Mandant muss Sicherheitsvorkehrungen treffen, dass nur der Endteilnehmer oder autorisiertes Personal (z.B. Sub-Registratoren und Derivate, Kapitel 1.3.2.2.2) Schlüsselmaterial über die Webseiten beantragen, sichern und herunterladen können.

Die Wiederherstellung des Schlüsselmaterials von Endteilnehmern ist erlaubt, sofern der Endteilnehmer bzw. Schlüsselverantwortliche der Wiederherstellung zustimmt. Liegt diese Erlaubnis nicht vor, darf der Mandant dennoch die Wiederherstellung durchführen lassen, wenn rechtliche Gründe vorliegen wie

- Anforderungen in einem gerichtlichen oder behördlichen Verfahren,
- im Rahmen polizeilicher Ermittlungen,
- gesetzliche oder staatliche Vorschriften,
- Organisationsrichtlinien des Mandanten.

6.2.4.1 Sicherung und Wiederherstellung des Verschlüsselungsschlüssels durch Enrollment-Software

Der Sub-Registrator kann bei der Personalisierung der Smartcard durch Verwendung geeigneter Enrollment-Software die passwortgeschützte Soft-PSE (privater Schlüsselverschlüsselungsschlüssel

inkl. Verschlüsselungs-Zertifikat) als auch die korrespondierende Passwortdatei (enthält das Passwort der Soft-PSE) verschlüsselt abspeichern.

Zur Einhaltung des 4-Augen-Prinzips muss die Soft-PSE und die Passwortdatei getrennt auf dedizierte Zertifikate verschlüsselt werden, die ausschließlich im Sicherung- und Wiederherstellungsprozess Verwendung finden.

Es empfiehlt sich die Soft-PSE auf Zertifikat Nr. 1 und die Passwortdatei auf Zertifikat Nr. 2 zu verschlüsseln. Zur Wiederherstellung ist die Passwortdatei mit dem privaten Schlüssel des Zertifikat Nr. 2 zu entschlüsseln. Danach erfolgt die Entschlüsselung der Soft-PSE mit Zertifikat Nr. 1. Die Soft-PSE ist erst nach Eingabe des Passworts in den Zertifikatsspeicher importierbar.

6.2.4.2 Sicherung und Wiederherstellung von Soft-PSE über das Betriebssystem

Bei der Sicherung von Soft-PSEn, die von einer internen Zertifizierungsstelle (Kapitel 1.3.1.2.2) ausgestellt wurden, kann das Schlüsselmaterial über das Betriebssystem (Zertifikatsspeicher) exportiert und verschlüsselt beim Mandanten gespeichert werden. Der Mandant wählt ein Speichermedium aus, das seinen Ansprüchen entspricht.

Die Soft-PSE ist mit einem Sitzungsschlüssel verschlüsselt gespeichert und per Passwort gesichert. Zur Nutzung der Soft-PSE bedarf es der Eingabe des Passworts.

6.2.4.3 Sicherung und Wiederherstellung von Soft-PSE durch die Bulk-Funktion

Schlüsselmaterialien und Passwortdateien, die per Bulk-Funktion generiert wurden, verbleiben verschlüsselt abgespeichert im Trust Center der Telekom Security. Der Sub-Registrator kann diese nur innerhalb einer definierten Frist herunterladen.

Der Sub-Registrator authentisiert sich mittels Zertifikat an der Webseite (TLS/SSL-Client-Authentifikation). Unter Eingabe der Bearbeitungsnummer (Bulk-ID) steht die Soft-PSE als auch das Passwort zum Herunterladen zur Verfügung.

6.2.5 Archivierung privater Schlüssel

Im Falle der Überschreitung des Gültigkeitszeitraums der Zertifikate der Stammzertifizierungsstelle (Root-CA), Zwischenzertifizierungsstelle (Sub-CA) oder des OCSP-Service wird das Schlüsselmaterial des jeweiligen Zertifikates vernichtet. Eine Archivierung findet nicht statt.

Das Trust Center der Telekom Security archiviert Kopien von privaten Schlüsseln von Endteilnehmern innerhalb einer definierten Frist

- die im Rahmen einer automatisierten Massengenerierung von Benutzer-Zertifikaten (Bulk siehe Kapitel 3.2.3.4) durch das CA-System generiert wurden und zu einem späteren Zeitpunkt abrufbar sein sollen.

Die Archivierung von privaten Schlüsseln von Endteilnehmern, deren Zertifikate von einer öffentlichen Zertifizierungsstelle (Kapitel 1.3.1.2.1) ausgestellt wurden, dürfen nicht durch die Master- oder Sub-Registratoren des Mandanten archiviert werden.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptographischen Modul

Das Schlüsselmaterial für ein Zertifikat einer Zwischenzertifizierungsstelle (Sub-CA) wird auf einem kryptografischen Hardware-Security-Modul (HSM) im Online-Betrieb generiert. Der zu zertifizierenden öffentlichen Schlüssel mit den Daten des Subject-DN werden in elektronischer Form (PKCS#10-Request) auf sicherem Wege auf die Offline-CA übertragen, die das Sub-CA-Zertifikat generiert. Anschließend wird das Sub-CA-Zertifikat auf sicherem Wege auf das HSM der Online-CA übertragen und dem privaten Schlüssel zugeordnet. Die Übertragung des Schlüsselmaterials und dem zugehörigem Sub-CA-Zertifikat zwischen den HSM im Online-Betrieb erfolgt in verschlüsselter Form.

Smartcards, auf denen bereits Schlüssel aufgebracht sind oder die selbst Schlüssel generieren, ist ein Export privater Schlüssel nicht möglich. Im Rahmen einer Schlüsselsicherung kann lediglich das Schlüsselmaterial des Verschlüsselungszertifikats in die Karte importiert werden.

6.2.7 Speicherung privater Schlüssel auf kryptographischen Modulen

Das Trust Center der Telekom Security speichert CA-Schlüssel in sicherer Form auf kryptografischen Hardware-Security-Modulen (HSM), welche nach FIPS 140-2/ Level 3 evaluiert sind.

Smartcards speichern extern erzeugte Schlüssel oder selbst generierte Schlüssel in sicherer Form.

6.2.8 Methode zur Aktivierung privater Schlüssel

Alle Endteilnehmer (inkl. Registratoren) und Schlüsselverantwortliche müssen die Aktivierungsdaten (z.B. PIN, Importpasswort) für ihren bzw. anvertrauten privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß der vorliegenden CPS schützen.

Der private Schlüssel des Zertifikats einer Zwischenzertifizierungsstelle (Sub-CA) bleibt aktiv bis der Gültigkeitszeitraum überschritten wurde oder ein Sperrgrund vorliegt, der die Zertifikatssperrung auslöst.

6.2.8.1 Private Schlüssel von Endteilnehmer- und Sub-Registratoren (und deren Derivate)

Der Endteilnehmer inkl. Sub-Registrator (und deren Derivate, Kapitel 1.3.2.2.2) hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer ähnlichen Sicherheitsmaßnahme, um den Endteilnehmer bzw. Sub-Registrator vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann auch z.B. ein Passwort zum Betrieb des privaten Schlüssels, beinhalten. Die vorherige Bestimmung gilt nicht für Geräte-Zertifikate.
- Es werden wirtschaftlich angemessene Maßnahmen zum physikalischen Schutz des PC-Arbeitsplatzes, Registrator-Arbeitsplatzes oder Geräts ergriffen, um die Nutzung dieses Platzes/Geräts in Verbindung mit der Nutzung des zugehörigen privaten Schlüssels, ohne Genehmigung des Registrators, Endteilnehmers oder autorisierten Person, zuverlässig zu verhindern.

Wenn Endteilnehmer-Zertifikate mit ihren zugehörigen privaten Schlüsseln deaktiviert (abgelaufen, gesperrt) sind, dürfen sie nur in verschlüsselter Form und/oder mit Passwort- bzw. PIN-Schutz aufbewahrt werden.

6.2.8.2 Private Schlüssel von Master-Registratoren

Der Master-Registrator hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Verwendung einer Smartcard und Festlegung einer PIN gemäß Kapitel 6.4.1 oder Integration einer gleichwertigen Sicherheitsmaßnahme, um den Master-Registrator vor der Aktivierung des privaten Schlüssels zu authentifizieren.
- Es sind Maßnahmen zum physikalischen Schutz des Registrator-Arbeitsplatzes zu ergreifen, um eine Nutzung dieses Platzes in Verbindung mit dem zugehörigen privaten Schlüssel, ohne Genehmigung des Registrators, zuverlässig zu verhindern.

6.2.8.3 Private Schlüssel von Stamm- und Zwischenzertifizierungsstellen

Schlüsselmaterial für CA- und Root-CA-Zertifikate wird entsprechend durch die autorisierten Personen aktiviert und auf kryptographischen Hardware-Security-Modulen (HSM) aufgebracht (Kapitel 6.2.2 und 6.4.1).

Der zum CA-Zertifikat gehörende private Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt (Kapitel 4.9.3.1).

Der zum Root-CA-Zertifikat gehörende private Schlüssel wird nur zur Erzeugung von weiteren CA-Zertifikaten aktiviert. Nach Ablauf des Root-CA-Zertifikats wird der private Schlüssel nicht mehr genutzt.

Wenn Zertifikate mit ihren zugehörigen privaten Schlüsseln deaktiviert (gesperrt, abgelaufen) werden, dürfen sie nur in verschlüsselter Form und/oder mit Passwort- bzw. PIN-Schutz aufbewahrt werden.

6.2.8.4 Private Schlüssel von Trust-Center-Administratoren und -Operatoren

Der Trust-Center-Administrator oder -Operator hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer gleichwertigen Sicherheitsmaßnahme, um den Administrator oder Operator vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann z. B. auch ein Kennwort zum Betrieb des privaten Schlüssels, ein Windows Anmelde- oder Bildschirmschonerkennwort, ein Anmeldekennwort für das Netzwerk beinhalten.
- Ergreifung geeigneter Maßnahmen zum physischen Schutz des Administrator- oder Operator-Arbeitsplatzes vor unberechtigtem Zugriff.

6.2.9 Methode zur Deaktivierung privater Schlüssel

Die Deaktivierung von CA- und Root-CA-Schlüsseln erfolgt ereignisbezogen und obliegt dem Personal des Trust Centers der Telekom Security.

Die Deaktivierung von privaten Schlüsseln (Endteilnehmer, Registratoren) obliegt dem Mandanten.

6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von CA-Schlüsseln erfordert die Teilnahme mehrerer vertrauenswürdiger Personen (Trusted Roles) des Trust Centers. Dabei ist sicherzustellen, dass nach Vernichtung keine Fragmente des Schlüssels übrigbleiben, die zu einer Rekonstruktion des Schlüssels führen könnte.

Telekom Security verwendet zur sicheren Schlüsselvernichtung eine integrierte Löschfunktion des HSM.

Die Vernichtung von privaten Schlüsseln der Endteilnehmer obliegt diesen bzw. dem Mandanten selbst.

6.2.11 Bewertung kryptographischer Module

Siehe Kapitel 6.2.1.

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Im Rahmen der regelmäßigen Sicherungsmaßnahmen von Telekom Security werden die Zertifikate (CA-, Root-CA-, Endteilnehmer-Zertifikate) gesichert und archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Zertifikatsgültigkeit beginnt mit der Generierung des Zertifikats und endet mit Ablauf des Gültigkeitszeitraums oder durch Sperrung. Die Gültigkeitsdauer von Schlüsselpaaren entspricht der Gültigkeitsdauer des zugehörigen Zertifikats. Die Zertifikate können jedoch weiterhin zur Entschlüsselung und Signaturvalidierung verwendet werden, sofern der dazu passende private Schlüssel vorliegt.

In Tabelle 20 bis Tabelle 23 sind die maximalen Gültigkeitszeiträume der in der Hierarchie beteiligten Zertifikate dargestellt, die zum Zeitpunkt des Inkrafttretens dieser CPS ausgestellt wurden.

Telekom Security stellt sicher, dass die CA- und Root-CA-Zertifikate vor Ablauf ausgewechselt werden, um die entsprechende Zertifikatsgültigkeit von Endteilnehmer-Zertifikaten gewährleisten zu können.

Tabelle 20: Gültigkeit von Root-CA-Zertifikaten (Teil 1)

Zertifikatstyp:	T-TeleSec GlobalRoot Class 2
Gültigkeit:	25 Jahre

Tabelle 21: Gültigkeit von Root-CA-Zertifikaten (Teil 2)

Zertifikatstyp:	Deutsche Telekom Internal Root CA 1, Deutsche Telekom Internal Root CA 2
Gültigkeit:	20 Jahre

Tabelle 22: Gültigkeit von Sub-CA-Zertifikaten

Zertifikatstyp:	TeleSec Business CA 1, Internal Business CA 2, Internal Business CA 3, Internal Business CA 5, Business CA
Gültigkeit:	12 Jahre bzw. mindestens 12 Jahre

Tabelle 23: Gültigkeit von Endteilnehmer-Zertifikaten

Zertifikatstyp:	Alle Endteilnehmer-Zertifikate (Master- und Sub-Registrator inkl. Derivate, Benutzer, Geräte)
Gültigkeit:	Standardmäßig 12, 24 oder 36 Monate (bzw. 1, 2 oder 3 Jahre), nach Vereinbarung kann eine abweichende Laufzeit von x Monate administriert werden. Hinweis: Die Zertifikatsgültigkeit wird bei der Einrichtung der Master-Domäne festgelegt und vererbt sich auch auf die Zuständigkeitsbereiche

	(Sub-Domänen). Innerhalb der Master-Domäne sind bei gleicher Namensgebung keine unterschiedlichen Gültigkeitszeiträume möglich. Für Server-Zertifikate, ausgestellt von einer öffentlichen Zertifizierungsstelle (Kapitel 1.3.1.2.1), gilt: ▪ Bis zum 31.08.2020: max 825 Tage oder 27 Monate ▪ Ab dem 01.09.202: max. 398 Tage oder 13 Monate

Tabelle 24: Gültigkeit von OCSP-Zertifikaten

Zertifikatstyp:	OCSP-Signer T-TeleSec GlobalRoot Class 2
Gültigkeit:	Max. 6 Monate
Zertifikatstyp:	OCSP-Signer je Sub-CA (Kapitel 1.3.1.2 ff)
Gültigkeit:	Max. 6 Monate

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

6.4.1.1 Telekom Security

Um die auf dem HSM hinterlegten privaten Schlüssel der CA- und Root-CA-Zertifikate schützen zu können, werden Aktivierungsdaten (Geheimnisanteile) nach dem in Kapitel 6.2.2 dieser CPS beschriebenen Anforderungen und dem Dokument „Key Ceremony“ generiert. Die Erstellung und Verteilung von Geheimnisanteilen werden protokolliert.

6.4.1.2 Externe Registrierungsstelle

Abhängig von den Eingabemedien (z.B. PC-Tastatur, Tastatur eines Smartcard-Lesers) empfiehlt Telekom Security zum Export von Soft-PSE oder Aktivierung/Nutzung des privaten Schlüssels die Vergabe von sicheren Passwörtern oder Kennphrasen, die folgender Syntax entsprechen:

- Zeichenlänge von mindestens 8 alphanumerischen Ziffern und Zeichen inkl. Sonderzeichen wie !, ?; /, usw.
- Groß- und Kleinschreibung,
- keine gängigen Bezeichnungen die in Lexika zu finden sind,
- keine Benutzernamen.

6.4.2 Schutz von Aktivierungsdaten

6.4.2.1 Telekom Security

Die Trust-Center-Administratoren bzw. autorisierte Personen der Telekom Security verpflichten sich, die Geheimnisanteile für die Aktivierung der privaten Schlüssel der CA-, Root-CA und OCSP-Zertifikate zu schützen.

6.4.2.2 Externe Registrierungsstelle

Die Durchsetzung des Schutzes nach Kapitel 6.4.1 obliegt der Verantwortung des Mandanten.

Für die Ausstellung des Sub-Registrator-Zertifikats gelten die Regelungen wie in Kapitel 6.1.1 beschrieben. Für die Nutzung von Smartcards ist mindestens eine 6-stellige PIN und eine 8-stellige PUK zu vergeben.

Bei der Nutzung einer Software-PSE empfiehlt Telekom Security folgende Regelungen:

- Beim Exportieren ist die Datei mit einem sicheren Passwort zu versehen und in sicherer Umgebung zu speichern.
- Beim Importieren dieser Datei ist die Funktion „Schlüssel als exportierbar markieren“ zu deaktivieren, die Funktion „Hohe Sicherheit für den privaten Schlüssel“ und die Sicherheitsstufe „hoch“ zu aktivieren, damit ein entsprechendes schwierig zu erratendes Passwort vergeben werden kann. Damit wird ein einfacher Export der Soft-PSE verhindert und bei der Nutzung des privaten Schlüssels (z.B. Signaturvorgang, Entschlüsselung) eine Passwortabfrage unterstützt.

  Hinweis: Alle o.g. Beschreibungen zum Import privater Schlüssel sind abhängig vom Browser und kann daher abweichen.

Der Mandant kann sich bei den Endteilnehmern eine schriftliche Bestätigung mit dem Umgang der Aktivierungsdaten einholen.

Zur Erhöhung der Sicherheit empfiehlt Telekom Security eine regelmäßige Änderung von Kennphrase bzw. PIN der Endteilnehmer-Zertifikate.

6.4.3 Weitere Aspekte von Aktivierungsdaten

6.4.3.1 Übertragung von Aktivierungsdaten

Sofern Aktivierungsdaten für private Schlüssel, unabhängig vom Übertragungsmedium, übertragen werden, müssen die Trust-Center-Administratoren die Übertragung mithilfe von Methoden zum Schutz gegen Verlust, Diebstahl, Änderung, unbefugter Offenlegung oder Nutzung dieser privaten Schlüssel schützen.

Bei der Verwendung der Kombination von Benutzername und Passwort zur Anmeldung an Netzwerken als Aktivierungsdaten für einen Endteilnehmer, müssen die in einem Netzwerk zu übertragenen Kennwörter ebenfalls gegen den Zugriff durch unbefugte Benutzer geschützt werden.

6.4.3.2 Vernichtung von Aktivierungsdaten

Nach dem Löschen der privaten Schlüssel (Kapitel 6.2.10) sind die Aktivierungsdaten nicht mehr schützenswert.

6.5 Computer-Sicherheitskontrollen

Telekom Security führt alle PKI-Funktionen mit Hilfe vertrauenswürdiger und geeigneter Systeme durch. Die Systeme werden von Monitoring-Systemen fortlaufend auf Funktion und Kapazität geprüft, so dass im Bedarfsfall zeitnah eine Erweiterung von Ressourcen durchgeführt werden kann.

Die im Monitoring (periodisch alle 5 Minuten) erhobenen Daten zu CPU-, Speicher- und Disk-Auslastung sind mit Warn- und Alarm-Schwellen versehen. Spätestens mit Eintreten der Warn-Stufe wird die Ressourcen-Planung geprüft und ggf. durch Erweiterungen (z.B. Hardware-Nachrüstung, Verlagerung von Diensten auf andere Systeme oder Zuweisung von weiteren Ressourcen an virtuelle Maschinen) angepasst.

Die Sicherheitsmaßnahmen für Computer der Zertifizierungsstelle (z.B. Netzwerksicherheit, Zugriffskontrolle, Überwachung etc.) sind im Sicherheitskonzept [SBCA Siko] beschrieben. Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.4 umgesetzt.

Die Systeme für Entwicklung, Test (SBCA-TU) und Produktion (SBCA-PU) sind vollkommen getrennt voneinander aufgebaut, sie befinden sich auf unterschiedlicher Hardware in verschiedenen Netzsegmenten, so dass eine gegenseitige Beeinflussung ausgeschlossen ist.

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

6.5.1.1 Telekom Security

Telekom Security stellt sicher, dass die Verwaltung der CA-Systeme vor unbefugtem Zugriff Dritter gesichert ist. Die CA-Komponenten sind räumlich und logisch von anderen Systemen getrennt und sind nur von autorisiertem Personal zugängig. Es werden aktuelle Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, 4-Augen-Prinzip) eingesetzt, um die CA-Funktionalitäten, Verzeichnisdienste und OCSP-Responder vor internen und externen Eindringligen zu schützen. Die CA verwendet auf Netzwerksebene implementierte Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS), die unnormale oder unautorisierte Zugriffsversuche erkennen und alarmieren. Der direkte Zugriff auf CA-Datenbanken, die die CA-Funktionalitäten unterstützen, ist auf geeignetes, geschultes und vertrauenswürdiges Betriebspersonal beschränkt.

Die Sicherheitsmaßnamen umfassen

- Physikalische Sicherheit und Sicherung der Umgebung,
- Die CA-Systeme sind so konfiguriert, dass nicht benötigte Ports, Accounts, Anwendungen, Services und unsichere Kommunikations-Protokolle entweder deaktiviert oder entfernt wurden,
- Maßnahmen zum Schutz der Systemintegrität, die mindestens aus Konfigurationsmanagement, Schutz von Sicherheitsanwendungen und Malware-Erkennung und -verhinderung bestehen,
- Netzwerksicherheit und Firewall Management, inklusive Portsperren und IP Adressfilterung, als auch Intrusion Detection System (IDS) und Intrusion-Prevention-Systeme (IPS),
- Benutzerverwaltung, Berechtigungsmatrix, Aufklärung, Sensibilisierung und Schulung/Ausbildung sowie
- Verfahrenskontrollen, Aktivitätsprotokollierung und Abschaltung bei Timeouts.

Auf den Systemen des Trust Centers werden Betriebssysteme eingesetzt, die die Durchsetzung von Sicherheitseinstellungen unterstützen. Keines der Systeme kann ohne Benutzeranmeldung verwendet werden.

Sicherheitskritische Einstellungen (beispielsweise Nutzkonten) werden nur im 4-Augen-Prinzip verändert werden. Die Durchsetzung der Zugangsbeschränkungen an den Systemen wird durch die umgesetzte restriktive Password Policy unterstützt.

Besonders sicherheitskritische Applikationen (beispielweise die Zertifikatsgenerierung) erfordern zusätzliche Authentisierungen des Bedieners im Trust Center.

PC-Arbeitsplätze, an denen die Ausstellung von Zertifikaten autorisiert wird, sind durch Multi-Faktor-Authentisierung abgesichert.

Der TSP lässt einen Penetrationstest (PEN-Test) an den TSP-Systemen durchführen

- bei der Einrichtung,
- umfangreichen Upgrades oder Änderungen der Infrastruktur oder der Anwendungen,
- mindestens aber ein Mal pro Jahr,

die der TSP als wesentlich erachtet.

Der TSP erbringt den Nachweis, dass jeder Penetrationstest von einer Person oder Organisation durchgeführt wurde, die über die erforderlichen Fähigkeiten, Werkzeuge, Kenntnisse, ethischen Grundsätze und Unabhängigkeit verfügt, um einen zuverlässigen Bericht erstellen zu können.

6.5.1.2 Externe Registrierungsstelle

Die Verwaltung der Master-Domäne (PKI-Mandant) durch den Master- und Sub-Registrator (inkl. Derivate) erfolgt über einen PC-Arbeitsplatz, den der Mandant eigenverantwortlich betreibt.

Für die Master- und Sub-Registratoren erhält der Mandant bzw. externe Registrierungsstelle von Telekom Security vertrauenswürdige und geeignete Hardware- und Software-Komponenten zur Bedienung der Registrator-Funktionalitäten auf den Registrator-PCs.

Die Sicherheitsmaßnahmen für Computer des Mandanten (beauftragte Drittpartei (Delegated Third Party) bzw. externe Registrierungsstelle ist beschrieben im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen der TeleSec Shared-Business-CA (SBCA)“ [SBCA PITR].

Ferner empfiehlt Telekom Security die Verwendung von Kennwörtern wie in Kapitel 6.4.1 beschrieben.

6.5.2 Bewertung der Computersicherheit

Nach jeder signifikanten System- oder Netzwerkänderung erfolgt innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan).

Die Schwachstellenprüfungen 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 einer Schwachstellenprüfung mit Angabe der Qualifikation der prüfenden Person oder Organisation wird durch das ISMS kontrolliert und zusammen mit den Ergebnissen dokumentiert.

Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen festgelegt und in einem definierten Plan umgesetzt.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Wenn eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

Zusätzlich werden einmal jährlich oder bei signifikanten Änderungen nach System- oder Netzwerkänderung sogenannte Penetrationstests (PEN-Test) durchgeführt. Auch hier werden entsprechend Maßnahmen abgeleitet und umgesetzt, sofern dies notwendig ist. Die PEN-Tests 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 eines PEN-Test wird mit Angabe der Qualifikation der prüfenden Person oder Organisation wird durch das ISMS kontrolliert und zusammen mit den Ergebnissen dokumentiert.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Systementwicklungskontrollen

Telekom Security hat Mechanismen und Kontrollen implementiert, um eingekaufte, entwickelte oder veränderte Software auf Schadelemente oder bösartigen Code (z.B. Trojaner, Viren) überwachen und schützen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Neue Software-Versionen der Software (geplante Updates) oder Fehlerbeseitigungen (kurzfristige Bugfixes) werden zunächst auf einem Entwicklungssystem des Herstellers/Entwicklers bereitgestellt und getestet.

Nach erfolgreicher Prüfung der Software in der Entwicklungsumgebung wird eine Software-Package des Herstellers erzeugt, das auf einem Testsystem (Test-Umgebung, Test Unit) im Netz bzw. Lokation der Telekom Security befindet (SBCA-TU).

Erst nach erfolgreichen Tests auf dem Testsystem erfolgt die Installation auf dem Wirksystem (SBCA-PU) der Telekom Security im georedundanten Rechenzentrum der Telekom Security.

Das bei der Telekom Security etablierte Change- und Release-Management findet Anwendung.

Die Verwaltung der PKI-Systeme (CA, HSM, Web-Server, …) durch die Trust-Center-Administratoren (Systemadministratoren) erfolgt über ein getrenntes Netz das ausschließlich diesen Rolleninhabern zur Verfügung steht [SBCA Siko] und [SRK TC]. Die Verwaltung anderer IT-Systeme (nicht PKI-Systems) über dieses Netz ist unzulässig.

6.6.2 Sicherheitsverwaltungskontrollen

Telekom Security hat Mechanismen und/oder Richtlinien implementiert, um die Konfiguration seiner CA-Systeme kontinuierlich zu kontrollieren und überwachen zu können.
Die Integrität der Systeme inklusive ihrer relevanten (Konfigurations-)Einstellungen wird kontinuierlich auf Änderungen überwacht. Bei Änderungen, die nicht auf Basis eines autorisierten Change durchgeführt wurden, wird den daraus resultierenden Alarmmeldungen durch qualifiziertes Personal nachgegangen.

Die Integrität wird vor der Installation manuell verifiziert.

Die Systemkonten (System Accounts) der Trust-Center-Administratoren werden spätestens nach 90 Kalendertagen überprüft. Nicht mehr benötigte Accounts werden deaktiviert.

6.6.3 Sicherheitskontrollen des Lebenszyklus

Telekom Security hat Mechanismen und Kontrollen implementiert, dass Sicherheitspatches innerhalb einer angemessenen Zeit, nachdem sie verfügbar sind, installiert werden. Die Integrität des Sicherheitspatchs wird vor der Installation manuell verifiziert.

Ein Sicherheitspatch wird nicht installiert, wenn zusätzliche Sicherheitslücken oder Instabilitäten entstehen, die die Vorteile der Anwendung des Sicherheitspatchs überwiegen. Der Grund für die Nichtanwendung von Sicherheitspatchs wird dokumentiert.

6.7 Netzwerk-Sicherheitskontrollen

Folgende Netzwerk-Sicherheitsmaßnahmen sind für den Dienst TeleSec Shared-Business-CA implementiert:

- Die Netzwerke des Zertifizierungsdienstes sind durch mehrstufige Firewalls abgesichert und in verschiedene Sicherheitszonen eingestuft.
- Sicherheitskritische Komponenten und Systeme, die vom Internet aus erreichbar sind (z.B. Verzeichnisdienst, OCSP-Responder), werden durch Firewalls von Internet und den internen Netzen getrennt. Alle anderen sicherheitskritischen Komponenten und Systeme (z.B. CA, DB, Signer) befinden sich in separaten Netzen, oder, im Falle der Offline-CA, ohne jegliche Netzanbindung.
- Die internen Netzwerke des Zertifizierungsdienstes sind nach dem Schutzbedarf der Systeme und Komponenten aufgeteilt und untereinander durch Firewalls getrennt.
- In regelmäßigen Abständen werden Schwachstellenüberprüfungen durchgeführt. Weitere Details sind in Kapitel 5.4.8 beschrieben.
- Alle berechtigten Nutzer müssen sich gegenüber den Systemen mit festgelegten Mechanismen authentifizieren, nicht mehr benötigte Accounts werden gelöscht oder deaktiviert.

- Das Trust Center ist georedundant über getrennte Zuführungen sowohl mit der Telematik-Infrastruktur als auch mit dem Internet verbunden. Ein Übergang von der Telematik-Infrastruktur ins Internet oder umgekehrt wird durch mehrere Firewallsysteme verhindert.

Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.8 umgesetzt.

6.8 Zeitstempel

Zertifikate, Sperrlisten, Online-Statusprüfungen und andere wichtige Informationen enthalten Datums- und Zeitinformationen, die aus einer zuverlässigen Zeitquelle abgeleitet werden (siehe Kapitel 5.5.5). Ein kryptografischer Zeitstempel wird nicht verwendet.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofil

Die von Telekom Security ausgestellten Zertifikate entsprechen folgenden Anforderungen:

- [RFC5280]
- [X.509]
- [CAB-BR]
- [ETSI NCP OVCP]

X.509.v3-Zertifikate müssen mindestens die in Tabelle 25 aufgeführten Inhalte aufweisen.

Tabelle 25: Zertifikatsattribute nach X509.v3

Feld:	**Wert oder Wertbeschränkung:**
Version:	Zertifikatsversion (Kapitel 7.1.1)
Zertifikats-Seriennummer:	Eindeutiger Wert zur Identifikation des Zertifikats. Die Zertifikats-Seriennummern werden von SBCA durch einen kryptographisch geeigneter Zufallszahlengenerator (CSPRNG) als mindestens 64-Bit-lange Zufallswerte (Entropie) generiert. Bei Server-Zertifikaten beträgt der Zufallswert (Entropie) 126 Bit.
Signaturalgorithmus:	RSA – SHA-256, RSASSA-PSS – SHA256 oder RSA – SHA-1 (abhängig von der ausstellenden Sub-CA (siehe Kapitel 1.3.1.2.1 und 1.3.1.2.2)
Aussteller:	Zertifizierungsstelle (Kapitel 1.3.1.2.1 und 1.3.1.2.2)
Gültig ab:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC5280 kodiert.
Gültig bis:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC5280 kodiert.
Antragsteller:	Eindeutiger Name (Kapitel 7.1.4); Benutzer-Zertifikate: 3.1.1.1.13
Öffentlicher Schlüssel:	Gemäß RFC5280 kodiert
Erweiterungen:	**Verweis auf:**
Schlüsselverwendung:	Kapitel 7.1.2.1
Zertifizierungsrichtlinie:	Kapitel 7.1.2.2
Alternativer Antragstellername:	Kapitel 7.1.2.3
Basiseinschränkungen:	Kapitel 7.1.2.4
Erweiterte Schlüsselverwendung:	Kapitel 7.1.2.5
Sperrlistenverteilungspunkt:	Kapitel 7.1.2.6
Schlüsselkennung des Antragstellers:	Kapitel 7.1.2.7
Stellenschlüsselkennung:	Kapitel 7.1.2.8
Zugriff auf Stelleninformation:	Kapitel 7.1.2.9
Zertifikatsvorlagename:	Kapitel 7.1.2.10

Zusätzliche Erweiterungen und Eigenschaften werden in den folgenden Kapiteln ausführlicher erklärt.

7.1.1 Versionsnummer(n)

Die von der TeleSec Shared-Business-CA ausgestellten X.509-Zertifikate für Endteilnehmer entsprechen der z. Zt aktuellen Version 3. Die zusätzlichen Erweiterungen und Eigenschaften werden in den folgenden Kapiteln ausführlicher erklärt.

Die CA- und Root-CA-Zertifikate sind ebenfalls vom Typ X.509v3.

7.1.2 Zertifikatserweiterungen

Um dem Standard X.509v3 zu erfüllen, ergänzt Telekom Security das Zertifikatsprofil um entsprechende Erweiterungen, die in den Kapiteln 7.1.2.1 bis 7.1.2.10 beschrieben sind.

Es können vom Mandanten selbst keine zusätzlichen Erweiterungen im Zertifikatsprofil aufgenommen werden.

7.1.2.1 Erweiterung „Schlüsselverwendung (KeyUsage)"

Die Schlüsselverwendung richtet sich nach den Regeln des RFC5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" und ist darin beschrieben.

In Tabelle 26 bis Tabelle 29 ist die Erweiterung „Schlüsselverwendung" den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Tabelle 26: Zuordnung der Erweiterung „Schlüsselverwendung" (Key Usage), Teil 1

Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Dual Key
Verwendung:	Je ein getrenntes Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	digitalSignature (Bit 0)
Hex-Wert:	80
Bezeichnung:	keyEncipherment (Bit 2)
Hex-Wert:	20
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Triple Key
Verwendung:	Je ein eigenes Zertifikat für Signatur, Verschlüsselung und LogOn
Bezeichnung:	digitalSignature (Bit 0)
Hex-Wert:	80
Bezeichnung:	keyEncipherment (Bit 2)
Hex-Wert:	20
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0

Tabelle 27: Zuordnung der Erweiterung „Schlüsselverwendung" (Key Usage), Teil 2

Zertifikatstyp:	**Server**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation und Verschlüsselung
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0
Zertifikatstyp:	**Mail-Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung

Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0
Zertifikatstyp:	**Router/Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0
Zertifikatstyp:	**Domain-Controller**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2) und dataEncipherment (Bit 3)
Hex-Wert:	B0

Tabelle 28: Zuordnung der Erweiterung „Schlüsselverwendung“ (Key Usage), Teil 3

Zertifikatstyp:	**Master-Registrator**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0
Zertifikatstyp:	**Sub-Registrator und Derivate**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	digitalSignature (Bit 0) und keyEncipherment (Bit 2)
Hex-Wert:	A0

Tabelle 29: Zuordnung der Erweiterung „Schlüsselverwendung“ (Key Usage), Teil 4

Zertifikatstyp:	**Stammzertifizierungsstelle (Root-CA)**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur von Zertifikatsschlüssel und CRL-Signatur
Bezeichnung:	keyCertSign (Bit 5) und CRLSign (Bit 6)
Hex-Wert:	06
Zertifikatstyp:	**Zwischenzertifizierungsstelle (Sub-CA)**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur von Zertifikatsschlüssel und CRL-Signatur
Bezeichnung:	keyCertSign (Bit 5) und CRLSign (Bit 6)
Hex-Wert:	06
Zertifikatstyp:	**OCSP**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Nichtabstreitbarkeit
Bezeichnung:	digitalSignature (Bit 0) und nonRepudiation (Bit 1)
Hex-Wert:	C0

Der Risikowert dieser Erweiterung ist als „kritisch“ gesetzt.

Auf Kundenwunsch kann das Zertifikatsprofil (außer für CA-Zertifikate) mit der Erweiterung „Schlüsselverwendung“ um weitere Werte (z.B. dataEncipherment) aus og. Tabelle ergänzt werden.

Im Falle, dass die Schlüsselverwendung als „unkritisch“ deklariert ist, besteht eine erweiterte Schlüsselverwendung (Extended Key Usage), die „kritisch“ markiert ist.

Obwohl das nonRepudiation-Bit in der Erweiterung „Schlüsselverwendung“ nicht gesetzt ist, unterstützt Telekom Security dennoch die Nichtabstreitbarkeit für diese „fortgeschrittenen“ Signatur-Zertifikate. Es ist z. Zt. nicht unbedingt erforderlich, das nonRepudiation-Bit in diesem Zertifikatstyp zu setzen, da die PKI-Industrie noch keinen Konsens darüber erzielt hat, welche Bedeutung das nonRepudiation-Bit tatsächlich hat. Bis ein solcher Konsens erzielt wird, hat das nonRepudiation-Bit für potenzielle Vertrauende Dritte keine Bedeutung.

Darüber hinaus werten die gängigsten Anwendungen (z.B. E-Mail) das nonRepudiation-Bit nicht. Aus diesem Grunde ist eine Definition des Bits für Vertrauende Dritte bei der Entscheidung über die Vertrauenswürdigkeit nicht hilfreich.

7.1.2.2 Erweiterung „Zertifizierungsrichtlinien (Certificate Policies)”

Die Erweiterung „Zertifizierungsrichtlinie“ besteht aus Objekt-Kennungen (Object Identifier, OID, siehe auch Kapitel 7.1.6) und einer URL, hinter der diese CPS abrufbar ist. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.3 Erweiterung „alternativer Antragstellername (subjectAltName)”

In Tabelle 30 ist die Erweiterung „alternativer Antragstellernamen“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Tabelle 30: Zuordnung der Erweiterung „alternativer Antragstellername (subjectAltName)“

Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	RFC822-Name, optional: User Principal Name
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Dual Key
Verwendung:	Je ein getrenntes Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	RFC822-Name, optional: User Principal Name
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Triple Key
Verwendung:	Je ein eigenes Zertifikat für Signatur, Verschlüsselung und LogOn
Bezeichnung:	RFC822-Name, User Principal Name
Zertifikatstyp:	**Server**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation und Verschlüsselung
Bezeichnung:	Ein bis mehrere DNS-Namen
Zertifikatstyp:	**Mail-Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	RFC822-Name
Zertifikatstyp:	**Router/Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation
Bezeichnung:	RFC822-Name, IP-Adresse, optional: DNS-Name

Zertifikatstyp:	**Domain-Controller**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation
Bezeichnung:	RFC822-Name, DNS-Name, Other Name (DS-Objekt-Guid)

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.4 Erweiterung „Basiseinschränkungen (BasicConstraints)”

Die Erweiterung „Basiseinschränkung“ definiert folgende Inhalte

- Benutzertyp (subjectTyp) und
- Beschränkung des Zertifizierungspfades (pathLenConstraint)

Der Benutzertyp gibt an, ob das ausgestellt Zertifikat für einen Endteilnehmer (cA = false) oder Zertifizierungsstellen (CA) bestimmt ist.

Die Einschränkung des Zertifizierungspfads gibt an, wie viele Zertifizierungsstellen in der Zertifikatshierarchie höchstens vorkommen dürfen.

In Abbildung 1 sind die vom PKI-Service „TeleSec Shared-Business-CA“ genutzten Root- und Sub-CA-Zertifikate dargestellt. Der PKI-Service „TeleSec Shared-Business-CA“ stellt kein weiteres Sub-CA-Zertifikat aus, das hierarchisch einer der dargestellten Sub-CAs untersteht.

Tabelle 31: Zuordnung der Erweiterung „Basiseinschränkungen“ (Basic Constraints)

Zertifikatstyp:	**Stammzertifizierungsstelle (Root-CA)**
Zertifikatsname:	T-TeleSec GlobalRoot Class 2
Beschränkung des Zertifizierungspfades:	Keine
Zertifikatstyp:	**Stammzertifizierungsstelle (Root-CA)**
Zertifikatsname:	Deutsche Telekom Internal Root CA 1
Beschränkung des Zertifizierungspfades:	1
Zertifikatstyp:	**Stammzertifizierungsstelle (Root-CA)**
Zertifikatsname:	Deutsche Telekom Internal Root CA 2
Beschränkung des Zertifizierungspfades:	Keine
Zertifikatstyp:	**Zwischenzertifizierungsstelle (Sub-CA)**
Zertifikatsname:	TeleSec Business CA 1
Beschränkung des Zertifizierungspfades:	0
Zertifikatstyp:	**Zwischenzertifizierungsstelle (Sub-CA)**
Zertifikatsname:	Internal Business CA 2
Beschränkung des Zertifizierungspfades:	0
Zertifikatstyp:	**Zwischenzertifizierungsstelle (Sub-CA)**
Zertifikatsname:	Internal Business CA 3
Beschränkung des Zertifizierungspfades:	0
Zertifikatstyp:	**Zwischenzertifizierungsstelle (Sub-CA)**
Zertifikatsname:	Internal Business CA 5
Beschränkung des Zertifizierungspfades:	0
Zertifikatstyp:	**Zwischenzertifizierungsstelle (Sub-CA)**
Zertifikatsname:	Business CA
Beschränkung des Zertifizierungspfades:	0
Zertifikatstyp:	**Endeinheit**

Zertifikatsname:	Diverse Endteilnehmer (Benutzer, Geräte, Registratoren, OCSP)
Beschränkung des Zertifizierungspfades:	Keine

Der Risikowert dieser Erweiterung ist für alle Zertifizierungsstellen als „kritisch“, der für alle Endteilnehmer als „unkritisch“ gesetzt.

7.1.2.5 Erweiterung „Erweiterte Schlüsselverwendung (ExtendedKeyUsage)”

In Tabelle 32 und Tabelle 33 sind die erweiterten Schlüsselverwendungen den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Tabelle 32: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung“ (Extended Key Usage), Teil 1

Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	Secure E-Mail (1.3.6.1.5.5.7.3.4) oder Client authentication (1.3.6.1.5.5.7.3.2) oder beide Werte
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Dual Key
Verwendung:	Je ein getrenntes Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	Secure E-Mail (1.3.6.1.5.5.7.3.4) oder Client authentication (1.3.6.1.5.5.7.3.2) oder beide Werte
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Triple Key
Verwendung:	Je ein eigenes Zertifikat für Signatur, Verschlüsselung und LogOn
Bezeichnung für Signatur / Verschlüsselung:	Secure E-Mail (1.3.6.1.5.5.7.3.4) oder Client authentication (1.3.6.1.5.5.7.3.2) oder beide Werte
Bezeichnung für LogOn:	Client authentication (1.3.6.1.5.5.7.3.2) und MS SmartcardLogon (1.3.6.1.4.1.311.20.2.2)

Tabelle 33: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung“ (Extended Key Usage), Teil 2

Zertifikatstyp:	**Server**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation und Verschlüsselung
Bezeichnung:	Server authentication (1.3.6.1.5.5.7.3.1) oder Client authentication (1.3.6.1.5.5.7.3.2) oder beide Werte
Zertifikatstyp:	**Mail-Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Bezeichnung:	Secure E-Mail (1.3.6.1.5.5.7.3.4)
Zertifikatstyp:	**Router/Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation
Bezeichnung:	Kein Wert gesetzt
Zertifikatstyp:	**Domain-Controller**
Zertifikats-Template:	Single Key

Verwendung:	Ein Zertifikat für Authentifikation
Bezeichnung:	Server authentication (1.3.6.1.5.5.7.3.1) und Client authentication (1.3.6.1.5.5.7.3.2)
Zertifikatstyp:	**OCSP**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Nichtabstreitbarkeit
Bezeichnung:	OCSPSigning (1.3.6.1.5.5.7.3.9)

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt. Auf Kundenwunsch kann diese Erweiterung als „kritisch“ markiert werden.

Registrator-Zertifikate erhalten keine „Erweiterte Schlüsselverwendung“.

7.1.2.6 Erweiterung „Sperrlistenverteilungspunkt (CRLDistributionPoints)”

Alle Endteilnehmer-Zertifikate verfügen über einen Sperrlistenverteilungspunkt, über dessen URL (HTTP und teilweise LDAP) die aktuelle und zugehörige Zertifikatssperrliste (CRL) abrufbar ist. Vertrauende Dritte benötigen diese URL zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Das CA-Zertifikat verfügt ebenfalls über einen Sperrlistenverteilungspunkt, über dessen URL (HTTP und LDAP) die aktuelle Sperrliste für Zertifizierungsstellen (CARL) auf dem Verzeichnisdienst abrufbar ist. Vertrauende Dritte benötigen diese zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Die Root-CA-Zertifikate enthalten keinen Sperrlistenverteilungspunkt.

7.1.2.7 Erweiterung „Schlüsselkennung des Antragstellers (subjectKeyIdentifier)”

In allen Endteilnehmer- und Registrator-Zertifikaten enthält die Erweiterung „Schlüsselkennung des Antragstellers“ als Attributswert SHA-1 Hashwert, der individuell aus dem jeweiligen öffentlichen Schlüssel gebildet wird.

Die Erweiterung „Schlüsselkennung des Antragstellers“ des TeleSec Shared-Business-CA-Zertifikats enthält als Attributswert einen SHA-1 Hashwert, der aus dem öffentlichen Schlüssel der TeleSec Shared-Business-CA gebildet wird. Dieser Wert stimmt mathematisch mit dem Wert der Erweiterung „Stellenschlüsselkennung“ (siehe Kapitel 7.1.2.8) des Endteilnehmer- und Registrator-Zertifikats überein.

Es gelten ebenfalls die Regelungen der jeweiligen hierarchisch übergeordneten Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.8 Erweiterung „Stellenschlüsselkennung (authorityKeyIdentifier)”

In Endteilnehmer- und Registrator-Zertifikaten enthält die Erweiterung „Stellenschlüsselkennung“ als Attributswert einen SHA-1-Hashwert, der mit dem Wert der Erweiterung „Schlüsselkennung des Antragstellers“ (siehe Kapitel 7.1.2.7) des Zertifikats der hierarchisch übergeordneten Zertifizierungsinstanz (CA) mathematisch übereinstimmt.

Es gelten ebenfalls die Regelungen der jeweiligen hierarchisch übergeordneten Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.9 Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)”

7.1.2.9.1 Endteilnehmer-Zertifikate

In Endteilnehmer- und Registrierungsstellenmitarbeiter-Zertifikaten enthält die Erweiterung „Zugriff auf Stelleninformation“ die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch HTTP-URL des jeweiligen OCSP-Responders.

- Endteilnehmer-Zertifikat ausgestellt von
  - Telesec Business CA 1: http://ocsp03.sbca.telesec.de/ocspr
  - Business CA: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 2: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 3: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 5: http://ocsp.telesec.de/ocspr

Zertifikate, die nach dem 26.02.2018 ausgestellt wurden, enthalten zusätzlich die Pfadangabe (HTTPS) des jeweiligen Sub-CA-Zertifikats. Die korrespondierende Objekt-Kennung (OID) lautet 1.3.6.1.5.5.7.48.2.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.9.2 Sub-CA-Zertifikate

In Zertifikaten von Zwischenzertifizierungsstellen enthält die Erweiterung „Zugriff auf Stelleninformation“ die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch HTTP-URL des jeweiligen OCSP-Responders.

- CA-Zertifikat
  - TeleSec Business CA 1: http://ocsp04.telesec.de/ocspr
  - Internal Business CA 2: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 3: http://ocsp-root.sbca.telesec.de/ocspr
  - Internal Business CA 5: http://ocsp.telesec.de/ocspr
  - Business CA: http://ocsp.sbca.telesec.de/ocspr

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.10 Erweiterung „Zertifikatsvorlagenname (Certificate Template Name)”

Für das Zertifikatsprofil „Domain-Controller“ ist die Erweiterung „Zertifikatsvorlagenamen“ belegt mit dem Namen „DomainController“.

7.1.3 Objekt-Kennungen (OIDs) - von Algorithmen

Innerhalb des PKI-Service „TeleSec Shared-Business-CA” stehen für das Signieren von Zertifikaten folgende Signatur-Algorithmen zur Verfügung:

- sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}, -> 1.2.840.113549.1.1.11
- sha-256WithRSASSA-PSS (Probabilistic Signature Scheme) OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}, -> 1.2.840.113549.1.1.10
- ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} -> 1.2.840.10045.4.3.2
- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}, -> 1.2.840.113549.1.1.5

Diese Signatur-Algorithmen beziehen sich auf alle Zertifikatstypen (Stammzertifizierungsstelle, Zwischenzertifizierungsstelle und Endteilnehmer).

Aus Sicherheitsgründen müssen alle Endteilnehmer-Zertifikate und Zertifikate der Zwischenzertifizierungsstelle (Sub-CA) den Signatur-Hash-Algorithmus SHA-256 verwenden.

Der Signatur-Hash-Algorithmus SHA-1 wird aus Sicherheitsgründen nicht mehr empfohlen und ist in Zertifikaten, die von einer öffentlichen Sub-CA ausgestellt werden, nicht zugelassen.

SHA-1 ist ausschließlich nur aus Interoperabilitätsgründen in Zertifikaten erlaubt, die von einer internen Sub-CA ausgestellt werden.

7.1.4 Namensformen

7.1.4.1 Informationen zum Aussteller

Alle von der „TeleSec Shared-Business-CA“ verwendeten CA-Zertifikate enthalten einen eindeutigen Ausstellernamen (Issuer-DN) (Kapitel 1.3.1.1 ff und 1.3.1.2 ff).

Die Endteilnehmer- und Registrator-Zertifikate der „TeleSec Shared-Business-CA“ enthalten einen, eindeutigen Ausstellernamen (Issuer-DN) der jeweiligen Zertifizierungsstelle (Kapitel 1.3.1.2.1 bis 1.3.1.2.2).

Der Name des Ausstellers in einem Zertifikat („Issuer-DN“) entspricht dem „Subject-DN“ des ausstellenden Zertifikats „Byte-für-Byte“.

7.1.4.2 Subject-Informationen der Endteilnehmer-Zertifikaten

Die Inhalte des Subject-DN (Antragsteller) von Endteilnehmer-Zertifikaten sind abhängig vom Zertifikatstyp (z.B. Benutzer, Server, Router/Gateway) und setzen sich wahlweise aus den Feldern wie in den Kapiteln 3.1.1.1.1 bis 3.1.1.1.13 beschrieben zusammen. Die Felder enthalten Pflichtangaben (mandatory), optionale oder automatisch erzeugte Angaben oder Vorbelegungen.

Sofern nicht alle Zertifikatsantragsdaten in den Subject-DN aufgenommen werden können, weil technische oder Interoperabilitätsbeschränkungen (z.B. Dateigröße des Zertifikats, nur ein OU-Eintrag) in Zertifikaten die Verwendung unmöglich machen, sind Abweichungen zu den vorangehenden Bestimmungen zulässig. Diese Zertifikate werden über die untergeordnete Zertifizierungsstelle (Sub-CA) „Business CA“ ausgestellt.

Die E-Mail-Adresse muss nicht zwingend Inhalt des Subject-DN sein, wenn sich diese in der Erweiterung „alternativer Antragstellername (subjectAltName) wiederfindet.

In Tabelle 34 sind die Bestandteile des Subject-DN und Subject Alternative Name für Endteilnehmer je Zertifikatstyp dargestellt.

Tabelle 34: Subject-DN- und Subject Alternative Name Angaben für Endteilnehmer je Zertifikatstyp

Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Vor und Nachname, Common Name (CN), E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatisch generierte Angaben im Subject:	Subject-DN Serial Number (SN)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3), User Principal Name (UPN), weitere E-Mail-Adressen
Eintrag im Subject Alternative Name:	Ein oder mehrere RFC822-Namen (Kapitel 3.1.1.2.1), optional: User Principal Name (Kapitel 3.1.1.2.2)
Zertifikatstyp:	**Benutzer**

Zertifikats-Template:	Dual Key
Verwendung:	Je ein getrenntes Zertifikat für Signatur und Verschlüsselung
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Vor und Nachname, Common Name (CN), E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatisch generierte Angaben im Subject:	Subject-DN Serial Number (SN)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3), User Principal Name (UPN), weitere E-Mail-Adressen
Eintrag im Subject Alternative Name:	Ein oder mehrere RFC822-Namen (Kapitel 3.1.1.2.1), optional: User Principal Name (Kapitel 3.1.1.2.2)
Zertifikatstyp:	**Benutzer**
Zertifikats-Template:	Triple Key
Verwendung:	Je ein eigenes Zertifikat für Signatur, Verschlüsselung und LogOn
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Vor und Nachname, Common Name (CN), E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatisch generierte Angaben im Subject:	Subject-DN Serial Number (SN)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3), weitere E-Mail-Adressen
Eintrag im Subject Alternative Name:	Ein oder mehrere RFC822-Namen (Kapitel 3.1.1.2.1), User Principal Name (Kapitel 3.1.1.2.2)
Zertifikatstyp:	**Server**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation und Verschlüsselung
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Locality Name (L), State or Province Name (St), Common Name (CN), E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatisch generierte Angaben im Subject:	Subject-DN Serial Number (SN)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3), weitere Servernamen, Street address, Postal code
Eintrag im Subject Alternative Name:	Ein bis mehrere DNS-Namen (Kapitel 3.1.1.2.3)
Zertifikatstyp:	**Mail-Gateway**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Signatur und Verschlüsselung
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Common Name (CN), E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3)
Eintrag im Subject Alternative Name:	RFC822-Name (Kapitel 3.1.1.2.1)
Zertifikatstyp:	**Router/Gateway**
Zertifikats-Template:	Single Key

Verwendung:	Ein Zertifikat für Authentifikation
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Common Name (CN), E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatisch generierte Angaben im Subject:	Subject-DN Serial Number (SN)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3), Unstructured Name
Eintrag im Subject Alternative Name:	IP-Adresse (Kapitel 3.1.1.2.49, RFC822-Name (Kapitel 3.1.1.2.1), optional: DNS-Name (Kapitel 3.1.1.2.3)
Zertifikatstyp:	**Domain-Controller**
Zertifikats-Template:	Single Key
Verwendung:	Ein Zertifikat für Authentifikation
Pflichtangaben im Subject:	Country Name (C), Organization Name (O), Common Name (CN), Microsoft GUID, E-Mail-Address (E)
Vorbelegungen im Subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Optionale Angaben im Subject:	Organizational Unit Name 3 (OU3)
Eintrag im Subject Alternative Name:	Anderer Name (Kapitel 3.1.1.2.5)

7.1.4.3 Subject-Informationen zu CA-Zertifikaten

Die Inhalte des Subject-DN (Antragsteller) von CA-Zertifikaten setzen sich wahlweise aus den Feldern wie in den Kapiteln 3.1.1.1.1 bis 3.1.1.1.13 beschrieben zusammen. Die Felder enthalten Pflichtangaben (mandatory) und ggf. optionale erzeugte Angaben.

Pflichtangaben enthalten folgende Felder:

- Country Name (C)
- Organization Name (O)
- Organizational Unit Name (OU)
- Common Name (CN)

Folgende Felder sind optional:

- StateOrProvince name (St)
- Locality (L)
- PostalCode
- StreetAddress (Street)

7.1.5 Namensbeschränkungen

TeleSec Shared-Business-CA betreibt keine Sub-CAs mit Namensbeschränkungen.

7.1.6 Objekt-Kennungen (OIDs) für Zertifizierungsrichtlinien

7.1.6.1 Objekt-Kennungen für „Root-CA-Zertifikate“

Die Root-CA-Zertifikate enthalten keine certificatePolicies Erweiterung.

7.1.6.2 Objekt-Kennungen für „Sub-CA-Zertifikate“

Alle CA-Zertifikat enthalten eine Erweiterung „Zertifizierungsrichtlinie (certificate policies)“. Neben der HTTP-URL findet sich folgende Objekt-Kennung für die CPS:

- policy OBJECT IDENTIFIER ::= {iso(1) iso identified organization(3) us department of defence(6) oid assignments(1) private(4) iana registrated private enterprises(1) T-TeleSec(7879) policy identifier(13) shared-business-ca(25)} -> 1.3.6.1.4.1.7879.13.25

Sub-CA-Zertifikate einer öffentlichen Zwischenzertifizierungsstelle (Kapitel 1.3.1.2.1) verwenden die in Kapitel 7.1.6.3.2 und/oder 7.1.6.3.3 dargestellte Policy-OID.

7.1.6.3 Objekt-Kennungen für „Endteilnehmer-Zertifikate“

7.1.6.3.1 Objekt-Kennungen der Zertifizierungsrichtlinie TeleSec Shared-Business-CA

Alle Endteilnehmer-Zertifikate inkl. Registrator-Zertifikate) enthalten eine Erweiterung „Zertifizierungsrichtlinie (certificate policies)“. Neben der HTTP-URL findet sich folgende Objekt-Kennung für die CPS:

policy OBJECT IDENTIFIER ::= {iso(1) iso identified organization(3) us department of defence(6) oid assignments(1) private(4) iana registrated private enterprises(1) T-TeleSec(7879) policy identifier(13) shared-business-ca(25)} -> 1.3.6.1.4.1.7879.13.25

7.1.6.3.2 Objekt-Kennungen für „Zertifizierungsrichtlinien der Baseline Requirements“

Vom CA/Browser Forum wurden in den Baseline Requirements [CAB-BR] folgende Policy-OIDs definiert:

- Domain Validation (DV): 2.23.140.1.2.1
- Organizational Validation (OV): 2.23.140.1.2.2
- Individual Validation (IV): 2.23.140.1.2.3
- Extended Validation (EV): 2.23.140.1.1

Alle Endteilnehmer-Zertifikate mit einem FQDN im Feld „Common Name” (Kapitel 3.1.1.1.7 und 3.1.1.2.3), die unter der Sub-CA „TeleSec Business CA 1“ ausgestellt werden, enthalten im Feld “Zertifizierungsrichtlinie (certificate policies)“ die folgende OID „Zertifizierungsrichtlinien der Baseline Requirements“:

- policy OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) subject-identity-validated(2)} -> 2.23.140.1.2.2

Für die, durch das CA/Browser-Forum in den [CAB-BR] definierten Policy-OIDs, gelten die folgenden Anforderungen, welche vom PKI-Dienst „TeleSec Shared-Business-CA“ eingehalten werden. Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.2 verwendet, müssen zwingend folgende Felder des Subject DN ausgefüllt sein:

- countryName (Kapitel 3.1.1.1.1)
- organizationName (Kapitel 3.1.1.1.2)
- localityName (Kapitel 3.1.1.1.9)
- stateOrProvinceName (Kapitel 3.1.1.1.10)

Die Policy-OIDs 2.23.140.1.2.1, 2.23.140.1.2.3 und 2.23.140.1.1 werden von „TeleSec Shared-Business-CA“ nicht verwendet, da keine DV-, IV- und EV-Zertifikate ausgestellt werden.

7.1.6.3.3 Objekt-Kennungen für „Zertifizierungsrichtlinien des ETSI“

Vom Europäische Institut für Telekommunikationsnormen (ETSI) wurden in den jeweiligen European Standards [ETSI NCP OVCP, ETSI EN TSP] folgende Policy-OIDs definiert:

- NCP: Normalized Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)} -> 0.4.0.2042.1.1
- NCP+: Normalized Certificate Policy OBJECT IDENTIFIER ::= {requiring a secure user device itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)} -> 0.4.0.2042.1.2
- LCP: Lightweight Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)} -> 0.4.0.2042.1.3
- EVCP: Extended Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)} -> 0.4.0.2042.1.4
- EVCP+: Extended Validation Certificate Policy requiring a secure user device OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcpplus (5)} -> 0.4.0.2042.1.5
- DVCP: Domain Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)} -> 0.4.0.2042.1.6
- OVCP: Organizational Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)} -> 0.4.0.2042.1.7
- IVCP: Individual Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ivcp (8)} -> 0.4.0.2042.1.8

Alle Endteilnehmer-Zertifikate mit einem FQDN im Feld „Common Name” (Kapitel 3.1.1.1.7 und 3.1.1.2.3) (z.B. Server-Zertifikate), die unter der Sub-CA „TeleSec Business CA 1“ ausgestellt werden, enthalten im Feld “Zertifizierungsrichtlinie (certificate policies)“ die folgende OID „Zertifizierungsrichtlinien der Baseline Requirements“:

- policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)} -> 0.4.0.2042.1.7

Alle Endteilnehmer-Zertifikate mit a.) einem Vor- und Nachnamen oder Präfix und FQDN im Feld „Common Name” (Kapitel 3.1.1.1.7 und 3.1.1.2.3) und b.) einer Mail-Adresse (Kapitel 3.1.1.1.8) und c.) einem RFC822-Namen (Kapitel 3.1.1.2.1) (z.B. Benutzer- und Mail-Gateway-Zertifikate), die unter der Sub-CA „TeleSec Business CA 1“ ausgestellt werden, enthalten im Feld “Zertifizierungsrichtlinie (certificate policies)“ die folgende OID „ETSI-Zertifizierungsrichtlinien“:

- policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)} -> 0.4.0.2042.1.1

Die Policy-OIDs 0.4.0.2042.1.2, 0.4.0.2042.1.3, 0.4.0.2042.1.4, 0.4.0.2042.1.5, 0.4.0.2042.1.6 und 0.4.0.2042.1.8 werden von „TeleSec Shared-Business-CA“ nicht verwendet, da keine NCP+, LCP, EVCP, EVCP+, DVCP und IVCP-Zertifikate ausgestellt werden.

7.1.7 Verwendung der Erweiterung „Richtlinienbeschränkungen (Policy Constraints)”

Nicht anwendbar.

7.1.8 Syntax und Semantik von Richtlinienkennungen

Es wird auf Kapitel 7.1.2.2 verwiesen. Es ist jeweils die aktuelle CPS hinterlegt. Ältere Versionen werden in entsprechender Ablage (Repository) abgelegt.

7.1.9 Verarbeitungssemantik der kritischen Erweiterung „Zertifikats-Richtlinien (critical Certificate Policies)”

Nicht anwendbar.

7.1.10 Subject-DN Serial Number (SN)

Weitere Informationen sind in Kapitel 3.1.1.1.13 dargestellt.

7.1.11 Objekt-Kennungen für „Certificate Transparency (CT)“

Für Server-Zertifikate, die unter einer öffentlichen Sub-CA ausgestellt werden (Kapitel 1.3.1.2.1), kann je PKI-Mandant optional die Funktion „Certificate Transparency (CT)“ aktiviert werden.

Nach der Ausstellung eine Server-Zertifikats mit CT-Funktion wird eine Erweiterung mit der OID „1.3.6.1.4.1.11129.2.4.2“ in das Zertifikat aufgenommen, das als Werte die jeweiligen „signed certificate timestamp“ (SCT) enthält.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.2 Sperrlistenprofil

Die von Telekom Security ausgestellten Sperrlisten entsprechen folgenden Anforderungen:

- [RFC5280]
- [X.509]

Zertifikatssperrlisten müssen mindestens die in Tabelle 35 aufgeführten Inhalte aufweisen.

Tabelle 35: Sperrlistenattribute nach X509.v2

Feld:	**Wert oder Wertbeschränkung:**
Version:	Sperrlistenversion (Kapitel 7.2.1)
Aussteller:	Zertifizierungsstelle (Kapitel 1.3.1.2.1 und 1.3.1.2.2)
Gültig ab (thisUpdate):	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC5280 kodiert.
Nächste Aktualisierung (nextUpdate):	Datum und Uhrzeit der nächsten geplanten Veröffentlichung.
Signaturalgorithmus:	RSA – SHA-256 oder RSA – SHA-1 (abhängig von der ausstellenden Sub-CA (siehe Kapitel 1.3.1.2.1 und 1.3.1.2.2)
Gesperrte Zertifikate:	Liste der gesperrten Zertifikate inkl. Seriennummer mit Sperrdatum- und zeitpunkt des gesperrten Zertifikats.

Erweiterungen:	**Verweis auf:**
Stellenschlüsselkennung:	Es gelten die Regelungengemäß Kapitel 7.2.2.1).
Sperrlistennummer:	Eindeutiger Wert (Kapitel 7.2.2.2)
Sperrgrund:	Kodierung des Sperrgrunds nach RFC5280 (Kapitel 7.2.2.3).

7.2.1 Versionsnummer(n)

Die von der TeleSec Shared-Business-CA ausgestellten X.509-Zertifikatssperrlisten entsprechen der Version 2.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

7.2.2.1 Erweiterung „Stellenschlüsselkennung (authorityKeyIdentifier)"

Die Sperrlisten enthalten die Erweiterung „Stellenschlüsselkennung" wie in Kapitel 7.1.2.8 beschrieben.

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.2.2.2 Erweiterung „Sperrlistennummer"

Die Sperrlisten enthalten die Erweiterung „Sperrlistennummer" als fortlaufende Seriennummer der Sperrliste.

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.2.2.3 Erweiterung „Sperrgrund" (Reason Code)

Bei der Sperrung von Zertifikaten muss zwingend ein Sperrgrund angegeben werden. Nach Tabelle 36 sind folgende Sperrgründe implementiert:

Tabelle 36: Erweiterung „Sperrgrund"

Eingabewert auf Webseite:	**Sperrgründe nach RFC5280:**	**Wert des Sperrgrundes nach RFC5280:**
Nicht spezifiziert	Nicht angegeben (unspecified)	0
Schlüssel kompromittiert	Schlüsselkompromittierung (keyCompromise)	1
Angaben im Zertifikat nicht mehr aktuell	Zuordnung geändert (affiliationChanged)	3
Zertifikat nach Erneuerung gesperrt	Abgelöst (superseded)	4

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.3 OCSP-Profil

OCSP (Online Certificate Status Protocol) stellt auf gleichnamiges Protokoll einen Validierungsdienst zur Verfügung, mit dessen Hilfe dem Vertrauenden Dritten eine zeitgerechte Information zum Sperrstatus von Endteilnehmer-Zertifikaten übermittelt wird.

Der eingesetzte OCSP-Responder erfüllt die Anforderungen des RFC6960.

7.3.1 Versionsnummer(n)

Es wird die Version 1 gemäß der OCSP-Spezifikation nach RFC6960 unterstützt.

7.3.2 OCSP-Erweiterungen

Das OCSP-Zertifikat, ausgestellt von der Zwischenzertifizierungsstelle (Sub-CA) (Übersicht siehe Abbildung 1), enthält in der X.509v3-Erweiterung „Erweiterter Schlüsselverwendung“ OCSPSigning mit der OID „1.3.6.1.5.5.7.3.9“. Zusätzlich ist die Erweiterung „OCSP noCheck“ (id-pkix-ocsp-nocheck) mit der OID 1.3.6.1.5.5.7.48.1.5 kodiert, die bedeutet, dass das OCSP-Zertifikat wird nicht validiert wird.

Die ArchiveCutOff Erweiterung wird nicht verwendet.

8 COMPLIANCE-AUDITS UND ANDERE PRÜFUNGEN

8.1 Intervall oder Gründe von Prüfungen

Die Stellen, die einem Audit, einer Überprüfung oder einer Untersuchung unterzogen werden, müssen Telekom Security und/oder einen beauftragten Dritten unterstützen.

Weiterhin ist Telekom Security berechtigt, die Durchführung dieser Audits, Überprüfungen und Untersuchungen auf Dritte (Kapitel 8.2) zu übertragen.

Die Telekom Security-Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319411-1, policy OVCP und policy NCP) unterzogen. Zertifizierungsgegenstand sind alle Prozesse, die zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (Kapitel 1.3.1.1.1 und 1.3.1.2.1) dienen.

Compliance-Audits finden in der Regel jährlich oder je nach Bedarf (Kapitel 8 ff) statt und werden auf Kosten der überprüften Stelle durchgeführt. Der Beginn dieser Maßnahme ist mindestens eine Woche vorher schriftlich anzukündigen. Audits werden über eine ununterbrochene Folge von Auditperioden durchgeführt, deren Zeitraum die Dauer von einem Jahr nicht überschreitet.

8.2 Identität/Qualifikation des Prüfers

Die Trust-Center-spezifischen Compliance-Audits werden von qualifizierten Mitarbeitern der Telekom Security oder einem Dritten (z.B. qualifiziertes Unternehmen wie TÜV IT) durchgeführt, die Erfahrung in den Bereichen Public-Key-Infrastructure-Technologie, Sicherheits-Auditing und Verfahren und Hilfsmittel der Informationssicherheit vorweisen können.

Für Auditoren, welche im Trust Center der Telekom Security ein Audit auf Anforderung eines oder mehrerer Anwendungssoftwareanbieter durchführen, gelten besondere Anforderungen. Für TeleSec Shared-Business-CA beauftragt das Trust Center einen für die ETSI-Zertifizierung akkreditierten Auditor. Dadurch ist die Einhaltung der besonderen Anforderungen (z.B. Qualifikation, Unabhängigkeit) an den Auditor gewährleistet.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die ETSI-Zertifizierungen handelt es sich um einen unabhängigen und qualifizierten Auditor (z.B. Wirtschaftsprüfer, Gutachter).

8.4 Abgedeckte Bereiche der Prüfung

Zielsetzung der Überprüfung ist die Umsetzung dieses Dokuments. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Endteilnehmer-Zertifikaten in Verbindung stehen:

- Ausstellung von Sub-Registrator-Zertifikaten und deren Derivate
- Authentifizierung und Registrierung durch Sub-Registratoren
- Identitätsprüfungen der Endteilnehmer
- Zertifikatsbeantragungsverfahren
- Bearbeitung von Zertifikatsanträgen
- Verteilung von Schlüsseln und Geheimnissen (Passwort, PIN)
- Zertifikatsannahmen
- Zertifikatserneuerung (Re-Zertifizierung)
- Schlüsselerneuerung (Re-Key)
- Zertifikatssperrungen
- Zutrittsschutz
- Zugriff auf Registrator-Arbeitsplätze

- Schlüsselsicherung und -archivierung
- Berechtigungs- und Rollenkonzept
- Einbruchshemmende Maßnahmen
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen der folgenden Audit-Kriterien geprüft:

- ETSI EN 319 411-1, Policy NCP
- ETSI EN 319 411-1, Policy OVCP

Risikobewertung und Sicherheitsplan

Das Trust Center der Telekom Security führt jährliche eine Risikobewertung durch, welches u.a. auch den PKI-Dienst TeleSec Shared-Business-CA abdeckt.

Die Überprüfung beinhaltet zumindest die folgenden Punkte:

1) Identifikation vorhersehbarer externer, als auch interner Gefährdungen (d.h. insbesondere die zu Grunde liegenden Schwachstellen), welche
   a) zu unbefugten Zugriffen auf relevante Daten oder Systeme,
   b) zur Weitergabe oder einem Missbrauch von relevanten Daten,
   c) zu Veränderungen oder Zerstörung von relevanten Daten,
   d) zur Beeinträchtigung, Störung oder Ausfall von Teilen oder des gesamten Zertifikatsverwaltungsprozesses

   führen können.
2) Beurteilung der Eintrittswahrscheinlichkeit und der daraus resultierenden potenziellen Schäden (d.h. Schadenshöhe) durch das Ausnutzten einer Schwachstelle. Dabei ist der besondere Schutzbedarf der Zertifikatsdaten und des Zertifikatsverwaltungsprozesses zu berücksichtigen.
3) Beurteilung der Wirksamkeit und Angemessenheit der getroffenen Gegenmaßnahmen (z.B. Richtlinien, Verfahren, eingesetzte Sicherheits-Systeme, Technologien, Versicherungen) welche die Gefährdung beseitigen oder das Risiko minimieren.

Basierend auf der Risikobewertung hat das Trust Center der Telekom Security einen Sicherheitsplan entwickelt, der regelmäßig überprüft und bei Bedarf angepasst wird. Der Sicherheitsplan besteht aus Verfahren, Maßnahmen und Produkten, um die Bewertung und Management der während der Risikobewertung identifizierten Risiken zu unterstützen. Der Sicherheitsplan enthält entsprechend der Sensibilität der Daten und des Zertifikatsverwaltungsprozesses administrative, organisatorische, technische und physische Sicherheitsmaßnahmen.

8.5 Maßnahmen zur Mängelbeseitigung

Werden bei einem Compliance-Audit von einem Prüfer bei einem Mandanten Mängel festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durch zu führen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheiden der Leiter Trust Center über den Zeitrahmen der Behebung.

8.6 Mitteilung der Ergebnisse

Die Ergebnisse der Prüfung werden in einem vom Prüfer erstellen Bericht dokumentiert und Telekom Security übergeben.

Telekom Security behält sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der Telekom Security.

Auditberichte, die auf Anforderung eines oder mehrerer Anwendungssoftwareanbieter abgelegt werden, welche ein Stammzertifizierungsstellenzertifikat der Telekom Security einbetten, müssen spätestens drei Monate nach Ablauf der jeweiligen Auditperiode veröffentlicht werden.

Für TeleSec Shared-Business-CA werden die geforderten Audits nach den ETSI EN 319 411-1-Kriterien abgelegt. Die zugehörigen Berichte (Audit Attestations) werden auf der Internetseite https://www.telesec.de/de/service/downloads/pki-repository/ veröffentlicht.

8.7 Selbst-Audits

Telekom Security führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durch (Kapitel 8.1).

Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits), die die Servicequalität sicherstellen, finden regelmäßig, jedoch mindestens vierteljährlich, statt. Es werden mindestens 3 (drei) Prozent der in diesem Zeitraum relevanten ausgestellten Zertifikate, aber in jedem Fall 1 ausgestelltes Zertifikat betrachtet, wobei die Auswahl zufällig erfolgt. Es wird immer der Zeitraum, der auf die Periode des vorangegangenen Selbstaufsichtsmaßnahme folgt, für die Auswahl herangezogen.

Als zusätzliche Selbstaufsichtsmaßnahmen werden von Telekom Security Daten überprüft, die sich auf die Identität des PKI-Mandanten als auch dessen Konfiguration beziehen, wie z.B.

- Nachweis der Namensgebung und der Eigentümerschaft des PKI-Mandanten (OU1-Feld, Kapitel 3.1.1.1.3)
- Regelkonformität der OU2- und OU3-Felder (Kapitel 3.1.1.1.4 und 3.1.1.1.5)
- Regelmäßige Prüfungen der Organisation und erlaubten Internet-Domänen (Kapitel 3.1.1.1.2, 3.2.2, 3.2.2.1, 3.2.5.2)

Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) werden von dafür qualifizierten Telekom Security -Mitarbeitern durchgeführt.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

Telekom Security ist berechtigt, für das Ausstellen, Erneuern und Verwalten von Endteilnehmer- und Registrator-Zertifikaten Entgelte zu berechnen. Dies gilt insbesondere für die Bereitstellung und Überlassung des Dienstes TeleSec Shared-Business-CA.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Telekom Security berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst der TeleSec Shared-Business-CA keine Entgelte.

Dritten ist es nur nach vorheriger, ausdrücklicher schriftlicher Genehmigung gestattet, die von Telekom Security öffentlich zur Verfügung gestellten Zertifikate selbst zu vermarkten oder zur Vermarktung anzubieten.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

Telekom Security berechnet für den Zugriff auf Sperrungs- oder Statusinformationen für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile keine Entgelte.

Dritten ist es nur nach vorheriger, ausdrücklicher schriftlicher Genehmigung gestattet, die von Telekom Security öffentlich zur Verfügung gestellten Sperr- und Statusinformationen selbst zu vermarkten oder zur Vermarktung anzubieten.

9.1.4 Entgelte für andere Leistungen

Telekom Security berechnet keine Entgelte auf den Abruf und der damit verbundenen Betrachtung dieses Dokuments „CPS“. Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1), die das Urheberrecht des Dokuments (Kapitel 9.5.2) besitzt.

Ebenfalls ist die Nutzung dieser CPS entgeltfrei, sofern Sie als mit geltende Vertragsunterlage für die Vertragsbeziehung zwischen Mandant und Telekom Security dient.

9.1.5 Entgelterstattung

Die Erstattung von Entgelten durch Telekom Security erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts.

9.2 Finanzielle Verantwortlichkeiten

Es gelten die Regelungen des Einzelvertrags.

9.2.1 Versicherungsschutz

Dem Mandanten obliegt die Pflicht sich im Rahmen seiner Betriebshaftpflichtversicherung bei einem Versicherungsträger oder mittels einer eigenen Deckungsvorsorge für einen wirtschaftlich angemessenen Versicherungsschutz abzusichern. Diese Versicherungsklausel findet ggf. keine Anwendung bei kommunalen, Landes- oder Staats-Behörden.

Telekom Security verfügt über einen entsprechenden Betriebs- und Vermögenshaftpflicht-versicherungsschutz.

9.2.2 Sonstige finanzielle Mittel

Dem Mandanten wird empfohlen, selbst über ausreichend finanzielle Mittel zu verfügen, um damit die Aufrechterhaltung ihres PKI-Betriebes als auch zur Erfüllung ihrer aus diesem Dokument beschriebenen und abgeleiteten Pflichten nachkommen zu können. Darüber hinaus muss der Mandant in der Lage sein, das Haftungsrisiko gegenüber den Endteilnehmern zu tragen, sofern dieses Risiko nicht übertragen werden kann.

Telekom Security wird nicht grundsätzlich den Nachweis über finanzielle Mittel fordern. Eine Ausnahme bildet jedoch Compliance-Audits wie in Kapitel 8 ff beschrieben.

9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang von vertraulichen Informationen

Unter vertraulichen Informationen werden alle Informationen von PKI-Beteiligten (siehe Kapitel 1.3.2 und 1.3.3) der TeleSec Shared-Business-CA eingestuft, die nicht unter Kapitel 9.3.2 fallen.

9.3.2 Umfang von nicht vertraulichen Informationen

Unter nicht vertraulichen Informationen werden alle impliziten und expliziten Informationen der TeleSec Shared-Business-CA eingestuft, die in ausgegebenen Zertifikaten (z.B. E-Mail-Adresse, Organisation, Vor- und Nachname), Sperrlisten, Statusinformationen enthalten sind oder davon abgeleitet werden können.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortlichkeit für den Schutz der vertraulichen Informationen sowie über die Einhaltung der datenschutzrechtlichen Bestimmungen liegt bei Telekom Security als PKI-Diensteanbieter.

Der Mandant hat die einschlägigen gesetzlichen Bestimmungen sowie ggf. weiteren Regelungen zum Datenschutz (Kapitel 9.4 ff) zu beachten.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

9.4.1 Datenschutzkonzept

Innerhalb der TeleSec Shared-Business-CA muss Telekom Security zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten.

Sollen von der Telekom Security besondere Kategorien personenbezogener Daten im Sinne Artikel 9 Datenschutz-Grundverordnung (DSGVO) [EU-DSGVO] verarbeitet werden, hat der Kunde die Telekom Security hierüber unverzüglich schriftlich zu unterrichten.

Entsprechend den Konzernvorgaben der Deutschen Telekom AG wurde für TeleSec Shared-Business-CA ein Datenschutzkonzept erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte um PKI-Dienst zusammen.

Das Datenschutzkonzept kann in Auszügen auf Anforderung bereitgestellt werden.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.1.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.2.

9.4.4 Verantwortung für den Schutz vertraulicher Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.3.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsantragsteller stimmt der Nutzung von personenbezogenen Daten durch eine CA oder RA zu, soweit dies zur Leistungserbringung erforderlich ist.

Ferner dürfen alle Informationen veröffentlicht werden, die nach Kapitel 9.4.3 als nicht vertraulich behandelt werden und deren Veröffentlichung durch den Mandanten nicht widersprochen wurde.

9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die Verpflichtung zur Geheimhaltung der vertraulichen Informationen oder personenbezogener Daten entfällt, soweit die Offenlegung kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens bestehen, die zur Offenlegung vertraulicher oder privater Informationen führen könnten, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei hierüber unter Beachtung der gesetzlichen Bestimmungen informieren.

9.4.7 Andere Gründe zur Offenlegung von Daten

Keine Bestimmungen.

9.5 Rechte des geistigen Eigentums (Urheberrecht)

Die nachfolgenden Kapitel 9.5.1 bis 9.5.4 gelten für geistige Eigentumsrechte von Endteilnehmern und Vertrauenden Dritten.

9.5.1 Eigentumsrechte an Zertifikaten und Sperrinformationen

Telekom Security behält sich jede geistigen Eigentumsrechte an Zertifikaten, Sperr- oder Statusinformationen, öffentlich zugängliche Verzeichnisdiensten und Datenbanken mit den ihnen enthaltenen Informationen vor, die die TeleSec Shared-Business-CA ausstellt bzw. verwaltet.

Sofern Zertifikate und deren Inhalte, die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt Telekom Security die Zustimmung, Zertifikate auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren.

Unter Voraussetzung, dass die Nutzung von Sperr- oder Statusinformationen und deren Inhalte, die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt Telekom Security die Zustimmung, Sperrlisten und Statusinformationen auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren, insbesondere an Vertrauende Dritte.

9.5.2 Eigentumsrechte dieser CPS

Dieses Dokument „CPS“ ist urheberrechtlich geschützt, alle geistigen Eigentumsrechte obliegen der Telekom Security. Jegliche andere Nutzung (z.B. Vervielfältigung, Verwendung von Texten und Bildern, Änderung oder Erzeugung eines vergleichbaren oder abgeleiteten Dokuments, Weitergabe an Personen ohne Interesse an dem in diesem Dokument beschriebenem Dienst), auch auszugsweise, bedarf der vorherige ausdrücklichen schriftliche Genehmigung des Herausgebers dieses Dokuments „CPS“ (siehe Kapitel 1.5.1).

9.5.3 Eigentumsrechte an Namen

Der Endteilnehmer behält, sofern zutreffend, alle Rechte an Namen oder Marken, die im Zertifikat enthalten sind, sofern das Zertifikat einen eindeutigen Namen beinhaltet.

9.5.4 Eigentumsrechte an Schlüsseln und Schlüsselmaterial

Die geistigen Eigentumsrechte von Schlüsselmaterial von CA- und Root-CA verbleiben bei Telekom Security, ungeachtet des Mediums, auf denen sie gespeichert sind. Kopien von CA- und Root-CA-Zertifikate dürfen vervielfältigt werden um diese in vertrauenswürdige Hardware- und Software-Komponenten zu integrieren.

Schlüsselmaterial, das der Mandant bzw. dessen Endteilnehmer selbst erzeugte, verbleibt sein Eigentumsrecht. Dies gilt auch für Schlüsselmaterial auf Smartcards, dass er erworben hat.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle

Die Zertifizierungsstelle „TeleSec Shared-Business-CA“ übernimmt die Verantwortung für alle Aspekte der Bereitstellung von Zertifizierungsdienstes, als auch für die Tätigkeiten, die an Unterauftragnehmer ausgelagert werden. Die Zertifizierungsinstanz hat die Verantwortlichkeiten klar geregelt und geeignete Vorkehrungen getroffen, um Kontrollen durch die Zertifizierungsinstanz bei Dritten durchführen zu dürfen. Die CA behält sich die Offenlegung der relevanten Praktiken für Parteien vor.

Die Zertifizierungsstelle stellt sicher, dass die Sicherheit der Informationen beibehalten wird, auch wenn die Tätigkeiten der Zertifizierungsstelle an andere Organisationen ausgelagert wird.

Die Zertifizierungsinstanz verfügt über eine dokumentierte Vereinbarung und ein aktuelles Vertragsverhältnis, die die Bereitstellung des PKI-Dienstes hinsichtlich Zulieferung, Ausgliederung von Betriebsfunktionen (Outsourcing) oder andere Vereinbarungen mit Dritten unterstützt.

Ebenfalls gelten die entsprechenden Regelungen „Delegierung von Tätigkeiten“ der [CAB-BR].

Die Telekom Security verpflichtet sich,

- keine unrichtigen Angaben in Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- dass alle Zertifikate den Anforderungen dieser CPS genügen, und
- dass die Sperrfunktionalitäten und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) allen wesentlichen Anforderungen der geltenden CPS erfüllen.

Weiterhin sichert das Telekom Security Trust Center zu, dass zum Zeitpunkt der Ausstellung eines [CAB-BR] konformen Zertifikates:

1) eine definierte Prozedur existiert um sicherzustellen, dass der Antragsteller das Recht hat, die im Zertifikat benannten Domains/IP-Adressen zu verwenden. Alternativ ist er über eine entsprechende Vollmacht autorisiert, welche von einer Person oder einer Organisation ausgestellt wurde, welche das Recht zur Verwendung hat.
2) die unter 1) genannte Prozedur befolgt wird und
3) das unter 1) benannte Verfahren in diesem CPS detailliert spezifiziert wird.
4) eine definierte Prozedur befolgt wird, um sicherzustellen, dass der im Zertifikat benannte Zertifikatsnehmer (Subjekt) die Ausstellung des Zertifikates genehmigt hat, sowie, dass der Repräsentant des Antragstellers berechtigt ist, den Antrag zu stellen.
5) die unter 4) genannte Prozedur befolgt wird und
6) das unter 4) benannte Verfahren in diesem CPS detailliert spezifiziert wird.
7) eine definierte Prozedur befolgt wird, um zu prüfen, dass im subject DN alle im Zertifikat enthaltenen Informationen korrekt sind
8) die unter 7) genannte Prozedur befolgt wird und
9) dass unter 7) benannte Verfahren in diesem CPS detailliert spezifiziert wird.
10) eine definierte Prozedur befolgt wird, um die Wahrscheinlichkeit zu minimieren, dass das OU-Feldes des subject DN irreführende Informationen enthält
11) die unter 10) genannte Prozedur befolgt wird und
12) dass unter 10) benannte Verfahren in diesem CPS detailliert spezifiziert wird.

Außerdem sichert das Telekom Security Trust Center zu, dass im Falle, dass das auszustellende TLS/SSL-Zertifikat Informationen zur Identität des Zertifikatsnehmers enthält

13) eine definierte Prozedur zur Überprüfung der angegebenen Identität befolgt wird, welche die Anforderungen der zum Zeitpunkt der Zertifikatsaustellung gültigen Version der [CAB-BR] Kapitel 9.2.4 und 11.2 erfüllt.
14) die unter 13) genannte Prozedur befolgt wird und
15) dass unter 13) benannte Verfahren in diesem CPS detailliert spezifiziert wird.

Das Telekom Security Trust Center sichert weiterhin zu, dass

16) falls der Zertifikatsnehmer einem Verbundenen Unternehmen (Affilate) angehört oder in dessen Namen für dieses auftritt, der Repräsentant des Antragstellers vor der Ausstellung eines Zertifikates die " „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ akzeptieren muss.
17) falls der Zertifikatsnehmer einer Beauftragten Drittpartei angehört oder in deren Namen für dieses auftritt, der Antragsteller mit der Telekom Security die "Bezugsvertrag" in einer rechtlich durchsetzbaren Form vereinbart.
18) es ein öffentlich zugängliches Verzeichnis betreibt, welches Status Informationen zu allen nicht abgelaufenen Zertifikaten (gültig oder gesperrt) enthält. Dieses Verzeichnis ist 7x24h verfügbar.
19) die ausgestellten Zertifikate aus allen in den [CAB-BR] aufgeführten Gründen sperren wird.
20) bei einer Kenntnisnahme der Zertifizierungsstelle über eine Kompromittierung die betroffenen Zertifikate sperren wird.

Die Telekom Security behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Mandanten abzuschließen.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle

Registrierungsstellen verpflichten sich,

- dass Master- bzw. Sub-Registrator-Zertifikat (und deren Derivate, Kapitel 1.3.2.2.2) nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- ihren privaten Schlüssel geheim zu halten vor unberechtigtem Zugriff durch Dritte zu schützen,
- bei Verlust oder Verdacht der Kompromittierung des privaten Schlüssels eine Sperrung des entsprechenden Master- bzw. Sub-Registrator-Zertifikat (und deren Derivate) zu veranlassen,
- keine wesentlich unrichtigen Angaben in Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- dass das von ihnen eingesetzte Zertifikat ausschließlich für autorisierte und legale Zwecke verwendet wird, die der Mandant vorgibt, und nicht den Regelungen dieser CPS widersprechen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der vorliegenden CPS beschriebenen Pflichten entstehen,
- dafür Sorge zu tragen, dass ihre Geräte bei der Zertifikatsbeantragung und –ausstellung als auch Zertifikats-Validierung keine technischen Schnittstellen des PKI-Service TeleSec Shared-Business-CA beeinträchtigen (rollenspezifische Webseiten, CMP, LDAP, SCEP, Mail, OCSP, CRL),
- auf Anforderung eines Endteilnehmers oder autorisierten Vertreters bei Verlust oder Verdacht der Kompromittierung des privaten Schlüssels eine Sperrung durchzuführen,
- dass alle Zertifikate den wesentlichen Anforderungen dieser CPS genügen, und
- dass die Sperrfunktionalitäten durch Master- und Sub-Registratoren und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) in allen wesentlichen Anforderungen der geltenden CPS erfüllen.

Die Telekom Security behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Mandanten abzuschließen.

9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Endteilnehmer verpflichten sich,

- das Endteilnehmer-Zertifikat nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- ihren privaten Schlüssel vor unberechtigtem Zugriff durch Dritte zu schützen. Im Falle von privaten Schlüsseln von Geräten erfolgt der Schutz durch autorisierte Personen,
- dass jede digitale Signatur mit dem privaten Schlüssel erstellt wird, die zum im Zertifikat zugehörigen öffentlichen Schlüssel passt und dem Endteilnehmer eindeutig zugeordnet werden kann,
- dass jede digitale Signatur mit dem Schlüsselmaterial eines gültigen und nicht gesperrten Zertifikats erfolgt,
- dass die in seinem Endteilnehmer-Zertifikat aufgenommenen Zertifikatsinhalte des Subject-DN der Wahrheit entsprechen. Im Falle von Geräten erfolgt die Prüfung der Zertifikatsinhalte durch autorisierte Personen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der vorliegenden CPS beschriebenen Pflichten entstehen,
- dafür Sorge zu tragen, dass ihre Geräte bei der Zertifikatsbeantragung und –ausstellung als auch Zertifikats-Validierung keine technischen Schnittstellen des PKI-Service TeleSec

Shared-Business-CA beeinträchtigen (rollenspezifische Webseiten, CMP, LDAP, SCEP, Mail, OCSP, CRL),

- bei Verlust oder Verdacht der Kompromittierung des privaten Schlüssels, wesentliche Änderungen der Zertifikatsangaben oder Missbrauchsvermutung eine Sperrung des entsprechenden Endteilnehmer-Zertifikat zu veranlassen bzw. selbst durchzuführen,
- bei Kompromittierung des privaten Schlüssels ist die Verwendung des privaten Schlüssels des Zertifikatsinhabers unmittelbar und dauerhaft einzustellen,
- dass das von ihnen eingesetzte Zertifikat ausschließlich für autorisierte und legale Zwecke die, diesem CPS entsprechen, verwendet wird und nicht den Regelungen dieser Erklärung widersprechen, und
- dass der Endteilnehmer tatsächlich ein Endteilnehmer ist und mit seinem privaten Schlüssel, dem der im Zertifikat enthaltene öffentliche Schlüssel zugeordnet ist, keine CA-Funktionalitäten durchführt wie z.B. Signatur von Zertifikaten oder Sperrlisten.

Die Telekom Security behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Endteilnehmers abzuschließen.

9.6.4 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der Vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

Der Vertrauende Dritte muss sein Gerät so konfigurieren, dass bei der Zertifikats-Validierung keine technischen Schnittstellen des PKI-Service TeleSec Shared-Business-CA beeinträchtigt werden (rollenspezifische Webseiten, CMP, LDAP, SCEP, Mail, OCSP, CRL).

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Nicht anwendbar.

9.7 Haftungsausschluss

Die Telekom Security haftet dem Kunden stets

a) für die von ihr sowie ihren gesetzlichen Vertretern oder Erfüllungsgehilfen vorsätzlich oder grob fahrlässig verursachten Schäden,
b) nach dem Produkthaftungsgesetz und
c) für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die der Anbieter, seine gesetzlichen Vertreter oder Erfüllungsgehilfen zu vertreten haben.

Die Telekom Security haftet bei leichter Fahrlässigkeit nicht, außer soweit sie eine wesentliche Vertragspflicht verletzt hat, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Kunde regelmäßig vertrauen darf.

Schäden (inkl. Imageschäden), die durch missbräuchlichen oder Zertifikatsinhalt (Kapitel 4.5.1, 5.8) oder missbräuchliche Nutzung von Warenzeichen, Markennamen, Markenrechte (Kapitel 3.1.6) entstehen, gehen zu Lasten des PKI-Mandanten (Kunden).

9.8 Haftungsbeschränkungen

9.8.1 Haftung des Anbieters (Telekom Security)

Diese Haftung ist bei Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden beschränkt. Dies gilt auch für entgangenen Gewinn und ausgebliebene Einsparungen. Die Haftung für sonstige entfernte Folgeschäden ist ausgeschlossen.

Bei Vereinbarung einer Einmal-Vergütung ist die Haftung bei Sach- und Vermögensschäden auf 10 % des Netto-Auftragsvolumens pro Schadensereignis und für alle Schäden innerhalb eines Vertragsjahres auf 25 % des Netto-Auftragsvolumens begrenzt. Bei Vereinbarung einer wiederkehrenden Vergütung ist die Haftung bei Sach- und sonstigen Schäden auf 10 % des Netto-Jahresentgelts pro Schadensereignis und für alle Schäden innerhalb eines Vertragsjahres auf 25 % des Netto-Jahresentgelts begrenzt. Die Parteien können bei Vertragsabschluss eine weitergehende Haftung gegen gesonderte Vergütung vereinbaren. Vorrangig ist eine gesondert vereinbarte Haftungssumme. Die Haftung gemäß Kapitel 9.7 bleibt von diesem Absatz unberührt.

Ergänzend und vorrangig ist die Haftung der Telekom Security wegen leichter Fahrlässigkeit - unabhängig vom Rechtsgrund - insgesamt begrenzt auf 2,5 Mio. EUR. Die Haftung gemäß Kapitel 9.7 Buchstabe b) bleibt von diesem Absatz unberührt.

Aus einer Garantieerklärung haftet die Telekom Security nur auf Schadensersatz, wenn dies in der Garantie ausdrücklich übernommen wurde. Diese Haftung unterliegt bei leichter Fahrlässigkeit den Beschränkungen gemäß Kapitel 9.8.1.

Bei Verlust von Daten haftet die Telekom Security nur für denjenigen Aufwand, der für die Wiederherstellung der Daten bei ordnungsgemäßer Datensicherung durch den Kunden erforderlich ist. Bei leichter Fahrlässigkeit der Telekom Security tritt diese Haftung nur ein, wenn der Kunde unmittelbar vor der zum Datenverlust führenden Maßnahme eine ordnungsgemäße Datensicherung durchgeführt.

Für Aufwendungsersatzansprüche und sonstige Haftungsansprüche des Kunden gegen die Telekom Security gelten die Kapitel 9.7 und 9.8 ff entsprechend.

9.8.2 Haftung des Zertifikatsinhabers

Der Zertifikatsinhaber (Zertifikatsnehmer) haftet gegenüber dem Anbieter (Telekom Security) und den beteiligten Parteien für Schäden, die aus Missbrauch, vorsätzlichem Fehlverhalten, Nichteinhaltung von aufsichtsrechtlichen Verpflichtungen oder Nichteinhaltung anderer Bestimmungen zur Nutzung des Zertifikats resultieren.

9.9 Schadenersatz

Für etwaige Schadensersatzansprüche gelten die Regelungen in Kapitel 9.7 und 9.8 ff.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Die Erstveröffentlichung dieses Dokuments „CPS“ als auch dessen Änderungen treten mit der Veröffentlichung auf öffentlichen Webseiten der Telekom Security (siehe Kapitel 2.3) in Kraft.

9.10.2 Beendigung

Diese CPS bleibt in der jeweils gültigen Version in Kraft, bis sie durch eine neue Version ersetzt wird.

9.10.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung des Dienstes TeleSec Shared-Business-CA bleiben alle Mandanten (Teilnehmer der Master-Domänen) als auch die Benutzer der daraus erzeugten Endteilnehmer-Zertifikaten an die in der CPS enthaltenen Regelungen gebunden, bis das letzte ausgegebene Zertifikat ungültig oder gesperrt wird.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Falls nicht anders vertraglich vereinbart, werden für individuelle Mitteilungen und Kommunikation mit der Zertifizierungsstelle TeleSec Shared-Business-CA werden die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben (siehe auch Dokument „Zertifikats- und Konfigurationsdatenblatt“).

9.12 Änderungen

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich die Telekom Security das Recht vor, Änderungen und Anpassungen dieses Dokuments durchzuführen.

9.12.1 Verfahren für Änderungen

Änderungen dieser CPS können nur von Change Advisory Board des Herausgebers (Kapitel 1.5 ff) durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und Veröffentlichungsdatum. Diese gilt auch für den Fall, das nach der jährlichen Überprüfung keine Änderungen festgestellt wurden.

Änderungen treten unverzüglich mit der Veröffentlichung in Kraft (siehe auch Kapitel 2.3).

Aktualisierte Versionen dieses Dokuments setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet das Telekom Security Advisory Board über weitere Vorgehensweise.

Innerhalb bestehender Verträge sind Änderungen dieser CPS mindestens sechs Wochen vor Wirksamwerden schriftlich der beauftragten Drittpartei (Delegated Third Party) mitzuteilen. Bei Änderungen zu Ungunsten der beauftragten Drittpartei (Delegated Third Party) steht diesem ein Sonderkündigungsrecht zum Zeitpunkt des Wirksamwerdens der Änderung zu. Erfolgt seitens der beauftragten Drittpartei (Delegated Third Party) innerhalb von sechs Wochen nach Zugang der Änderungsmitteilung keine schriftliche Kündigung, werden die Änderungen zum Zeitpunkt des Wirksamwerdens Vertragsbestandteil.

9.12.2 Benachrichtigungsverfahren und -zeitraum

Die Mandanten werden über die Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch ein zu legen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion wie unter Kapitel 9.12.1 in Kraft. Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Falls das Telekom Security Advisory Board der Ansicht ist, dass z.B. gravierende sicherheitsrelevante Änderungen unverzüglich erforderlich sind, dann tritt die neue CPS unverzüglich mit der Freigabe (siehe Kapitel 9.12.1) in Kraft.

9.12.3 Gründe, unter denen die Objekt-Kennung (Objekt – ID) geändert werden muss

Telekom Security Advisory Board entscheidet darüber, ob Änderungen der Objekt-ID der CPS notwendig werden. Andernfalls erfordern Änderungen keine Änderungen der Objekt-ID der Zertifizierungsrichtlinie.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

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

9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Frankfurt am Main, Deutschland.

9.15 Einhaltung geltenden Rechts

Das vorliegende Dokument unterliegt den geltenden deutschen Gesetzen, Vorschriften, Richtlinien, Verordnungen, Erlassen und Anordnungen, insbesondere den darin beschriebenen Import und Export Bestimmungen von Security-Komponenten (Software, Hardware oder technischer Informationen). Geltende zwingende Gesetze, Vorschriften, Richtlinien, Verordnungen, Erlasse und Anordnungen setzen die entsprechenden Bestimmungen der vorliegenden CPS außer Kraft.

9.16 Verschiedene Bestimmungen

9.16.1 Vollständiger Vertrag

Nicht anwendbar.

9.16.2 Abtretung

Nicht anwendbar.

9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieser CPS unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser CPS im Übrigen nicht. Statt der unwirksamen und undurchführbaren Bestimmung gilt eine solche Bestimmung als vereinbart, die dem wirtschaftlichen Zweck dieses Dokuments in rechtswirksamer Weise am nächsten kommt. Das Gleiche gilt für die Ergänzung etwaiger Vertragslücken.

9.16.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Nicht anwendbar.

9.16.5 Höhere Gewalt

Es gelten die Regelungen des Einzelvertrags.

Innerhalb des gesetzlich zulässigen Rahmens müssen Verträge mit Mandanten, Vertrauende Dritte oder Endteilnehmer Schutzklauseln über Höhere Gewalt enthalten, um Telekom Security schützen zu können.

Mit dieser Regelung soll sichergestellt werden, dass Telekom Security mit seinen Mandanten, Vertrauende Dritte oder Endteilnehmer vereinbart, dass Telekom Security nicht in Verzug gerät, wenn sich die Leistung infolge höherer Gewalt verzögert oder unmöglich wird.

9.17 Sonstige Bestimmungen

9.17.1 Barrierefreiheit

Der Zugang zu den TC-Services erfolgt im Wesentlichen browserbasiert. Betriebssysteme bieten hier eine Vielzahl unterschiedlicher Barrierefreiheitsfeatures, um behinderten Personen den Zugriff auf die Web-Portale der Trust Center Services zu erleichtern. Diese kompensieren insbesondere Einschränkungen des Seh- und Hörvermögens, physischen Einschränkungen sowie Wahrnehmungsstörungen (z.B. „Informationen zur Barrierefreiheit für IT-Experten“).

Des Weiteren erfolgen Analysen mit den SW-Entwicklungspartnern des Trust Centers, ob es ergänzend zu diesen Standardboardmitteln weitere sinnvolle, betriebssystemunabhängige Möglichkeiten (z.B. mittels HTML5) zur Gestaltung der Barrierefreiheit gibt.

Sollten vorgenannte Maßnahmen nicht ausreichen, bietet Telekom Security darüber hinaus behinderten Menschen zur Unterstützung bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten kostenlosen telefonischen Support.

Anhang A: ABKÜRZUNGEN

BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BR	Baseline Requirements
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Country
CAA	Certification Authority Authorization
CAB	CA/Browser Forum
CARL	Certification Authority Revcation List
cc	Country Coded
CMP	Certificate Management Protocol
CN	Common Name
DK	Dual Key
CA	Certification Authority
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
CSPRNG	kryptographisch geeigneter Zufallszahlengenerator (cryptographically suitable random number generator)
CT	Certificate Transparency
DCF77	Zeitzeichensender (Langwellensender) in Mainflingen bei Frankfurt am Main
DIN	Deutsche Industrie Norm
DN	Distinguished Name
DNS	Domain Name Systems
DSGVO	Datenschutz-Grundverordnung
DV	Domain Validation
ECC	Elliptic Curve Cryptography
EDV	Elektronische Datenverarbeitung
eIDAS	electronic Identification and Signature
ERP	Enterprise-Resource-Planning
ETSI	European Telecommunications Standards Institute (deutsch: Europäisches Institut für Telekommunikationsnormen)
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GPS	Global Positioning System
GRP	Kennzeichner für Gruppen, Funktions-, Rollenzertifikat
GUID	Globally Unique Identifier
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
IPSec	Internet Protocol Security
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)
ISO	International Organization for Standardization
ISP	Internet Service Providers
ITIL	Information Technology Infrastructure Library

IV	Individual Validation
L	Locality
LB	Leistungsbeschreibung
LDAP	Lightweight Directory Access Protocol
MTO	Maximum Tolerable Outage
NCP	"Normalized" Certificate Policy
NIC	Network Information Center
NTP	Network Time Protocol
n.v.	nicht vorhanden
O	Organisation
OCSP	Online Certificate Status Protocol
OID	Object Identifier, Objekt-Kennung
opt.	optional
OU	Organisation Unit Name
OV	Organizational Validated
OVCP	Organizational Validation" Certificate Policy
PED	PIN Entry Device
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudonym
PSE	Personal Security Environment
PU	Productive Unit (Wirkumgebung)
PUK	Personal Unblocking Key
PTC	Publicly-trusted certificate
RA	Registration Authority
RFC	Requests for Comments
RSA	Rivest Shamir Adleman
RSASSA-PSS	RSA Probabilistic Signature Scheme
RTO	Recovery Time Objective
St	Stee or Province Name
SAN	Subject Alternative Name
SBCA	Shared Business CA
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key
SLA	Service Level Agreement
SMS	Short Message Service
SOAP	Simple Object Access Protocol
S/MIME	Secure Multipurpose Internet Mail Extension
SCT	signed certificate timestamp
SHA	Signature Hash Algorithm
SigG	Signaturgesetz
SN	Serial Number
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TC	Trust Center
TLD	Top Level Domain
TLS	Transport Layer Security
TK	Triple Key
TU	Test Unit (Test-Umgebung)
UPN	User Principal Name

URL	Uniform Resource Locator
USV	Unterbrechungsfreie Stromversorgung
UTC	Universal Time Coordinated
XML	Extensible Markup Language

Anhang B: GLOSSAR

Begriff:	Beschreibung:
Antrag auf ein Zertifikat mit erhöhtem Risiko	Ein Antrag, für den die CA eine Zusatzprüfung im Hinblick auf interne Kriterien und Datenbanken vorsieht, die von der CA geführt werden. Dies kann Namen betreffen, die in Bezug auf Phishing oder eine andere betrügerische Nutzung einem höheren Risiko ausgesetzt sind, Namen, die in zuvor abgelehnten Zertifikatsanträgen oder widerrufenen (gesperrten) Zertifikaten enthalten sind, Namen, die auf der MillerSmiles-Phishing-Liste oder auf der Safe-Browsing-Liste von Google stehen bzw. Namen, die die CA anhand ihrer eigenen Risikominderungskriterien identifiziert.
Antragsteller	Die natürliche Person, die ein Zertifikat (oder dessen Erneuerung) beantragt. Ist das Zertifikat einmal ausgestellt, wird der Antragsteller als Zertifikatnehmer bezeichnet. Bei für Geräte ausgestellten Zertifikaten ist der Antragsteller die Organisation, die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt, auch wenn das Gerät den eigentlichen Antrag auf das Zertifikat sendet.
Anwendungssoftware-anbieter	Ein Anbieter von Internetbrowser-Software oder anderer Anwendungssoftware der vertrauenden Seite, die Zertifikate anzeigt oder verwendet und Stammzertifikate (Root) beinhaltet.
Ausstellende Zertifizierungsstelle (CA)	Die Zertifizierungsstelle (CA), die ein bestimmtes Zertifikat ausgestellt hat.
Authentifizierung	Prüfung einer Identität an Hand behaupteter Merkmale.
Beauftragte Drittpartei	Eine natürliche Person, die nicht identisch mit der Zertifizierungsstelle (CA) ist, jedoch von dieser bevollmächtigt ist, den Zertifikatsverwaltungsprozess zu unterstützen, indem sie Aufgaben zur Erfüllung einer oder mehrerer Anforderungen erfüllt. Im Kontext mit der PKI-Lösung Shared-Business-CA bestehen folgende „beauftragte Drittparteien“: Externe Registrierungsstelle (Externe RA); dazu zählt auch das „Derivat“ der Registrierungsstelle eines Unternehmens (Enterprise RA)
Berechtigungsdokument	Die Dokumentation, die die Berechtigung eines Antragstellers belegt, ein oder mehrere Zertifikat(e) für eine bestimmte natürliche Person, Personen- und Funktionsgruppen oder Gerät zu beantragen. Es kann sich auch um ein Dokument der Zertifizierungsstelle über eine Kommunikation mit der betreffenden Person oder Organisation handeln.
Bezugsvertrag (Subscriber Agreement)	Eine Vereinbarung zwischen der Zertifizierungsstelle (CA) und dem Antragsteller/Zertifikatnehmer, in der die Rechte und Verpflichtungen der Parteien festlegt werden.
Bulk	Funktion der Shared-Business-CA mit der der Sub-Registrator Soft-PSE per Massengenerierung erzeugen kann.
Certification Authority Revocation List (CARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (außer Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der CARL überprüft werden, ob dieses noch verwendet werden darf.
Certification Authority Authorization (CAA)	Ein Verfahren, bei dem der Domain-Inhaber im DNS festlegen kann, welche Zertifizierungsstelle(n) für seine Domain(s) Zertifikate ausstellen dürfen.

Certificate Management Protocol (CMP)	Das Zertifikat-Verwaltungsprotokoll, ist ein von der IETF entwickeltes Protokoll, zur Verwaltung von X.509-Zertifikaten innerhalb einer Public-Key-Infrastruktur (PKI). Das Protokoll regelt die Interaktion zwischen den Komponenten einer PKI. In Bezug auf die TeleSec Shared-Business-CA zwischen der Zertifizierungsstelle (CA) und der beauftragten Drittpartei (Delegated Third Party) befindlichen Anwendung.
Certificate Policy (CP)	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Signing Request (CSR) [TC]	Von einem Gerät (z.B. Server) elektronisch erstellt und mit dem privaten Schlüssel signierter Zertifikatsantrag, der in kodierter Form den öffentlichen Schlüssel und die Zertifikatsdaten enthält. Die Syntax wird durch den Standard PKCS#11 beschrieben.
Certificate Revocation List (CRL)	Siehe Sperrliste.
Certificate Transparency (CT)	Ein Google-Projekt für Zertifikatstransparenz: Ausgestellte Zertifikate werden in öffentlich überprüfbare, manipulationsgeschützte Logserver geschrieben, um missbräuchlich oder fehlerhaft ausgestellte TLS/SSL-Zertifikate schneller ermitteln und blockieren zu können. Während dem Zertifikatsausstellungsprozess werden erforderliche CT-Logserver kontaktiert. Diese wiederum liefern in ihrer Antwort je einen SCT zurück, die dann im Zertifikat hinterlegt werden und nachweisen, dass das Zertifikat auf einem Logserver registriert wurde.
Certification Authority (CA)	Siehe Zertifizierungsstelle.
Certification Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
Chipkarte	Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.
crt.sh	Eine Suchmaschine zur Überprüfung von Zertifikaten hinsichtlich Transparenzkontrolle.
Dezentrales Registrierungsmodell	Der Benutzer stellt über die Benutzer-Webseite oder per Mail-Request oder das Gerät stellt über seine SCEP-Schnittstelle den Zertifikatsantrag, den der Sub-Registrator bearbeitet (Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage)).
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Domain-Berechtigungsdokument	Die Dokumentation, die von der Domain-Namen-Registrierungsstelle (Domain Name Registrar), einem registrierten Domain-Inhaber (Domain Name Registrant) oder der Person bzw. Organisation bereitgestellt wird, die in WHOIS als registrierter Domain-Inhaber aufgeführt ist (einschließlich aller privaten, anonymen oder Proxy-Registrierungsservices), und die Berechtigung eines Antragstellers belegt, ein Zertifikat für einen bestimmten Domain-Namensraum zu beantragen. Es kann sich auch um ein Dokument der Zertifizierungsstelle über eine Kommunikation mit der betreffenden Person oder Organisation handeln.
Domain-Name	Die Bezeichnung, die einem Knoten im Domain Name System (DNS) zugeordnet ist.

Dual-Key-Zertifikat	Variante, bei der für Verschlüsselung und Signatur getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt zwei korrespondierende Zertifikate.
Endteilnehmer	Siehe auch Zertifikatnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Endteilnehmer-Zertifikat	Ein Zertifikat, welches nicht die Basiseinschränkung (basic constraints) „Zertifizierungsstelle“ verwendet, daher selber keine Zertifikate signieren kann.
Erklärung zum Zertifizierungsbetrieb (CPS)	Eines von mehreren Dokumenten, die allgemeine und spezifische Rahmenbedingungen vorgibt. Das beninhaltet insbesondere eine Beschreibung der Verfahrensweise, wie die Zertifizierungsstelle (CA) Zertifikate ausstellt, verwaltet, sperrt und erneuert.
Erlaubte Internet-Domänen	Ein Domänenname, der aus der Top-Level-Domain und weiteren Sub-Domains besteht, und nach erfolgreicher Prüfung durch die interne Registrierungsstelle als „erlaubte Internet-Domäne“ in die PKI-Konfiguration des Mandanten (Master-Domäne) aufgenommen wird.
ETSI-Zertifizierung	Überprüfung und Bestätigung für Zertifizierungsstellen durch einen unabhängigen Gutachter, dass die PKI nach den ETSI-Kriterien „ETSI EN 319 411-1“ betrieben werden. Ziel der ETSI-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken. Für Shared-Business-CA gilt die Zertifizierung nach Policy NCP / OVCP PTC-BR.
Externe Registrierungsstelle	Ein Mitarbeiter (Beschäftigter) oder Vertreter eines der Zertifizierungsstelle (CA) nicht verbundenen Unternehmens (non Affiliate), der die Ausstellung von Zertifikaten für Dritte genehmigt. Diese Rollen (Trusted Roles) werden bei SBCA vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen.
Gerät	Komponente wie beispielsweise Router, Server, Gateway, Applikation, die zertifikatsbasierende Funktionen unterstützen, selbst aber nicht oder nur begrenzt selbst Zertifikate beantragen können. Häufig werden Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.
Geräte-Zertifikat	X.509 V3 Zertifikat, welches im commonName-Feld (CN) des distinguishedName des Zertifikatnehmers (Subject) und/oder in mindestens einer subjectAltName-Erweiterung entweder einen Hostname, IP-Adresse oder E-Mail-Adresse enthält.
Gültiges Zertifikat	Ein Zertifikat, das dem in RFC5280 dargelegten Validierungsverfahren besteht.
Gültigkeitsdauer	Der Zeitraum vom Ausstellungsdatum (not before) des Zertifikats bis zum Ablaufdatum (not after).
Hardware Security Modul (HSM)	Hardware zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hashwert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
Identifizierung	Der Prozess der Mitteilung der Identität eines Subjekts oder Objekts (z.B. Benutzer, Gerät) an ein System. Die Identifizierung ist ein Bestandteil der Validierung.

Interface	Schnittstelle als Teil eines Systems, dass zur Kommunikation (Ein- und Ausgabe) dient.
Interne Registrierungsstelle	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer der CA, der die vom PKI-Mandanten benannten „Domain“ prüft und diesem zur Zertifikatsbeantragung zur Verfügung stellt. Diese Rolle (Trusted Role) wird bei SBCA vom Trust-Center-Operator der Telekom Security wahrgenommen.
Interner Server-Name	Ein Server-Name (der einen nicht registrierten Domain-Namen enthalten kann oder nicht), der nicht mit dem öffentlichen Domain Name System (DNS) aufgelöst werden kann.
Issuer-Distinguished-Name (Issuer-DN)	Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Issuer-DN bezeichnet eindeutig die Zertifizierungsstelle.
Juristische Person	Eine Gesellschaft, ein Konzern, eine Partnerschaft, Einzelfirma, Treuhandgesellschaft, Regierungsbehörde oder eine andere klagebefugte Rechtspersönlichkeit innerhalb des Rechtssystems eines Landes.
Key-Back-Up	Mechanismus zur Schlüsselsicherung. Um beispielsweise verschlüsselte E-Mails bei Schlüsselverlust wieder herstellen zu können empfiehlt sich das Key-Back-Up des Schlüsselmaterials des Verschlüsselungsschlüssels. Key-Back-Up wird auch als Synonym für Key-Archiving benutzt.
Key-Recovery	Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert.
Kompromittierung	Ein privater Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
Land	Entweder ein Mitglied der Vereinten Nationen oder eine geographische Region, die von mindestens zwei Mitgliedsländern der UNO als souveräner Staat anerkannt wird.
Latenzzeit	Zeitraum zwischen einer Aktion und dem Eintreten einer verzögerten Reaktion (Verzögerungszeitraum). Bei der Latenzzeit erfolgt die Aktion im Verborgenen und wird erst durch die Reaktion festgestellt.
LDAP-Server	Server, der Informationen speichert, die über LDAP abrufbar sind.
Lightweight Directory Access Protocol (LDAP)	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Mail-Security	Security-Funktionen wie Digitale Signatur und Verschlüsselung, die Standard-E-Mail-Anwendungen unterstützen.
Managementsystem für Informationssicherheit (ISMS)	Das „Managementsystem für Informationssicherheit“ (ISMS) ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Der Begriff wird im Standard ISO/IEC 27002 verwendet, ISO/IEC 27001 definiert ein ISMS.

Mandant	Der Mandant stellt eine eigene logische abgeschlossene Einheit mit eigener Rechte-, Organisations- und Datenverwaltung innerhalb des Systems dar. Der Mandant strukturiert somit die Nutzung des Systems. Als Mandant wird bei SBCA die Master-Domäne bezeichnet. Innerhalb der Master-Domäne bestehen weitere Untergliederungen in Form von Zuständigkeitsbereichen (auch als Sub-Domänen bezeichnet). Weitere Informationen finden Sie auch unter: Mandant
Mandantenfähigkeit	Als Mandantenfähigkeit bezeichnet man in der Informationstechnik (IT) die Eigenschaft einer Software bzw. Server, auf einer Installation mehrere logisch voneinander vollständig getrennte Mandanten abzubilden. Die jeweiligen Mandanten, etwa unterschiedliche rechtliche Einheiten oder Firmen, haben dabei keinerlei gegenseitigen Einblick in die Daten, Benutzerverwaltung oder Ähnliches der anderen Parteien/Mandanten.
Master-Domäne	Eigenständiger, mit einem eindeutigen Namen festgelegter Verwaltungsbereich innerhalb der Shared-Business-CA, der ausschließlich für eine beauftragte Drittpartei (Delegated Third Party) eingerichtet wird. Innerhalb des Mandanten kann die beauftragte Drittpartei Zertifikate genehmigen und verwalten. Der Mandant wird mit dem Master-Registrator-Zertifikat verwaltet. Weitere Informationen finden Sie auch unter: Mandant.
Master-Registrator	Natürliche Person (Trusted Role) der die Master-Domäne verwaltet.
Nicht registrierter Domain-Name	Ein Domain-Name, der kein registrierter Domain-Name ist.
Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA	Bestimmungen bezüglich der Verwahrung und zugelassenen Verwendungszwecke eines ausgestellten Zertifikats in Übereinstimmung mit den gegebenen Anforderungen, wenn der Antragsteller/Zertifikatnehmer beispielsweise ein verbundenes Unternehmen der Zertifizierungsstelle (CA) ist.
Object Identifier (OID)	Ein eindeutiger alphanumerischer oder numerischer Bezeichner, der unter dem jeweiligen Standard für ein bestimmtes Objekt oder eine Objektklasse der Internationalen Organisation für Normung (ISO) registriert ist.
Online Certificate Status Protocol (OCSP) [BR]	Ein Protokoll zur Online-Zertifikatsvalidierung, mit dessen Hilfe die Anwendungssoftware der vertrauenden Seite den Status eines identifizierten Zertifikats bestimmen kann. Siehe auch OCSP-Responder.
OCSP-Responder	Ein Online-Server, der der Zertifizierungsstelle (CA) untersteht und mit deren zentrale Datenablage (Repository) zur Bearbeitung von Zertifikatsstatusanfragen verbunden ist. Siehe auch Online Certificate Status Protocol (OCSP).
Öffentlicher Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Inhaber des entsprechenden privaten Schlüssels offen gelegt werden darf und der von der vertrauenden Seite verwendet wird, um digitale Signaturen zu verifizieren, die mit dem privaten Schlüssel des Inhabers erstellt wurden, und/oder um Mitteilungen zu verschlüsseln, die nur mit dem zugehörigen privaten Schlüssel des Inhabers entschlüsselt werden können.
Öffentliches Geräte-Zertifikat	Ein Geräte-Zertifikat, welches in der CA-Hierarchie von einer ausstellenden Zertifizierungsstelle unterhalb eines öffentlichen Root-Zertifikates ausgestellt wurde.
Personal Identification Number (PIN)	Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.

Personal Security Environment (PSE)	In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Phishing	Angriffsmethode im Internet, um an (geheime) Daten (z.B. PINs, TANs, Passwörter) eines Internetnutzers zu gelangen. Meist werden die Opfer dazu auf gefälschte Webseiten gelockt und zur Eingabe der Daten aufgefordert. Da die Seite auf den ersten Blick offiziellen Charakter hat, ist der Nutzer oft bereit, diese Daten preiszugeben.
Policy	Richtlinien bzw. Erklärung, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
Privater Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Schlüsselpaarinhaber geheim gehalten und verwendet wird, um digitale Signaturen zu erstellen und/oder elektronische Daten und Dateien zu entschlüsseln, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
Public Key Service (PKS)	Service des Telekom Security Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Public Key Infrastruktur	Hardware, Software, Personen, Verfahren, Regeln, Richtlinien und Verpflichtungen, mit denen die vertrauenswürdige Generierung, Ausstellung, Verwaltung und Verwendung von Zertifikaten und Schlüsseln auf der Basis der Public-Key-Kryptographie ermöglicht wird.
Qualifizierter Auditor	Eine natürliche Person, welche die an sie gestellten Anforderungen erfüllt.
Registrierter Domain-Name	Ein Domain-Name, der bei einer Domain-Namen-Registrierungsstelle (Registrar) registriert wurde.
Registrierungsstelle (RA)	Eine juristische Person, die für die Identifizierung und Authentifizierung von Zertifikatssubjekten zuständig ist. Sie ist jedoch keine CA und signiert somit keine Zertifikate und stellt diese nicht aus. Eine RA kann bei der Beantragung oder beim Widerruf eines Zertifikats oder in beiden Fällen Unterstützung leisten. Wenn „RA“ als Adjektiv verwendet wird, um eine Rolle oder eine Funktion zu beschreiben, ist nicht zwangsläufig von einer eigenständigen Stelle die Rede. Sie kann jedoch Teil der CA sein. Im Kontext mit der PKI-Lösung Shared-Business-CA bestehen folgende Registrierungsstellen: Interne RA Externe RA, inkl. Derivat Enterprise-RA
Registrierungsmodell	Standardmäßig unterstützt Shared-Business-CA zwei unterschiedliche Registrierungsmodelle: Zentrales Registrierungsmodell (siehe dort) Dezentrales Registrierungsmodell (siehe dort)
Registrierungsstelle eines Unternehmens (Enterprise RA)	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der nicht der Zertifizierungsstelle (CA) angegliedert ist (non Affiliate), der die Ausstellung von Zertifikaten für diese Organisation genehmigt. Diese Rollen (Trusted Roles) werden bei SBCA vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
Root-CA	Siehe Wurzelzertifizierungsstelle.

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

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

Vertrauenswürdiges Zertifikat	Ein Zertifikat, dem aufgrund der Tatsache vertraut wird, dass sein entsprechendes Stammzertifikat als Vertrauensanker in weit verbreiteter Anwendungssoftware verteilt ist
Vertreter des Antragstellers	Falls abweichend vom Antragsteller, eine natürliche Person oder Kostenträger, ein Beschäftigter des Antragstellers oder ein Handlungsbevollmächtigter ist, der die ausdrückliche Befugnis besitzt, den Antragsteller zu vertreten: (i) die im Namen des Antragstellers einen Antrag auf ein Zertifikat unterzeichnet, einreicht oder genehmigt, und/oder (ii) die im Namen des Antragstellers eine Bezugsvertrag (Subscriber Agreement) unterzeichnet und einreicht, und/oder (iii) die im Namen des Antragstellers die Nutzungsbestimmungen des Zertifikats anerkennt und ihnen zustimmt, wenn der Antragsteller eine verbundene Unternehmen (Affiliate) der Zertifizierungsstelle (CA) ist.
Verzeichnisdienst	Datenspeicher zum Abruf von Zertifikaten und Zertifikats-Validierungsinformationen (Sperrlisten).
Vollmacht	Unter einer Vollmacht versteht man die durch ein Rechtsgeschäft begründete Vertretungsmacht. Die Vollmacht entsteht durch einseitige empfangsbedürftige Willenserklärung des Vollmachtgebers gegenüber dem Vollmachtnehmer.
Voll qualifizierter Domain-Name (FQDN)	Korrekter und vollständiger Domain-Name, d.h. Verkettung aller Labels eines Pfades im Domain-Namensraum (weitere Informationen siehe RFC2181).
Wildcard-Zertifikat	Ein Zertifikat, das ein Sternchen (*) in der äußersten linken Position eines in dem Zertifikat enthaltenen voll qualifizierten Domain-Namens (Fully-Qualified Domain Names) des Subjekts aufweist. Im Kontext mit Shared-Business-CA wird dieses Merkmal nicht unterstützt.
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zentrale Datenablage (Repository)	Eine Online-Datenbank, die öffentliche PKI-Dokumente (z.B. Zertifizierungsrichtlinie, Erklärung zum Zertifizierungsbetrieb, CA-Zertifikate) sowie Zertifikatsstatusinformationen, entweder in Form einer CRL- oder OCSP-Antwort, enthält.
Zentrales Registrierungsmodell	Nach erfolgreicher Registrierung beantragt der Sub-Registrator über die Sub-RA-Webseite das Zertifikat (per Webformular oder Bulk) und erhält dieses bzw. das Schlüsselmaterial für den Endteilnehmer (außer Registrator-Zertifikat) direkt ausgestellt.
Zertifikat	Ein elektronisches Dokument, das eine digitale Signatur verwendet, um einen öffentlichen Schlüssel an eine Identität (z.B. Person, Gerät) zu binden.
Zertifikat einer Stammzertifizierungs-stelle (Root-Zertifikat)	Das selbstsignierte Zertifikat, das von der Stammzertifizierungsstelle (Root-CA) zur Eigenidentifizierung ausgestellt wurde. Ferner soll dieses Zertifikat auch bei der Prüfung (Validierung) ausgestellten Sub-Zertifikate unterstützen.
Zertifikatnehmer	Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die rechtlich durch die Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA gebunden ist.
Zertifikatsantrag	Ein in elektronischer oder schriftlicher Form erstellter Antrag, der Daten zu einem Antragsteller enthält.
Zertifikatsdaten	Zertifikatsanträge und damit verbundene Daten (vom Antragsteller oder anderweitig eingeholt), die sich im Besitz der Zertifizierungsstelle (CA) befinden, die der Kontrolle durch die CA unterliegen oder auf die die CA Zugriff hat.

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

Anhang C: QUELLENNACHWEISE

[CAB-BR]	Zum jeweiligen Zeitpunkt gültige Version des vom CA/Browser-Forum unter https://cabforum.org/baseline-requirements/ veröffentlichten Dokuments „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“
[Trust Center CP]	Zum jeweiligen Zeitpunkt gültige Version des vom Trust Center unter https://www.telesec.de/de/service/downloads/pki-repository veröffentlichten Dokuments „Telekom Security Certification Policy“
[CP/CPS Class2]	CP bzw. CPS der T-TeleSec GlobalRoot Class 2
[CP/CPS DTIRCA1]	CP bzw. CPS der Deutsche Telekom Internal Root CA 1
[CP/CPS DTIRCA2]	CP bzw. CPS der Deutsche Telekom Internal Root CA 2
[ETSI NCP OVCP]	ETSI EN 319 411-1 V1.1.1 (2016-02), European Telecommunications Standards Institute, „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, policy NCP and OVCP
[ETSI EN TSP]	ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures
[EU-DSGVO]	Europäische Datenschutz-Grundverordnung 2016/679, in Kraft getreten am 25.05.2018
[ISAE3402]	ISAE3402-Report, International Standards for Assurance Engagements, http://isae3402.com/ISAE3402_reports.html
[SBCA PITR]	Personelle, Infrastrukturelle und Technische Rahmenbedingungen der TeleSec Shared-Business-CA (SBCA)
[PKCS]	RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“, http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile
[RFC6844]	DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013
[RFC6962]	Certificate Transparency
[SBCA Siko]	Sicherheitskonzept Shared-Business-CA, Vers. 04.00
[SRK TC]	Sicherheitsrahmenkonzept des Trust-Center-Informationsverbunds
[X.509]	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07), http://www.itu.int/rec/T-REC-X.509/en
[Apple-Root-CA]	Apple Root CA Program, https://www.apple.com/certificateauthority/ca_program.html

Anhang D: ERGÄNZENDE LITERATUR

Basis-Dokumentation

- Leistungsbeschreibung (LB)
- Service Level Agreement (SLA)
- Rahmen-SLA für Trust Center Services
- Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)
- Installationsanleitung RA-Platz

Arbeitsanweisung, Schnittstellenbeschreibungen und rollenspezifische Handbücher

- Arbeitsanweisung für Kunden
- Master-Registrator-Handbuch
- Sub-Registrator-Handbuch
- Benutzer-Handbuch
- SCEP-Schnittstelle
- Mail-Schnittstelle