Deutsche Telekom Security GmbH
Certification Practice Statement Root

Deutsche Telekom Security GmbH

Öffentlich

Version: 15.00

Gültig ab: 01.03.2022

Status: Freigabe

Letztes Review: 18.02.2022

ÄNDERUNGSHISTORIE

Tabelle 1: Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
8.0	15.05.2018	T-Systems	Initialversion nach RFC 3647 Struktur und Auftrennung zwischen CP und CPS. Aus diesem Grund wurde eine neue Änderungshistorie begonnen. Ältere Versionen des CP/CPS basieren auf einer abweichenden Struktur.
9.0	12.10.2018	T-Systems	Einarbeitung Änderungen in Kapitel 1.5.2, 4.9 und 5
10.0	10.10.2019	T-Systems	Einarbeitung BR-Änderungen gemäß BR 1.5.7 bis 1.6.6 Einarbeitung EV-Änderungen gemäß EV 1.6.9 bis 1.7.0
11.0	13.03.2020	T-Systems	- Änderung Dokumentenvorlage auf Barrierefreiheit - Einarbeitung Mozilla 2.7 Anforderungen - Einarbeitung BR-Änderungen gemäß BR 1.6.7 - Einarbeitung EV-Änderungen gemäß EV 1.7.1
12.00	08.06.2020	T-Systems	Änderung von T-Systems International GmbH zu Deutsche Telekom Security GmbH
13.00	15.03.2021	Telekom Security	Neu-Auflage entsprechend neuer Telekom Security CP
14.00	29.04.2021	Telekom Security	Einarbeitung [MRSP] 2.7.1 und diverse formale Anpassungen. Kap. 4.9.12, 7.2.2, 7.3
15.00	18.02.2022	Telekom Security	Jährliches Review, Formale Verbesserungen

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS

1 EINLEITUNG

1.1 Überblick

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

Bei dem vorliegenden Dokument handelt es sich um das Certification Practice Statement (CPS) der Stammzertifizierungsstellen des Trust Centers der Telekom Security (kurz: CPS Root). Dieses CPS gilt für alle öffentlichen sowie qualifizierten Root-CA-Zertifikate und ergänzt die CPS der jeweiligen Zertifizierungsdienste, welche Zertifikate unterhalb dieser Root-CAs ausstellen.

Das Dokument beschreibt in der Struktur des RFC3647 die Umsetzung der in der Telekom Security CP gestellten Anforderungen mit Bezug zu den öffentlichen und qualifizierten Root CAs. Es werden hierbei grundsätzlich die Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42), die jeweils aktuellen Versionen der unter http://www.cabfourm.org veröffentlichten „CA/Browser-Forum Baseline Requirements“ [BR] und der „CA/Browser-Forum EV-Guidelines“ [EVCG] sowie der ETSI EN 319 411-1 (insbesondere EVCP-Policy) und ETSI EN 319 411-2 eingehalten. Im Falle eines Widerspruchs zwischen dieser CPS und den referenzierten Dokumenten haben die Regelungen aus den referenzierten Dokumenten Vorrang.

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument trägt den Namen „Telekom Security CPS Root“ und wird durch die OID 1.3.6.1.4.1.7879.13.39 gekennzeichnet. Die OID ist wie folgt zusammengesetzt:

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Telekom Security CPS Root (39)}

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

Die folgenden Stammzertifizierungsstellen (Root-CAs) der Telekom Security sind im Gültigkeitsbereich dieser CPS:

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

Name	Schlüssel-typ	Seriennummer	Gültigkeitszeit-raum	Fingerprint
T-TeleSec GlobalRoot Class 2	RSA 2048	01	2008-10-01 bis 2033-10-01	590d2d7d884f402e617ea562321765cf17d894e9

T-TeleSec GlobalRoot Class 3	RSA 2048	01	2008-10-01 bis 2033-10-01	55a6723ecbf2eccdc3237470199d2abe11e381d1
TeleSec qualified Root CA 1	ECC 521	1179a2c470e121c3	2017-04-05 bis 2047-04-05	90c6136c7defefe97cc764f9d2678ead03e55296
Telekom Security TLS ECC Root 2020	ECC 384	363a968cc95cb258cdd0015dc5e55700	2020-08-25 bis 2045-08-25	c0f896c5a93b01062107da184248bce99d88d5ec
Telekom Security TLS RSA Root 2020	RSA 4096	0db6f3c9e660fb30b2119970a84b45b0	2020-08-25 bis 2045-08-25	4513520839b22e20153c7b367a513ad2beaeda2a
Telekom Security ECC Root 2020	ECC 384	21b5a90c375f9871bf260a08f3f9c6f0	2020-08-25 bis 2045-08-25	9bb84a99d51df08e1e3f9ab2a0629ca61b6ae00f
Telekom Security RSA Root 2020	RSA 4096	3db1afb04b9faa744a258f8189831579	2020-08-25 bis 2045-08-25	c445da958e79728451c16245f548dbacc76fce07
Telekom Security SMIME ECC Root 2021	ECC 384	152add14c918d1a4564086a625af075f	2021-03-18 bis 2046-03-17	b7f91d98ec2593f35014849aa87e22103cc43927
Telekom Security SMIME RSA Root 2021	RSA 4096	18556aa0cc0bac5eb980ec892b1b70d8	2021-03-18 bis 2046-03-17	1afd6890e0de61c4810f517b4798bf67a0e1fb04

1.3.2 Registrierungsstellen (Registration Authorities, RA)

Die Ausstellung von CA-Zertifikaten basiert auf internen Prozessen, welche die Authentizität und Integrität sicherstellen. Einzige Registrierungsstelle ist damit das Trust Center selbst.

1.3.3 Endteilnehmer

Endteilnehmer-Zertifikate sind nicht im Gültigkeitsbereich dieser CPS.

1.3.4 Vertrauende Dritte

Vertrauende Dritte sind Personen oder IT-Prozesse, welche den Zertifikaten vertrauen und zur Prüfung digitaler Signaturen nutzen. Vertrauende Dritte sollten die Sperr- bzw. Statusinformationen gemäß Kapitel 4.9 abfragen, bevor sie einem Zertifikat vertrauen.

1.3.5 Andere Teilnehmer

Keine Bestimmungen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Die Root-CAs werden ausschließlich zur Signatur von Sub-CA-Zertifikaten und OCSP-Signer-Zertifikaten sowie zur Signatur von Sperrlisten verwendet.

1.4.2 Unzulässige Verwendung von Zertifikaten

Die Root-CAs werden nicht für andere als den in Kapitel 1.4.1 aufgeführten Anwendungsfällen verwendet.

1.5 Verwaltung des Dokuments

1.5.1 Verwaltende Organisation dieses Dokuments

Deutsche Telekom Security GmbH

Trust Center & ID-Solutions

Untere Industriestraße 20

57250 Netphen, Deutschland

1.5.2 Ansprechpartner

Ansprechpartner für dieses CPS ist das Root-Team des Trust Centers:

- FMB_Trust_Center_Rootpogram@t-systems.com
- https://telesec.de/de/service/kontakt/anfragemitteilung/

Zertifikatsmissbräuche, Schlüsselkompromittierungen, fehlerhafte bzw. nicht-konforme Zertifikate, andere sicherheitsrelevante Zertifikatsprobleme oder der Verdacht auf solche Vorfälle können via

FMB_Trust_Center_Rootprogram@t-systems.com

an Telekom Security gemeldet werden. Dabei sollten möglichst viele Informationen enthalten sein, die eine Verifizierung des Problems möglich machen. Im Falle einer Schlüsselkompromittierung sollte dies bspw. einen mit dem betroffenen privaten Schlüssel signierten CSR mit commonName „Compromised Key“ beinhalten.

1.5.3 Instanz für die Feststellung der Konformität dieses CPS zur CP

Zuständig für die Feststellung der Konformität dieses CPS zur Telekom Security CP ist das Root-Team des Trust Centers. Für Kontakte siehe Kap. 1.5.2.

1.5.4 Genehmigungsverfahren dieses CPS

Jede Version dieses CPS wird von der Leitung des Trust Centers freigegeben und behält seine Gültigkeit, bis es widerrufen oder durch eine neue Version ersetzt wird.

Dieses CPS wird bei Bedarf, z.B. aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, mindestens aber einmal pro Jahr einem Review durch das Trust Center Root-Team unterzogen. Änderungen sowie das jährliche Review werden in der Änderungshistorie dieses Dokuments aufgeführt. Dies gilt auch für den Fall, dass beim jährlichen Review keine inhaltlichen Änderungen vorgenommen werden. Jede neue Version wird von der Leitung des Trust Centers freigegeben, erhält eine neue aufsteigende Versionsnummer und wird gemäß den Vorgaben aus Kapitel 2.2 veröffentlicht.

1.6 Definitionen und Abkürzungen

1.6.1 Glossar

Siehe Telekom Security CP.

1.6.2 Abkürzungsverzeichnis

Siehe Telekom Security CP.

1.6.3 Referenzen

Siehe Telekom Security CP.

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

Telekom Security betreibt ein Repository mit Informationen und Dokumenten (siehe Kap. 2.2) sowie Zertifikatsstatusdienste (siehe insbesondere Kap. 4.9 bzw. 4.10).

2.2 Veröffentlichung von Informationen zu Zertifikaten

Telekom Security veröffentlicht im PKI-Repository des Trust Centers https://www.telesec.de/de/service/downloads/pki-repository/ folgende Informationen bzw. Dokumente:

- Telekom Security CP
- Certification Practice Statements (dieses Dokument)
- alle CA-Zertifikate im Gültigkeitsbereich dieser CPS
- Audit Attestations zu öffentlichen und qualifizierten Root-CA-Zertifikaten der Telekom Security (Verlinkung zu den offiziellen Web-Seiten des Auditors).

Das CPS Rootwird in deutscher und englischer Sprache veröffentlicht. Die deutschen und englischen Versionen eines Dokuments haben immer die gleiche Versionsnummer und werden inhaltlich synchronisiert. Im Streitfall ist jedoch die deutsche Version autoritativ.

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

Zu allen öffentlichen Root-CAs, unter denen TLS-Serverzertifikate ausgestellt werden, werden jeweils folgende Test-Web-Seiten betrieben:

- eine Test-Webseite mit einem gültigen TLS-Serverzertifikat
- eine Test-Webseite mit einem abgelaufenen TLS-Serverzertifikat
- eine Test-Webseite mit einem gesperrten TLS-Serverzertifikat

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Die in Kap. 2.2 aufgeführten Informationen werden wie folgt veröffentlicht:

- Öffentliche Root-CA-Zertifikate werden sowohl im eigenen Repository als auch in der CCADB veröffentlicht.
- Sub-CAs unterhalb der öffentlichen Root-CAs werden innerhalb von 7 Tagen nach ihrer Ausstellung und in jedem Falle vor Inbetriebnahme sowohl in der CCADB als auch im eigenen Repository veröffentlicht.
- Audit Attestations werden innerhalb von 7 Tagen nach ihrer Ausstellung sowohl in der CCADB als auch im eigenen Repository veröffentlicht bzw. verlinkt.
- Neue Versionen des Root-CPS werden spätestens mit Beginn der Gültigkeit im Repository des Trust Centers veröffentlicht sowie an die CCADB kommuniziert. Eine Aktualisierung und damit verbundene Veröffentlichung des CPS findet mindestens jährlich statt und ist

grundsätzlich mit einer neuen Versionsnummer und einem entsprechenden Eintrag in der Änderungshistorie verbunden, selbst wenn es keine weiteren Änderungen gibt.

2.4 Zugang zu den Verzeichnissen

Die in Kapitel 2.2 aufgeführten Informationen sind für den lesenden Zugriff ohne Zugriffsbeschränkung erreichbar. Die Verfügbarkeit und Integrität der bereitgestellten Informationen werden durch entsprechende technische Maßnahmen sichergestellt.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

3.1.1 Namensformen

Es werden in alle Zertifikate die Namen der Zertifikatsinhaber in Form eines Distinguished Names gemäß X.500 Namenskonventionen aufgenommen, siehe Kapitel 7.1.4.

3.1.2 Aussagekraft von Namen

Jedes CA-Zertifikat erhält einen CommonName, welcher die Zugehörigkeit dieser CA zur Deutschen Telekom Security GmbH bzw. dem DFN unmissverständlich wiedergibt.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Nicht anwendbar.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

Jedes Root-CA-Zertifikat der Deutschen Telekom Security GmbH und alle unter einer jeweiligen Root-CA ausgestellten Sub-CA-Zertifikate erhalten einen einzigartigen CommonName und damit SubjectDistinguishedName.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Nicht anwendbar.

3.2 Initiale Validierung der Identität

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Die Root-CA-Schlüssel werden im Rahmen einer Root-Zeremonie im Mehr-Personen-Prinzip unter Aufsicht eines externen Auditors unmittelbar im Zusammenhang mit der Erzeugung des korrespondierenden Root-CA-Zertifikats generiert.

Für die Ausstellung eines Sub-CA-Zertifikats ist ein mit dem privaten Schlüssel signierter CSR (Certificate Signing Request) notwendig, welcher ebenfalls und nachweisbar in einer Zeremonie im Mehr-Personen-Prinzip erzeugt werden muss.

3.2.2 Authentifizierung von Organisationen

Eine Authentifizierung ist bei internen Antragstellern nicht erforderlich. Der DFN wurde bei Vertragsabschluss authentifiziert.

3.2.3 Authentifizierung von natürlichen Personen

Nicht anwendbar, da CA-Zertifikate nicht an natürliche Personen ausgegeben werden.

3.2.4 Nicht überprüfte Informationen

Keine Bestimmungen.

3.2.5 Validierung der Bevollmächtigung

Interne Anträge werden von dem bevollmächtigten Leiter VDA genehmigt.

Antragsteller des DFN müssen eine Bevollmächtigung vorweisen, die von einer vertretungsberechtigten Person des DFN unterzeichnet ist.

3.2.6 Cross-Zertifikate

Es werden keine Cross-Zertifikate für externe Organisationen ausgestellt.

3.3 Identifizierung und Authentifizierung für Zertifikatserneuerungen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Zertifikatserneuerungen

Nicht anwendbar.

3.3.2 Identifizierung und Authentifizierung für Zertifikatserneuerungen nach einer Sperrung

Nicht anwendbar.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Für die Sperrung von CA-Zertifikaten ist ein vom Betreiber der Sub-CA oder der Leitung des Trust Centers (digital) signierter Sperrantrag erforderlich.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Berechtigte Antragsteller für Root-CA-Zertifikate sind die Vertreter des Trust Center Root-Team. Subjekt der Root-CA-Zertifikate ist die Deutsche Telekom Security GmbH.

Berechtigte Antragsteller für Sub-CA-Zertifikate sind die Betreiber der jeweiligen Zertifizierungsdienste der Deutschen Telekom Security GmbH, der Deutschen Telekom AG, der T-Systems Internation GmbH sowie Vertreter des DFN (Deutsches Forschungsnetz).

4.1.2 Antragsprozess und -verantwortlichkeiten

Die Beantragung von Root-CA-Zertifikaten erfolgt in Abstimmung mit der Leitung des Trust Centers, welche auch die finale Freigabe erteilt.

Für die Beantragung eines Sub-CA-Zertifikats wird von den Betreibern der jeweiligen Zertifizierungsstelle

- ein Zertifikatsrequest im PKCS#10-Format („Certificate Signing Request“, CSR) sowie
- ein unterzeichnetes Antragsformular

verlangt.

In dem Antragsformular bestätigt der Antragsteller

- die Korrektheit der gemachten Angaben,
- die Einhaltung der Vorgaben zur Generierung der Schlüssel einer Sub-CA

und gibt als eindeutige Referenz auf den CSR dessen Fingerprint an.

Hinweis: Zertifikatsantragsformulare in elektronischer Form werden akzeptiert, wenn sie mit einer mindestens fortgeschrittenen elektronischen Signatur eines berechtigten Antragstellers unterzeichnet sind.

4.2 Bearbeitung der Zertifikatsanträge

4.2.1 Durchführung der Identifizierung und Authentifizierung

Anträge zur Ausstellung von Sub-CA-Zertifikaten werden auf Vollständigkeit sowie darauf, ob sie von einem gemäß Kapitel 3.2 authentifizierten und autorisierten Antragsteller unterschrieben wurden, geprüft.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Anträge zur Ausstellung von Sub-CA-Zertifikaten werden inhaltlich auf Konformität zu bestehenden Anforderungen geprüft. Bei Bedarf werden weitere notwendige Informationen angefordert. Die Leitung des Trust Centers erteilt anschließend die finale Freigabe zur Zertifikatsausstellung.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Bestimmungen.

4.3 Ausstellung von Zertifikaten

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

Die Ausstellung von CA-Zertifikaten erfolgt gemäß einer fest vorgegebenen Zeremonie an der Offline-CA des Trust Centers. Im Rahmen der Zeremonie werden u.a. folgende Punkte abgedeckt:

- Vorliegende Antragsformulare werden auf Vollständigkeit und gültige Unterschriften geprüft.
- Der Fingerprint des CSR wird mit den im Antrag gemachten Angaben verglichen und validiert.
- Es wird mindestens ein Sechs-Augen-Prinzip eingehalten, bei der Generierung von Root-CA-Schlüsseln und -Zertifikaten sogar mindestens ein Acht-Augen-Prinzip.
- Das Wissen zu Aktivierungsdaten ist immer auf zwei Personen in unterschiedlichen vertrauenswürdigen Rollen verteilt.

4.3.2 Benachrichtigung des Antragstellers über die Ausstellung eines Zertifikats

Nach der Ausstellung eines Zertifikats wird der Antragsteller darüber informiert und das Zertifikat über den vereinbarten Weg übergeben.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Nach Ausstellung eines Sub-CA-Zertifikats hat der jeweilige Betreiber dieser Sub-CA eine Frist von maximal 7 Tagen, um das neue Zertifikat auf Korrektheit zu prüfen und zu akzeptieren. Sollte das Zertifikat abgelehnt werden oder innerhalb der vereinbarten Frist keine Rückmeldung vorliegen, welche die Akzeptanz des neuen Zertifikats bestätigt, wird das Zertifikat gesperrt.

4.4.2 Veröffentlichung des Zertifikats durch die TSP

Siehe Kap. 2.3.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP

Siehe Kap. 2.3.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Antragsteller

Die Schlüssel der Root-CAs werden ausschließlich während des Gültigkeitszeitraums für die in Kapitel 1.4.1 aufgeführten erlaubten Zwecke verwendet. Nach Ablauf der Gültigkeitsdauer oder bei Außerbetriebnahme werden die Schlüssel gelöscht.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte

Vertrauende Dritte haben die Verantwortung, die CA-Zertifikate zur Gültigkeitsprüfung der gesamten Zertifikatskette eines Endteilnehmerzertifikats zu nutzen.

4.6 Zertifikatserneuerung unter Beibehaltung der Schlüssel (Renewal)

4.6.1 Umstände für ein Renewal

Ein Renewal von CA-Zertifikaten wird nicht unterstützt.

4.6.2 Antragsberechtigte für ein Renewal

Nicht anwendbar.

4.6.3 Verarbeitung von Anträgen auf Renewal

Nicht anwendbar.

4.6.4 Benachrichtigung des Endteilnehmers über die Ausstellung neuer Zertifikate

Nicht anwendbar.

4.6.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Nicht anwendbar.

4.6.6 Veröffentlichung erneuerter Zertifikate durch die TSP

Nicht anwendbar.

4.6.7 Information Dritter über die Ausstellung neuer Zertifikate durch die TSP

Nicht anwendbar.

4.7 Zertifikatserneuerung mit neuen Schlüsseln (Re-Keying)

4.7.1 Umstände für ein Re-Keying

Ein Re-Keying von CA-Zertifikaten wird nicht unterstützt.

4.7.2 Antragsberechtigte für ein Re-Keying

Nicht anwendbar.

4.7.3 Verarbeitung von Anträgen auf Re-Keying

Nicht anwendbar.

4.7.4 Benachrichtigung des Endteilnehmers über die Ausstellung eines erneuerten Zertifikats

Nicht anwendbar.

4.7.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Nicht anwendbar.

4.7.6 Veröffentlichung erneuerter Zertifikate durch die TSP

Nicht anwendbar.

4.7.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

Nicht anwendbar.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Änderung von Zertifikatsdaten

Eine Änderung der Zertifikatsdaten von CA-Zertifikaten wird nicht unterstützt.

4.8.2 Antragsberechtigte für eine Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.3 Verarbeitung von Anträgen auf eine Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.4 Benachrichtigung des Endteilnehmers über die Ausstellung eines erneuerten Zertifikats

Nicht anwendbar.

4.8.5 Verhalten, das die Annahme eines geänderten Zertifikats bestätigt

Nicht anwendbar.

4.8.6 Veröffentlichung geänderter Zertifikate durch die TSP

Nicht anwendbar.

4.8.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

Nicht anwendbar.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Sperrgründe

Ein Sub-CA-Zertifikat wird gesperrt, wenn

- ein schriftlicher Sperrantrag, auch ohne Angabe von Gründen, vom Betreiber der Sub-CA gestellt wurde,
- festgestellt wird, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- festgestellt wird, dass der private Schlüssel der Sub-CA kompromittiert oder einer nicht autorisierten Person oder einer Organisation, die nicht mit der Sub-CA verbunden ist,

bekannt gegeben wurde oder nicht mehr den Anforderungen (siehe Kap. 6.1.5 und 6.1.6) entspricht,
- festgestellt wird, dass das Zertifikat missbräuchlich eingesetzt wurde,
- festgestellt wird, dass das Sub-CA-Zertifikat nicht konform zu dieser CP herausgegeben wurde oder der Betreiber der Sub-CA nicht konform zu dieser CP arbeitet,
- festgestellt wird, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist,
- der Betrieb der Root-CA oder der Sub-CA eingestellt wird und keine Regelungen zur Weiterführung des Sperrservice getroffen wurden,
- das Recht der Root-CA oder Sub-CA, Zertifikate gemäß den Anforderungen dieser CP auszustellen erlischt oder widerrufen oder beendet wird und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden,
- gesetzliche Vorschriften, richterliche Urteile oder eine Weisung einer aufsichtsführenden Behörde vorliegen.

Gesperrte Zertifikate werden nicht wieder entsperrt.

4.9.2 Berechtigte Sperrantragsteller

Die Sperrung einer Sub-CA kann grundsätzlich nur durch einen berechtigten Vertreter des Betreibers der Sub-CA beantragt werden. Sollte einer der in Kapitel 4.9.1 aufgeführten Sperrgründe durch das Trust Center festgestellt bzw. durch Dritte dem Trust Center bekannt gemacht und vom Trust Center nachvollzogen werden, so wird ebenfalls eine Sperrung veranlasst.

4.9.3 Verfahren zur Beantragung von Sperrungen

Die Sperrung eines Sub-CA-Zertifikats kann durch die Betreiber der Zertifizierungsstellen oder durch die Leitung des Trust Centers mit einem rechtskräftig unterzeichneten Sperrantrag beantragt bzw. angeordnet werden.

Hinweis: Zertifikatssperranträge in elektronischer Form werden akzeptiert, wenn sie mit einer mindestens fortgeschrittenen elektronischen Signatur eines berechtigten Antragstellers unterzeichnet sind.

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

Nach der Sperrung eines Sub-CA-Zertifikats werden der Zertifikatsinhaber informiert und die CCADB innerhalb von 7 Tagen oder im Falle eines Sicherheitsvorfalls innerhalb von 24 Stunden durch Telekom Security aktualisiert.

4.9.4 Fristen zur Beantragung einer Sperrung

Der Betreiber einer Sub-CA ist dazu verpflichtet, unverzüglich einen Sperrantrag zu stellen, wenn ein Sperrgrund gemäß Kapitel 4.9.1 festgestellt wird.

4.9.5 Fristen zur Verarbeitung von Sperranträgen durch die TSP

Bei Vorliegen eines Sperrgrunds gemäß Kapitel 4.9.1 wird grundsätzlich unter Berücksichtigung der Umstände (Vorhandene und entstehende Sicherheitsrisiken, Aufwand etc.) die Sperrung eines Sub-CA-Zertifikats in einem angemessenen Zeitraum durchgeführt. Für Sub-CAs, die TLS-Serverzertifikate unter den Baseline Requirements [BR] ausstellen, gilt dabei eine Frist von maximal 7 Tagen. Dies beinhaltet die Umsetzung des Sperrstatus in den Zertifikatsstatusdiensten.

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

4.9.6 Anforderungen an Dritte zur Prüfung von Sperrinformationen

Vertrauende Dritte sind dazu angehalten, den Status von Zertifikaten mithilfe der vom Trust Center angebotenen Zertifikatsstatusdienste gemäß Kap. 4.10 abzufragen, bevor sie einem Zertifikat vertrauen.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Sperrlisten der Root CAs, welche Auskunft über gesperrte Sub-CAs geben (Certificate Authority Revocation List (CARL)), werden innerhalb von 24 Stunden nach einer durchgeführten Sperrung eines Sub-CA-Zertifikats sowie regelmäßig alle 3 Monate aktualisiert.

4.9.8 Maximale Latenzzeit von Sperrlisten

Neu erstellte CARLs werden innerhalb von 24 Stunden in den Verzeichnissen veröffentlicht.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Neben den oben genannten Sperrlisten werden auch Online-Statusinformationen per OCSP bereitgestellt. In der Zertifikatserweiterung „Zugriff auf Stelleninformationen“ („Authority Information Access“) eines jeden Zertifikats ist die URL des jeweils relevanten OCSP-Responders enthalten.

4.9.10 Anforderungen an Online Überprüfungsverfahren

Dritte sind dazu angehalten, bei der Prüfung eines Zertifikatsstatus per OCSP die Vorgaben zur Verarbeitung von OCSP-Antworten gemäß RFC6960 zu berücksichtigen.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine Bestimmung.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Dritte, die eine Schlüsselkompromittierung melden wollen, können die in Abschnitt 1.5.2 beschriebenen Kontaktmöglichkeiten 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.

4.9.13 Umstände für eine Suspendierung

Eine Suspendierung von CA-Zertifikaten wird nicht unterstützt.

4.9.14 Berechtigte Antragsteller für eine Suspendierung

Nicht anwendbar.

4.9.15 Ablauf einer Suspendierung

Nicht anwendbar.

4.9.16 Begrenzung der Suspendierungsperiode

Nicht anwendbar.

4.10 Zertifikatsstatusdienste

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

4.10.1 Betriebliche Vorgaben

Alle Dienste für Zertifikatsstatusauskünfte (Sperrlisten und OCSP) werden regelmäßig (maximal 24 Stunden) zeitsynchronisiert (siehe auch Kapitel 5.4.1).

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

4.10.1.1 Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

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

OCSP-Antworten haben eine Gültigkeit von 5 Tagen. Sie werden nach einer Anfrage für 120 Minuten vorgehalten und für weitere Anfragen wiederverwendet, soweit sich der Status des angefragten Zertifikats in dieser Zeit nicht ändert.

Nach der Sperrung eines Sub-CA-Zertifikats ist innerhalb von 24 Stunden eine aktualisierte Auskunft im OCSP-Responder abrufbar.

OCSP-Anfragen zu nicht vergebenen Seriennummern werden protokolliert.

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

Sperrlisten zu Sub-CA-Zertifikaten (CARL) werden alle 3 Monate ausgestellt und haben eine Gültigkeit von 6 Monaten.

Gesperrte Zertifikate sind auch nach ihrem Gültigkeitsende in der Sperrliste enthalten.

4.10.2 Verfügbarkeit

Die Zertifikatsstatusdienste stehen 7x24h zur Verfügung. Es sind Maßnahmen getroffen worden, die im Falle einer Störung die Wiederherstellung der Verfügbarkeit der Zertifikatsstatusdienste innerhalb von 6 Stunden gewährleisten. Darüber hinaus werden größtmögliche Bemühungen unternommen, Störungen so schnell wie möglich zu beheben.

Es stehen ausreichende Kapazitäten zur Verfügung, so dass die Antwortzeit unter normalen Betriebsbedingungen 3 Sekunden nicht überschreitet.

4.10.3 Optionale Merkmale

Keine Bestimmungen.

4.11 Kündigung durch Zertifikatsinhaber

Nicht anwendbar.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und-Praktiken

Nicht anwendbar.

4.12.2 Richtlinien und Praktiken für die Kapselung und Wiederherstellung von Sitzungsschlüsseln

Nicht anwendbar.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE REGELUNGEN

Das Trust Center der Deutschen Telekom Security GmbH liegt im Geltungsbereich einer vom Management freigegebenen Sicherheitsleitlinie und einem dazugehörigen Informationssicherheitsmanagementsystem (ISMS), welches nach ISO 27001 zertifiziert ist.

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

5.1 Physikalische Maßnahmen

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

5.1.1 Standort und Bauweise

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

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

Hinweis: Die Offline-CA befindet sich an einem anderen sicheren Standort außerhalb der Rechenzentren. Die nachfolgend aufgeführten Aussagen treffen jedoch auch auf den Standort der Offline-CA zu.

5.1.2 Physikalischer Zutritt

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

5.1.3 Stromversorgung und Klimatisierung

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

5.1.4 Wassereinwirkung

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

5.1.5 Brandvorsorge und Brandschutz

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

5.1.6 Aufbewahrung von Medien

Medien werden ausschließlich in den Betriebsräumen des Trust Centers, vor Feuer- und Wassereinwirkung sowie unberechtigtem Zugriff geschützt, aufbewahrt. Es werden keine Medien zur dauerhaften oder langfristigen Speicherung oder Archivierung eingesetzt.

5.1.7 Abfallentsorgung

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

5.1.8 Externe Sicherung

Keine Bestimmungen.

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

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

- Leiter TSP: trägt die gesamte Verantwortung für die bereitgestellten Dienste des Trust Centers

- Informationssicherheitsbeauftragter: plant und überwacht die Implementierung von Sicherheitsmaßnahmen, verantwortet Schwachstellenscans und Penetrationstests, leitet das ISMS
- ISMS-Teammitglied: unterstützt den Informationssicherheitsbeauftragten in seinen Aufgaben
- Administrator: konfiguriert und wartet die IT-Infrastruktur (Netzwerke, Datenbanken, Server etc.)
- CA Operator: generiert Root-CA-Schlüssel und Zertifikate
- Interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten Zertifikate, Prozesse, Dokumentationen und begutachtet die Konformität von Schlüssel- bzw. Root-Zeremonien
- Root-Team/Compliance-Team (PKI): koordiniert die Umsetzung von Anforderungen, überwacht Anforderungsquellen (Mailing-Listen, Root-Store-Policies, ETSI), übernimmt Außenkommunikation zu Root-Store-Betreibern und „Bugzilla“, berät bei Vorfällen und Änderungen, verantwortet CP, bearbeitet Anträge für CA-Ausstellungen

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

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

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

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

- Generierung, Sicherung und Wiederherstellung von CA-Schlüsseln
- Jegliche Tätigkeiten an der Offline-CA bzw. Zugriff auf die Offline-CA:
    - Ausstellung von Zertifikaten und Sperrlisten
    - Sperrung von Zertifikaten
    - Änderungen an der Konfiguration
- Jeglicher Zugriff auf die Offline-HSMs (inkl. Backup-HSMs)
- Bearbeitung von Anträgen für CA-Zertifikate
- Bewertung von Sicherheitsvorfällen
- Änderungen an der Konfiguration von CA-Systemen
- Änderungen an Zertifikatsprofilen

5.2.3 Identifizierung und Authentifizierung für jede Rolle

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

Vor der Übertragung einer vertrauenswürdigen Rolle (oder schon bei der Einstellung als Mitarbeiter) wird die entsprechende Person unter Vorlage eines amtlichen Ausweises persönlich identifiziert und es werden von dieser Person sowie der Leitung des Trust Centers

die Akzeptanz zur Übertragung der Rolle, der damit verbundenen Verantwortung und den daraus resultierenden Pflichten zur Gewährleistung der Sicherheit eingeholt.

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

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

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

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

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

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

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

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Folgende Rollen werden voneinander getrennt:

- Management/Leiter Trust Center
- IT-Sicherheitsbeauftragter/Compliance-/Root-TeamInterner Auditor
- Administrator/CA-Operator

5.3 Personelle Maßnahmen

5.3.1 Qualifikationen, Erfahrung und Berechtigungen

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

Die Mitarbeiter des Trust Centers erfüllen die Anforderung an hinreichendes Expertenwissen zur korrekten Ausübung ihrer Tätigkeiten aufgrund von Ausbildung, spezifischer Schulungen, langjähriger Erfahrung oder einer Kombination aus diesen. Darüber hinaus werden alle Mitarbeiter der Telekom Security und die des Trust Centers im Besonderen regelmäßig zu

allgemeinen Sicherheits- und Datenschutzbestimmungen, aktuellen Gefahren sowie den konkreten Vorgaben des ISMS informiert (bspw. vom ISMS oder konzernweiten Informationsveranstaltungen).

5.3.2 Verfahren zur Hintergrundprüfung

Alle Mitarbeiter in vertrauenswürdigen Rollen weisen ihre Vertrauenswürdigkeit durch regelmäßige Vorlage eines amtlichen Führungszeugnisses nach.

5.3.3 Schulungsanforderungen

Siehe Kap. 5.3.1.

5.3.4 Nachschulungsintervalle und -anforderungen

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

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Arbeitsplatzrotationen finden nicht statt.

5.3.6 Sanktionen bei unbefugten Handlungen

Mitarbeiter des Trust Centers sind rechenschaftspflichtig für ihr Handeln. Verstöße gegen Vorgaben haben, in Abhängigkeit der Schwere des Verstoßes, entsprechende arbeitsrechtliche Konsequenzen.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Nicht anwendbar, da im Umfeld der Root-CA kein externes Personal zum Einsatz kommt.

5.3.8 Dokumentation, die dem Personal zur Verfügung gestellt wird

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

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

enthalten.

5.4 Protokollierungsverfahren

5.4.1 Arten von Ereignissen, die protokolliert werden

5.4.1.1 Aktivitäten von Personen

Es werden alle Aktivitäten der Mitarbeiter des Trust Centers im Zusammenhang mit dem Lebenszyklus von CA-Zertifikaten und -Schlüsseln (Schlüsselgenerierung, -speicherung, -Backup, -wiederherstellung und -zerstörung, Generierung und Sperrung der CA-Zertifikate sowie die Lebenszyklen der HSMs) aufgezeichnet.

5.4.1.2 Technische Systemereignisse

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

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

Darüber hinaus werden alle (physikalischen) Ein- und Ausgänge zu den Sicherheitszonen protokolliert.

5.4.2 Häufigkeit der Log-Verarbeitung

Die in Kap. 5.4.1.1 aufgeführten Ereignisse werden in den jeweiligen Zeremonien protokolliert.

Die in Kap. 5.4.1.2 aufgeführten Ereignisse werden kontinuierlich durch die Systeme protokolliert (in den Systemen der Offline-CA nur solange diese im Rahmen einer Zeremonie in Betrieb sind).

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

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

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

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten werden für 7 Jahre über die Gültigkeit des jeweiligen Root-CA-Zertifikats hinaus aufbewahrt, dieses gilt auch bei

Beendigung eines Dienstes. Für qualifizierte Root-CA-Zertifikate werden die Aufzeichnungen dauerhaft aufbewahrt.

5.4.4 Schutz der Audit-Protokolle

Die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten an der Offline-CA werden vertraulich und integritätsgesichert und vor Zerstörung und Löschung geschützt aufbewahrt. Bei Papieranträgen bzw. Protokollen erfolgt dies im sicheren Papierarchiv des Trust Centers, bei elektronischen Anträgen (bspw. signierte PDF) erfolgt dies in dafür zugelassenen sicheren und dauerhaft verfügbaren elektronischen Ablagen.

Technische Systemereignisse der online-Systeme gemäß Kapitel 5.4.1.2 werden unverzüglich an eine separate und manipulationsgeschützte Log-Appliance gesendet.

5.4.5 Backup-Verfahren für Audit-Protokolle

Siehe Kap. 5.4.4.

5.4.6 Audit-Sammelsystem

Jegliche Protokolldaten technischer Ereignisse der online-Systeme werden unverzüglich nach der Generierung an ein zentrales und integritätsgeschütztes System (Log-Appliance) gesendet, welches speziell für die Sammlung und Sicherung von Protokolldaten konzipiert ist.

5.4.7 Benachrichtigung der Person, die ein Ereignis ausgelöst hat

Keine Bestimmungen.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Bestimmungen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Art der archivierten Datensätze

Es werden alle in Kap. 5.4.1.1 aufgeführten Daten archiviert.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Siehe Kap. 5.4.3.

5.5.3 Schutz von Archiven

Siehe Kap. 5.4.4.

5.5.4 Backup-Verfahren für Archive

Die elektronischen Ablagen zur Aufbewahrung der elektronisch signierten Anträge und ggf. digitalisierten Protokolle sind mehrfach redundant aufgebaut und werden regelmäßig gesichert.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Siehe Kap. 6.8.

5.5.6 Archivsystem (intern oder extern)

Es kommen ausschließlich interne Archivsysteme zum Einsatz.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

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

5.6 Schlüsselwechsel

Siehe Kap. 6.3.2.

5.7 Kompromittierung und Notfall-Wiederherstellung

5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

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

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

Sollte ein Vorfall einen Verstoß gegen eine Root Store Policy darstellen, so wird vom Trust Center Root-Team zeitnah ein Incident Report unter Berücksichtigung der jeweiligen Vorgaben

erstellt. Die Ausstellung betroffener Zertifikatstypen wird ggf. eingestellt, bis die Ursache beseitigt wurde oder weitere Schäden ausgeschlossen werden können.

5.7.2 Wiederherstellung bei Beschädigung von Computern, Software oder Daten

Siehe Kap. 5.7.1.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

Die Kompromittierung, der Verdacht auf Kompromittierung oder der Verlust eines privaten Root-CA-Schlüssels wird als Notfallszenario behandelt und entsprechend der in der Notfalldokumentation definierten Prozesse bearbeitet.

5.7.4 Geschäftsfortführung nach einem Notfall

Siehe Kap. 5.7.1.

5.8 Einstellung des CA oder RA Betriebes

Die Telekom Security verfügt über einen fortlaufend aktualisierten Beendigungsplan.

Im Falle einer Beendigung des Betriebs einer Root-CA sieht die Telekom Security vor, die Betreiber der betroffenen Sub-CAs frühzeitig zu informieren, so dass diese wiederum ihre Endkunden rechtzeitig informieren und ihre Dienste inkl. ihrer Endkunden möglichst vor Einstellung des Root-CA-Betriebs zu einer anderen Root-CA der Telekom Security oder eines anderen Betreibers migrieren können und damit mögliche Störungen für die Endteilnehmer vermeiden.

Eine geplante Beendigung wird frühzeitig auf den Web-Seiten des Trust Centers veröffentlicht, damit sich auch vertrauende Dritte frühzeitig darüber informieren können. Darüber hinaus werden die betroffenen Root-Stores explizit informiert.

Alle zum Zeitpunkt der geplanten Außerbetriebnahme einer Root-CA noch nicht gesperrten Sub-CA-, Cross- und Endteilnehmerzertifikate werden gesperrt, bevor die Root-CA endgültig außer Betrieb genommen wird.

Zur Außerbetriebnahme werden die privaten Schlüssel der Root-CA gemäß Kap. 6.2.10 gelöscht.

Der Betrieb der Statusdienste wird bis zum Ablauf der Gültigkeit aller Endteilnehmerzertifikate an die Deutsche Telekom AG übergeben, die als Vertrauensdienstanbieter (VDA) gemäß Vertrauensdienstegesetz fungiert. Ebenso werden die archivierten Aufzeichnungen der Deutschen Telekom AG zur Aufbewahrung bis zum Ablauf der festgelegten Aufbewahrungsfrist übergeben.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Hinweis: Da die Root-CA grundsätzlich keine Schlüssel für untergeordnete Sub-CAs und Endteilnehmer erzeugt, wird an dieser Stelle auf die Generierung solcher Schlüssel nicht eingegangen und stattdessen auf die CPS der jeweiligen Betreiber verwiesen, in denen die Umsetzung der diesbezüglichen Anforderungen aus der Telekom Security CP beschrieben sind. Bzgl. der Prüfung der Einhaltung der Anforderungen an die Generierung der Schlüssel einer Sub-CA sei auf Kap. 4.3 verwiesen.

Die Schlüssel einer Root-CA der Telekom Security werden in einem HSM gemäß Kap. 6.2.1 an der Offline-CA in der sicheren Umgebung des Trust Centers im Rahmen einer Root-CA-Zeremonie generiert, in der auch unmittelbar nach Erstellung der Schlüssel das Root-CA-Zertifikat erzeugt wird. Voraussetzung für die Generierung der Schlüssel ist, dass ein von der Leitung des Trust Centers freigegebener Antrag auf Ausstellung eines Root-CA-Zertifikats vorliegt, siehe dazu Kap. 4.1ff.

Die an der Zeremonie beteiligten vertrauenswürdigen Rollen und deren Aufgaben vor, während und nach der Schlüsselzeremonie sind in einer Arbeitsanweisung beschrieben. Dort ist auch festgelegt, welche Arbeitsschritte zur Schlüsselgenerierung und zum Backup im Mehr-Personen-Prinzip mit unterschiedlichen Rollen erfolgen müssen. Dazu zählen unter anderem

- das Starten der Offline-CA und des HSM inkl. der Integritätsprüfung des Systems,
- die Aktivierung des HSMs mittels geteilter Aktivierungsdaten,
- das Backup der Schlüssel auf mehrere Backup-HSM unter Verwendung geteilter Token („n von m“),
- das Herunterfahren der Offline-CA und des HSM inkl. Integritätssicherung des Systems,
- getrennte Aufbewahrung der Token zur Widerherstellung der Schlüssel aus dem Backup („n von m“).

Die Root-Zeremonien werden sowohl von einem qualifizierten internen Auditor als auch von einem qualifizierten externen Auditor einer Konformitätsbewertungsstelle (siehe Kapitel 8.2) überwacht. Nach korrekter Durchführung der Zeremonie bestätigt der interne Auditor dies im Protokoll der Zeremonie. Darüber hinaus erstellt die Konformitätsbewertungsstelle eine Audit-Bestätigung.

6.1.2 Bereitstellung der privaten Schlüssel an Antragsteller

Nicht anwendbar, da die privaten Schlüssel für Sub-CAs von den Antragstellern selbst in sicheren Umgebungen generiert werden müssen.

6.1.3 Übergabe öffentlicher Schlüssel an Zertifikatausssteller

Öffentliche Schlüssel zu beantragten Sub-CA-Zertifikaten werden mittels signiertem CSR an die Offline CA übergeben.

Die Schlüssel für Root-CAs werden an der Offline CA selbst generiert und müssen nicht übergeben werden.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

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

6.1.5 Schlüssellängen

Für Root-CAs werden ausschließlich RSA-Schlüssel mit einer Schlüssellänge von 4096 Bit und einer durch 8 teilbaren Länge des Moduls oder EC-Schlüssel der Kurve secp384r1 (NIST P-384) verwendet. Für qualifizierte Root CAs sind zudem EC-Schlüssel der Kurve secp521r1 (NIST P-521) erlaubt.

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

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

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

6.1.7 Schlüsselverwendung

Die privaten Schlüssel der Root-CAs werden ausschließlich zur Signatur von CA-Zertifikaten, delegierten OCSP-Signer-Zertifikaten und Sperrlisten verwendet.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

Die Root-CA-Schlüssel werden ausschließlich in HSM erzeugt und verwendet, welche nach FIPS 140-2 Level 3 zertifiziert sind und auch in dem entsprechenden FIPS-Modus betrieben werden.

6.2.2 Mehrpersonenkontrolle über private Schlüssel (n von m)

Die Generierung und Nutzung der privaten Root-Schlüssel im HSM sowie das Wiederherstellen der Schlüssel aus einem Backup ist nur im Vier-Augen-Prinzip möglich, siehe dazu Kap. 6.2.4 und 6.2.8. Beim Import und Export der Schlüssel in die bzw. aus den Backup-

HSM kommen Authentisierungstoken zum Einsatz, über die das „n von m“ Prinzip umgesetzt wird.

6.2.3 Hinterlegung privater Schlüssel

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

6.2.4 Sicherung privater Schlüssel

Die privaten Schlüssel der Root-CAs werden im Rahmen der Key-Zeremonie zur Schlüsselgenerierung (siehe Kap. 6.1.1) ausschließlich auf zwei Backup-HSM kopiert, welche unter einem zum Betrieb der Offline CA vergleichbaren Sicherheitsniveau aufbewahrt werden. Der Zugriff auf die Backup-HSM zur Rücksicherung der Schlüssel in ein HSM ist nur über Authentisierungstoken nach dem „n von m“ Prinzip möglich. Die Token werden an mehrere Mitarbeiter in unterschiedlichen vertrauenswürdigen Rollen vergeben und getrennt voneinander sicher aufbewahrt.

6.2.5 Archivierung privater Schlüssel

Eine Archivierung von privaten Schlüsseln der Root-CAs findet nicht statt.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Die privaten Schlüssel der Root-CAs werden in Backup-HSM gesichert (siehe Kap. 6.2.4) und können ausschließlich über diese Backup-HSM in weitere kompatible operative HSM transferiert bzw. zurückgesichert werden.

6.2.7 Speicherung privater Schlüssel in kryptografischen Modulen

Die privaten Schlüssel der Root-CAs werden ausschließlich in HSM oder Backup-HSM generiert, gespeichert und angewendet (siehe Kap. 6.1.1, 6.2.4 und 6.2.6).

Eine Aufbewahrung außerhalb der operativen HSM oder Backup-HSM ist nicht möglich.

6.2.8 Methoden zur Aktivierung privater Schlüssel

Die HSM mit den privaten Schlüsseln der Root-CAs können aufgrund der Aufteilung der Passwörter zur Aktivierung auf zwei Personen in unterschiedlichen Rollen ausschließlich im Vier-Augen-Prinzip aktiviert werden. Die Einhaltung des Vier-Augen-Prinzips wird durch einen Auditor überwacht und protokolliert.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

Die HSM mit den privaten Schlüsseln der Root-CAs werden am Ende einer jeden Root-Zeremonie im Vier-Augen-Prinzip deaktiviert und heruntergefahren. Die Einhaltung des Vier-Augen-Prinzips wird durch einen Auditor überwacht und protokolliert.

6.2.10 Methoden zur Zerstörung privater Schlüssel

Die privaten Schlüssel werden am Ende des Lebenszyklus des korrespondierenden Root-CA-Zertifikats, d.h. mit Ablauf der Gültigkeitsdauer oder der Außerbetriebnahme bzw. Beendigung des Dienstes, zerstört und nicht weiterverwendet. Die Zerstörung der Schlüssel erfolgt wie die Generierung von Root-CA-Schlüsseln in einer Zeremonie im Beisein der Auditoren (siehe Kap. 6.1.1) und berücksichtigt alle Kopien der Schlüssel.

Die Schlüssel werden mit den Bordmitteln der FIPS 140-2 Level 3 zertifizierten HSM zerstört.

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

6.2.11 Bewertung kryptografischer Module

Siehe Kap. 6.2.1.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des öffentlichen Schlüssels

Keine Bestimmungen.

6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Root-CA-Zertifikate werden mit einer Gültigkeitsdauer von maximal 25 Jahren ausgestellt. Die Schlüssel werden jedoch nur solange genutzt, wie die verwendeten Algorithmen als hinreichend sicher angesehen werden können. Darüber hinaus werden die Schlüssel bei Bedarf aus anderen Gründen (z.B. Ersatz des Root-CA-Zertifikats oder Beendigung des Betriebs) vorzeitig außer Betrieb genommen.

Sub-CA-Zertifikate werden mit einer Gültigkeitsdauer von maximal 10 Jahren ausgestellt.

Das Gültigkeitsende eines Sub-CA-Zertifikats überschreitet nicht das Gültigkeitsende des ausstellenden Root-CA-Zertifikats („Schalenmodell“).

Zur Gewährleistung eines ununterbrochenen Betriebs wird rechtzeitig vor Ablauf eines CA-Zertifikats oder dem Ende der Nutzbarkeit der Schlüssel ein Folgezertifikat ausgestellt.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Mit Inbetriebnahme eines HSM bzw. einer neuen Partition eines HSM werden die Passwörter zur Aktivierung im Mehr-Personen-Prinzip in der Form vergeben, dass jede Person nur einen Teil des gesamten Passworts vergibt.

6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten sind immer nur in Teilen den wissenden Personen bekannt (siehe Kap. 6.4.1). Für den Notfall werden die einzelnen Teile der Aktivierungsdaten an verschiedenen Stellen sicher hinterlegt, auf die keine Person alleinigen Zugriff hat.

6.4.3 Andere Aspekte der Aktivierungsdaten

Keine Bestimmungen.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Hinweis: Das Zertifikatsmanagementsystem der Root-CA wird als reine Offline-CA ohne jegliche Netzverbindung nach außerhalb des Systems betrieben, die Statusdienste der Root-CA (Sperrlisten, OCSP) sind jedoch online verfügbar. Die nachfolgenden Ausführungen gelten dementsprechend nur bedingt für die Offline-CA und betreffen teilweise nur die Systeme der online verfügbaren Statusdienste.

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

Die geforderte Trennung von vertrauenswürdigen Rollen (siehe Kap. 5.2.4) wird von allen notwendigen Systemen technisch unterstützt. Insbesondere werden die Accounts der für den Betrieb der kritischen Systeme erforderlichen vertrauenswürdigen Rollen (siehe Kap. 5.2.1) so verwaltet, dass der Zugriff auf die Systeme und Daten auf die für diese Rollen identifizierten und authentifizierten Personen (siehe Kap. 5.2.3) mit den minimal erforderlichen Berechtigungen beschränkt wird. Alle Accounts werden regelmäßig, mindestens aber alle 3 Monate, geprüft und bei Bedarf in angemessener Zeit geändert oder gelöscht.

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

Die CA-, Zertifikatsmanagement-, Sicherheits- und Frontend-Systeme sowie, falls anwendbar, weitere interne Systeme zur Unterstützung des Betriebs werden standardmäßig nach konzernweiten Vorgaben bzw. Best Practices gehärtet, d.h. für den Betrieb der CAs nicht benötigte Accounts, Dienste, Protokolle und Ports werden deaktiviert.

Die Systeme der Telekom Security werden mit einem Integritätsschutz versehen, der vor Viren, Schadcode und dem Einspielen unerlaubter Software schützt, und hinsichtlich Auslastung und verfügbarer Ressourcen überwacht, um einen ununterbrochenen Betrieb zu gewährleisten. Diese und weitere Sicherheitsmaßnahmen für Systeme des Trust Centers sind im Sicherheitskonzept beschrieben.

Die zur Zertifikatserzeugung und ggf. -sperrung erfassten Daten inkl. der Protokolldaten gemäß Kap. 5.4.1 werden so gesichert, dass deren Integrität, Vertraulichkeit und Verfügbarkeit über den gesamten Aufbewahrungszeitraum sichergestellt ist.

Die Entwicklungs-, Test- und Produktivumgebungen des Trust Centers werden auf unterschiedlicher Hardware in unterschiedlichen Netzsegmenten betrieben und sind daher gänzlich voneinander getrennt.

6.5.2 Sicherheitsbewertung von Computern

Keine Bestimmungen.

6.6 Technische Kontrollen des Lebenszyklus

Hinweis: Das Zertifikatsmanagementsystem der Root-CA wird als reine Offline-CA ohne jegliche Netzverbindung nach außerhalb des Systems betrieben, die Statusdienste der Root-CA (Sperrlisten, OCSP) sind jedoch online verfügbar. Die nachfolgenden Ausführungen gelten dementsprechend nur bedingt für die Offline-CA und betreffen teilweise nur die Systeme der online verfügbaren Statusdienste.

6.6.1 Steuerung der Systementwicklung

Die Telekom Security steht im regelmäßigen und engen Austausch mit dem Software-Lieferanten der Offline-CA und hat die OCSP-Systeme zur Statusauskunft selbst entwickelt, so dass die Berücksichtigung der Sicherheitsanforderungen bei der Systementwicklung sowohl für das Zertifikatsmanagement als auch die Statusdienste sichergestellt ist.

6.6.2 Maßnahmen des Sicherheitsmanagements

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

Alle Änderungen, die sich auf das festgelegte Sicherheitsniveau auswirken, werden zuvor von der Leitung des Trust Centers freigegeben.

Das Schwachstellenmanagement des Trust Centers ist so geregelt, dass

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

Die Systeme loggen, soweit möglich, alle sicherheitsrelevanten Ereignisse. Dabei werden die Systeme unter anderem auf folgende Aktivitäten überwacht (inkl. geeigneter Alarmierungsfunktionen):

- Sicherheitsrelevante Systemereignisse, dazu zählen:
  - erfolgreiche und erfolglose Zugriffsversuche auf die Zertifikatssysteme,
  - durchgeführte Tätigkeiten an den Zertifikats- und Sicherheitssystemen,
  - Starten und Abschalten der Protokollierungsfunktionen,
- Verfügbarkeit und Nutzung der benötigten Dienste,
- Änderungen von Sicherheitsprofilen,
- Installation, Aktualisierung und Entfernung von Software auf einem Zertifikatssystem,
- Systemabstürze, Hardware-Ausfälle und andere Anomalien,
- Firewall und Router-Aktivitäten und
- Zu- und Austritte in und aus den Betriebsräumen der Zertifikatsmanagementsysteme.

Die 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 Telekom Security überwacht den Kapazitätsbedarf der Systeme, um sicherzustellen, dass dauerhaft angemessene Verarbeitungsleistungen und Speicherkapazitäten zur Verfügung stehen.

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

6.6.3 Sicherheitskontrollen während des Lebenszyklus

Der Einsatz kryptographischer Schlüssel und Algorithmen berücksichtigt neben stets aktualisierten Konzernvorgaben die Empfehlungen aus Standards von anerkannten Institutionen wie dem BSI, SOGIS etc.

6.7 Netzwerk-Sicherheitskontrollen

Hinweis: Das Zertifikatsmanagementsystem der Root-CA wird als reine Offline-CA ohne jegliche Netzverbindung nach außerhalb des Systems betrieben. Die nachfolgenden Ausführungen gelten dementsprechend ausschließlich für die Systeme der online verfügbaren Statusdienste (Sperrlisten, OCSP) der Root-CA.

Die internen Netze und Systeme werden mithilfe von mehrstufigen Firewalls, IDS und IPS, Zoning sowie weiteren Schutzmaßnahmen vor unautorisierten Zugriffen und Angriffen geschützt. Alle Netzwerkkomponenten sind dabei so konfiguriert, dass nur die minimal erforderlichen Protokolle, Dienste und Zugänge verfügbar sind.

Die Segmentierung des Netzwerks basiert auf einer Risikobetrachtung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehungen zwischen vertrauenswürdigen Systemen und Diensten.

Alle für den CA-Betrieb kritischen Systeme werden in sicheren oder hochsicheren Zonen untergebracht. Die Kommunikation zwischen Systemen innerhalb der Sicherheitszonen wird durch entsprechend implementierte und konfigurierte Sicherheitsverfahren geschützt.

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

Innerhalb einer Zone gelten für alle Systeme die gleichen Mindestsicherheitsanforderungen.

Zwischen den Zonen sind Firewalls implementiert, welche die Systeme und Kommunikation innerhalb der sicheren Zonen sowie die Kommunikation mit den Systemen außerhalb der Zonen schützen. Die Verbindungen sind so eingeschränkt, dass nur die zum Betrieb erforderlichen Verbindungen möglich sind, nicht benötigte Verbindungen werden explizit verboten oder deaktiviert.

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

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

Die Kommunikation zwischen allen vertrauenswürdigen sowie weiteren Systemen ist grundsätzlich auf mehreren Schichten verschlüsselt und wird für fast alle Systeme, mindestens jedoch für die vertrauenswürdigen Systeme, über vertrauenswürdige Kanäle realisiert, die sich logisch von anderen Kommunikationskanälen unterscheiden und eine sichere Identifizierung ihrer Endpunkte gewährleisten.

Alle externen Netzwerkverbindungen sind redundant aufgebaut.

Nach jeder signifikanten System- oder Netzwerkänderung erfolgt i.d.R. innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenprüfung an vom Trust Center identifizierten öffentlichen und privaten IP-Adressen. 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.

Bei Inbetriebnahme, signifikanten Änderungen an der Infrastruktur bzw. Anwendungen, mindestens jedoch einmal pro Jahr werden die Systeme Penetrationstests unterzogen. Die Penetrationstests werden von Personen oder Organisationen durchgeführt, die über die für eine zuverlässige Prüfung und Dokumentation erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung der Penetrationstests mit Angabe der Qualifikation der prüfenden Person oder Organisation wird durch das ISMS kontrolliert und zusammen mit den Ergebnissen dokumentiert.

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

6.8 Zeitstempel

Die Zeitinformation der Offline-CA wird zu Beginn einer jeden Zeremonie geprüft, um sicherzustellen, dass die Zertifikate und Sperrlisten mit der Angabe korrekter Zeitinformationen signiert werden.

Die Systeme der OCSP-Responder werden gemäß Kap. 5.5 regelmäßig über den Zeitserver mit verlässlichen Zeitinformationen synchronisiert, so dass die OCSP-Antworten mit der Angabe korrekter Zeitinformationen signiert werden.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

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

Alle Zertifikatsprofile entsprechen dem RFC5280 sowie den Empfehlungen der ITU-T X.509. Alle von einer Root-CA ausgestellten Zertifikate erhalten eine eindeutige, zufällige Seriennummer mit einer Länge zwischen 64 und 126 Bit.

7.1.1 Versionsnummer

Alle X509-Zertifikate werden in der Version 3 ausgestellt.

7.1.2 Zertifikatserweiterungen

Die Root-CA-Zertifikate der Telekom Security erhalten ausschließlich folgende Zertifikatserweiterungen:

- authorityKeyIdentifier (nur qualifizierte Root CAs):
  Die Erweiterung authorityKeyIdentifier wird mit dem „keyIdentifier“ gem. RFC5280 #4.2.1.1 gesetzt und nicht als kritisch markiert.
- subjectKeyIdentifier:
  Die Erweiterung subjectKeyIdentifier wird mit dem „keyIdentifier“ gem. RFC5280 #4.2.1.1 gesetzt und nicht als kritisch markiert.
- keyUsage:
  Die Erweiterung keyUsage wird mit den Werten „keyCertSign“ und „cRLSign“ gesetzt und als kritisch markiert.
- basicConstraints;
  In der Erweiterung basicConstraints wird der Wert des „cA“-Flags auf „true“ gesetzt, eine maximale Pfadlänge wird nicht angegeben. Die Erweiterung wird als kritisch markiert.

In den von der Telekom Security ausgestellten Sub-CA-Zertifikaten werden die o.g. Erweiterungen der Root-CA-Zertifikate analog gesetzt. Darüber hinaus werden ausschließlich folgende Erweiterungen gesetzt:

- authorityKeyIdentifier:
  Die Erweiterung authorityKeyIdentifier wird mit dem Wert des subjectKeyIdentifier des ausstellenden Root-CA-Zertifikats gesetzt und als nicht kritisch markiert.
- CertificatePolicies (optional, Pflicht nur bei SSL):
  Die Erweiterung certificatePolicies in Sub-CA-Zertifikaten zur Ausstellung von TLS-Serverzertifikaten enthält mindestes die entsprechende Policy-OID der Baseline Requirements (siehe Kapitel 7.1.6).
- ExtendedKeyUsage:
  Die Erweiterung extendedKeyUsage wird wie folgt gesetzt:

- In Sub-CA-Zertifikaten, die zur Ausgabe von TLS-Serverzertifikaten genutzt werden, werden ausschließlich „id-kp-serverAuth“ und optional „id-kp-clientAuth“ gesetzt.
- In Sub-CA-Zertifikaten, die zur Ausgabe von S/MIME-Zertifikaten genutzt werden, werden ausschließlich „id-kp-emailProtection“ und optional „id-kp-clientAuth“ gesetzt.

Die Erweiterung wird als nicht kritisch markiert.

- cRLDistributionPoints:
  Die Erweiterung cRLDistributionPoints wird mindestens mit einer http-URL gesetzt, welche auf die CARL der Root-CA, welche das Sub-CA-Zertifikat ausgestellt hat, verweist.
- authorityInfoAccess:
  Die Erweiterung authorityInfoAccess wird mindestens mit einer http-URL gesetzt, die auf den OCSP-Responder der Root-CA, welche das Sub-CA-Zertifikat ausgestellt hat, verweist (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)).
  In Sub-CA-Zertifikaten, die zur Ausgabe von TLS-Serverzertifikaten genutzt werden, wird darüber hinaus eine http-URL gesetzt, die einen Downloadpunkt des Root-CA-Zertifikats enthält (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).

Telekom Security betreibt derzeit keine technisch eingeschränkten CAs, die Erweiterung nameConstraints wird daher nicht gesetzt.

In qualifizierten Sub-CA-Zertifikaten kann zudem eine Erweiterung für das Kettenmodell aufgenommen werden.

7.1.3 Algorithmen-OID

Es werden die folgenden Signatur-Algorithmen verwendet:

- sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
- sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13)
- RSASSA-PSS (OID 1.2.840.113549.1.1.10)
  - MGF-1 with SHA-256 and a salt length of 32 bytes
  - MGF-1 with SHA-384 and a salt length of 48 bytes
  - MGF-1 with SHA-512 and a salt length of 64 bytes
- ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)
- ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)
- ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4)

7.1.4 Namensformen

Es werden in den subjectDN von CA-Zertifikaten ausschließlich folgende Attribute aufgenommen:

- commonName
- organizationName
- countryName
- organizationalUnit (nur qualifizierte Zertifikate)
- organizationIdentifier (nur qualifizierte Zertifikate)

7.1.5 Namensbeschränkungen

In CA-Zertifikaten werden keine Namensbeschränkungen gesetzt.

7.1.6 OIDs der Erweiterung „CertificatePolicies“

In Sub-CA-Zertifikaten für die Ausstellung von TLS-Server-Zertifikaten werden die OIDs der Baseline Requirements verwendet:

- 2.23.140.1.2.1 (Domain Validation)
- 2.23.140.1.2.2 (Organizational Validation)
- 2.23.140.1.2.3 (Individual Validation)
- 2.23.140.1.1 (Extended Validation)

In Sub-CA-Zertifikaten für die Ausstellung von SMIME-Zertifikaten werden die OIDs von ETSI gesetzt:

- 0.4.0.2042.1.1 (NCP)
- 0.4.0.2042.1.2 (NCP+)
- 0.4.0.2042.1.3 (LCP)

In qualifizierten Sub-CA-Zertifikaten werden die OIDs entsprechend den Anforderungen gesetzt (siehe dazu die spezifische CPS).

7.1.7 Verwendung der Erweiterung „Policy Constraints“

Die Erweiterung „Policy Constraints“ wird nicht gesetzt.

7.1.8 Syntax und Semantik der „Policy Qualifier“

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

7.1.9 Verarbeitungssemantik für die kritische Erweiterung „Certificate Policies“

Die Erweiterung „Certificate Policies“ wird nicht als kritisch markiert, sodass es im Ermessen der Zertifikatsnutzer liegt, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

Alle Sperrlisten werden gemäß den Anforderungen des RFC 5280 ausgestellt und werden von der jeweiligen Root-CA signiert.

7.2.1 Versionsnummer(n)

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

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Alle Sperrlisten für CA-Zertifikate enthalten die CRL-Erweiterung AuthorityKeyIdentifier und cRLNumber sowie die CRL-Eintragserweiterung reasonCode. Die CRLReason ist nicht als kritisch gekennzeichnet und wird so gewählt, dass er den am besten geeigneten Grund für die Sperrung angibt. Unterstützte Werte sind: keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5). Andere CRLReason werden nicht angewandt.

7.3 OCSP-Profil

Alle OCSP-Antworten werden gemäß den Anforderungen des RFC 6960 ausgestellt und von einem delegierten OCSP-Signer signiert, dessen Zertifikat von der jeweiligen Root-CA ausgestellt wurde. Alle OCSP-Signer-Zertifikate enthalten die Erweiterung id-pkix-ocsp-nocheck mit dem Wert NULL und haben eine Gültigkeitsdauer von 3 Monaten.

In OCSP-Antworten für CA-Zertifikate, die widerrufen wurden, ist das Feld revocationReason innerhalb der RevokedInfo des CertStatus vorhanden. Die angegebene CRLReason enthält einen für CRLs zulässigen Wert, wie in Abschnitt 7.2.2 spezifiziert.

7.3.1 Versionsnummer(n)

Es wird OCSP in der Version 1 gemäß RFC 6960 eingesetzt.

7.3.2 OCSP-Erweiterungen

Keine Bestimmungen.

8 AUDITS UND ANDERE BEWERTUNGS-KRITERIEN

Alle unter diese CPS fallenden CA-Zertifikate werden öffentlich bekannt gegeben und in Übereinstimmung mit den Anforderungen dieses Kapitels vollständig geprüft.

8.1 Häufigkeit und Art der Prüfungen

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

Darüber hinaus werden alle Schlüsselgenerierungen und Zertifikatsausstellungen für Root-CAs durch externe Auditoren überwacht. Sub-CA-Zertifikate für den DFN werden nur ausgestellt, wenn Nachweise vorliegen, dass die zugehörige Schlüsselgenerierung von einem externen Auditor überwacht und für konform befunden wurde.

Es werden grundsätzlich alle Tätigkeiten an der Offline-CA durch einen internen Auditor überwacht, welcher auf die Einhaltung von organisatorischen und technischen Maßnahmen achtet. Sub-CA-Zertifikate für das Trust Center werden nur ausgestellt, wenn Nachweise vorliegen, dass die zugehörige Schlüsselgenerierung von einem internen Auditor überwacht und für konform befunden wurde.

8.2 Identität/Qualifikation der Prüfer

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

- Die Auditoren sind unabhängig vom Prüfgegenstand
- Die Auditoren können Prüfungen durchführen, welche die in geeigneten Prüfungsschemata gemäß Kap. 8.4 festgelegten Kriterien erfüllen,
- Die Auditoren sind kompetent in der Prüfung von PKI-Technologien, Informationssicherheits-Tools und -Techniken, Informationstechnologien und Sicherheitsüberprüfungen und beherrschen die Funktion der Bestätigung als Drittpartei.
- Die Auditoren sind durch Gesetz, staatliche Vorschriften oder berufsethische Regeln gebunden.
- Die Auditoren unterhalten eine Berufshaftpflicht-, Fehler- und Unterlassungsversicherung mit einer Deckungssumme von mindestens einer Million US-Dollar.
- Die Auditoren sind gemäß ISO 17065 unter Anwendung der in ETSI EN 319 403 festgelegten Anforderungen akkreditiert.

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

8.3 Beziehung des Prüfers zur geprüften Stelle

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

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

8.4 Abgedeckte Bereiche der Prüfung

Die Root-CAs inklusive aller dazugehörigen Prozesse, Systeme, Infrastrukturen und organisatorischen Maßnahmen sind Teil der Zertifizierungen nach den aktuellen Versionen der ETSI EN 319 411-1 bzw. der ETSI EN 319 411-2. Die folgenden Policies werden angewandt:

- T-TeleSec GlobalRoot Class 2: LCP, NCP, NCP+, DVCP, OVCP
- T-TeleSec GlobalRoot Class 3: EVCP, QCP-wTeleSec qualified Root CA 1: QCP-n-qscd
- Telekom Security ECC Root 2020: LCP, NCP, NCP+, OVCP
- Telekom Security RSA Root 2020: LCP, NCP, NCP+, OVCP
- Telekom Security TLS ECC Root 2020: DVCP, OVCP, EVCP, IVCP, QCP-w
- Telekom Security TLS RSA Root 2020: DVCP, OVCP, EVCP, IVCP, QCP-w
- Telekom Security SMIME ECC Root 2021: LCP, NCP, NCP+
- Telekom Security SMIME RSA Root 2021: LCP, NCP, NCP+

8.5 Maßnahmen infolge von Mängeln

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

Darüber hinaus werden jegliche, festgestellte Mängel schnellstmöglich beseitigt. Hierbei werden die Fristen des Trust Center ISMS und weiterer interner Vorgaben sowie bei externen Prüfungen nach ETSI die folgenden Fristen je nach Einstufung eines Findings eingehalten:

- Recommendation: Innerhalb von 12 Monaten
- NC-B: Innerhalb von 3 Monaten
- NC-A: Zertifizierungsverhindernd, Beseitigung wird unverzüglich vorgenommen.

8.6 Mitteilung der Ergebnisse

Die von externen Prüfern erstellten Audit-Bescheinigungen aller CAs werden unverzüglich, spätestens jedoch innerhalb von 3 Monaten in der „Common CA Database“ (CCADB) veröffentlicht. Im Falle einer Verzögerung von mehr als drei Monaten wird das Trust Center ein vom externen Prüfer unterzeichnetes Erläuterungsschreiben vorlegen.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

Die Höhe der zu entrichtenden Entgelte für die Ausstellung oder Erneuerung von CA-Zertifikaten ist in den internen und externen Verträgen geregelt.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Es werden keine Entgelte für den Zugriff auf CA-Zertifikate erhoben.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

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

9.1.4 Entgelte für andere Leistungen

Die Höhe ggf. zu entrichtender Entgelte für andere Leistungen ist in den internen und externen Verträgen geregelt.

9.1.5 Erstattung von Entgelten

Die Erstattung von Entgelten ist in den internen und externen Verträgen geregelt.

9.2 Finanzielle Verantwortlichkeiten

9.2.1 Versicherungsschutz

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

9.2.2 Sonstige finanzielle Ressourcen

Die Telekom Security verfügt als 100%-Tochter der Deutschen Telekom AG über die finanzielle Stabilität und Ressourcen, die zu einem zur Telekom Security CP konformen Betrieb inkl. einer geplanten Einstellung gemäß Kap.5.8 erforderlich sind. Dazu ist ein Beherrschungs- und Gewinnabführungsvertrag geschlossen, in dem geregelt ist, dass die Deutsche Telekom AG alle Verluste der Telekom Security übernimmt.

9.2.3 Versicherungs- oder Garantiedeckung für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

Die Telekom Security schützt vertrauliche Geschäftsinformationen entsprechend ihrer Klassifizierung.

9.3.1 Umfang an vertraulichen Informationen

Die Telekom Security unterliegt den konzernweiten Richtlinien der Deutsch Telekom AG zum Schutz vertraulicher Informationen. Alle Informationen werden nachfolgenden Schutzklassen eingestuft:

- offen
- intern
- vertraulich
- vertraulich (Kunde)

Als vertrauliche Informationen im Sinner dieser CPS gelten alle Informationen, die gemäß der o.g. Klassifizierung nicht als „offen“ eingestuft sind. Das sind alle Informationen, die nicht explizit als „nicht vertraulich“ in Kap. 9.3.2 aufgeführt sind.

9.3.2 Umfang an nicht vertraulichen Informationen

Nicht vertrauliche Informationen im Sinne dieser CPS sind alle veröffentlichten Informationen zu CA-Zertifikaten. Dazu zählen unter anderem

- die veröffentlichten und verlinkten Informationen im Repository des Trust Centers,
- die in der CCADB veröffentlichten Informationen,
- die in „Bugzilla“ (https://bugzilla.mozilla.org/) oder sonstigen Diskussionsforen von der Telekom Security veröffentlichten Informationen,
- die in der EU-TSL veröffentlichen Informationen.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Alle Mitarbeiter der Telekom Security sind dazu verpflichtet, die Konzernvorgaben zum Umgang mit vertraulichen Informationen zu berücksichtigen und einzuhalten. Hierzu werden bei der Einstellung und in regelmäßigen Abständen Schulungen zur korrekten Einstufung von Informationen gemäß der o.g. Schutzklassen sowie zu daraus resultierenden Maßnahmen durchgeführt. Auftragnehmer oder Dritte werden ebenfalls vertraglich zur Einhaltung der Konzernvorgaben verpflichtet.

9.4 Schutz von personenbezogenen Daten

9.4.1 Datenschutzkonzept

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

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

Zum Schutz der personenbezogenen Daten werden im Betrieb der Offline-CA inkl. der Registrierungsprozesse angemessene technische und organisatorische Maßnahmen getroffen, welche regelmäßig im Rahmen eines konzernweit verbindlichen Verfahrens geprüft werden. Das erfolgreiche Durchlaufen dieses Verfahrens ist die Voraussetzung für die dauerhafte datenschutzrechtliche Freigabe des Betriebs.

9.4.2 Als vertraulich zu behandelnde personenbezogene Informationen

Alle personenbezogenen Daten, die von der Telekom Security verarbeitet werden, gelten als schützenswert, sofern sie nicht über andere Wege ohnehin öffentlich verfügbar sind und somit gemäß Kap. 9.4.3 als nicht vertraulich geltende Informationen eingestuft sind.

9.4.3 Nicht als vertraulich zu behandelnde personenbezogene Informationen

Nicht als vertraulich geltende personenbezogene Informationen, die von der Telekom Security verarbeitet werden, sind alle Informationen über die betroffenen Personen, die öffentlich zugänglich sind, z.B. über die Web-Seiten der Betreiber der Sub-CAs, Handelsregisterauszüge, etc. Hierzu zählen auch die sich aus der Kommunikation ergebenden geschäftlichen Kontakte, z.B. geschäftliche Adressen, E-Mail-Adressen und Telefonnummern.

9.4.4 Verantwortung für den Schutz personenbezogener Informationen

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

9.4.5 Hinweis und Zustimmung zur Verwendung privater Informationen

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

9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

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

9.4.7 Andere Umstände der Offenlegung von Informationen

Nicht anwendbar.

9.5 Urheberrecht

Es gelten die gesetzlichen Vorschriften.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Root CAs

Die Telekom Security sichert einen zuverlässigen, vertrauenswürdigen, diskriminierungsfreien und legalen Betrieb der Dienstleistung sowie die Einhaltung der Konformität zur Telekom Security CP zu.

Darüber hinaus sichert die Telekom Security zu, angemessene Vorkehrungen zu treffen, um sicherzustellen, dass auch die TSP, die Sub-CA-Zertifikate von den öffentlichen und qualifizierten Telekom Root-CAs erhalten, ihre Dienstleistung zuverlässig, vertrauenswürdig und diskriminierungsfrei betreiben und die Konformität zur Telekom Security CP wahren.

Als Betreiber der Root-CAs informiert die Telekom Security die TSP, die Sub-CA-Zertifikate von den öffentlichen und qualifizierten Telekom Root-CAs erhalten, rechtzeitig über die etablierten Kommunikationskanäle über geplante und beschlossene Änderungen.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Die Telekom Security nutzt im Rahmen der Tätigkeiten als Betreiber der Root-CAs ausschließlich eigene Mitarbeiter für die Registrierungstätigkeiten, siehe daher Kap. 9.6.1.

9.6.3 Zusicherungen und Gewährleistungen der Antragsteller

Die TSP, welche Sub-CA-Zertifikate von einer öffentlichen Root-CA der Telekom Security beantragen oder besitzen, verpflichten sich

- genaue und vollständige Informationen zu liefern,
- das Schlüsselpaar nur in Übereinstimmung mit etwaigen Einschränkungen, die dem Antragsteller mitgeteilt wurden, zu verwenden,
- die privaten Schlüssel der CA zu keinem unerlaubten Zweck zu nutzen,

- den Betreiber der Root-CA unverzüglich zu benachrichtigen, wenn während der Gültigkeitsdauer eines Zertifikats eines der folgenden Ereignisse eintritt:
    - ein privater Schlüssel ist verloren gegangen, gestohlen oder möglicherweise kompromittiert worden,
    - die Kontrolle über einen privaten Schlüssel ist verloren gegangen, z.B. aufgrund einer Kompromittierung von Aktivierungsdaten oder aus anderen Gründen,
    - es werden Inkorrektheiten oder notwendige Änderungen der Zertifikatsinhalte festgestellt,
- nach Kompromittierung eines privaten Schlüssels die Verwendung dieses Schlüssels sofort und dauerhaft einzustellen,
- ein Zertifikat unverzüglich zu sperren oder sperren zu lassen, wenn ein Sperrgrund gemäß Kap.4.9.1 vorliegt.
- nach Sperrung eines Zertifikats die Verwendung des korrespondierenden privaten Schlüssels sofort und dauerhaft einzustellen,
- nach Bekanntwerden der Kompromittierung der ausstellenden Root-CA die Verwendung des privaten CA-Schlüssels sofort und dauerhaft einzustellen,
- zur Generierung der Schlüssel unter Verwendung geeigneter Algorithmen und Schlüssellängen gemäß Kap. 6.1.5,
- den privaten Schlüssel unter der Kontrolle zu halten,
- den privaten Schlüssel nur innerhalb sicherer kryptografischer Module zu verwenden,
- die Schlüssel innerhalb des sicheren kryptografischen Moduls zu generieren,
- alle angemessenen Maßnahmen zu ergreifen, um die Vertraulichkeit und Kontrolle über die privaten Schlüssel und Aktivierungsdaten zu gewährleisten,
- den Inhalt des Zertifikats auf Richtigkeit zu überprüfen,
- innerhalb eines angemessenen Zeitraums auf die Anweisungen des Betreibers der Root-CAs bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauch zu reagieren,
- zu akzeptieren, dass der Betreiber der Root-CA berechtigt ist, ein Zertifikat sofort zu sperren, wenn ein Sperrgrund gemäß Kap. 4.9.1 vorliegt,
- jede Änderung der Registrierungsdaten dem Betreiber der Root-CAmitzuteilen.

Darüber hinaus informiert die Telekom Security als Betreiber der Root-CA die TSP zu folgenden Aspekten:

- die anwendbare Policy gemäß ETSI EN 319 411-1 bzw. -2,
- eine Information, was als Akzeptanz des Zertifikats gilt,
- der Zeitraum, über den die Aufzeichnungen (siehe Kap. 5.5.2) aufbewahrt werden,
- die Anforderungen an vertrauende Dritte gemäß Kap. 9.6.4,
- ob und wenn ja, auf welche Art und Weise die Anforderungen der Telekom Security CP ergänzt oder weiter einschränkt werden,
- alle Beschränkungen der Nutzung des angebotenen Dienstes,
- die Haftungsbeschränkungen der Telekom Security als Betreiber der Root-CA,
- das anwendbare Recht,
- die Verfahren bei Beschwerden und zur Streitbeilegung,
- Häufigkeit und zugrundeliegende Auditschemata der Auditierungen gemäß Kap. 8.1 und 8.4,
- Kontaktinformationen des Betreibers der Root-CA,
- Aussagen zur Verfügbarkeit der bereitgestellten Dienste.

9.6.4 Zusicherungen und Gewährleistungen vertrauender Dritter

Siehe Kap. 4.5.2 und 4.9.6.

9.6.5 Zusicherungen und Gewährleistungen sonstiger Teilnehmer

Keine Bestimmungen.

9.7 Gewährleistungsausschlüsse

Etwaige Gewährleistungsausschlüsse werden in den internen und externen Vereinbarungen geregelt.

9.8 Haftungsbeschränkungen

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

Etwaige Haftungsbeschränkungen werden in den internen und externen Vereinbarungen geregelt und entsprechen grundsätzlich geltendem Recht.

9.9 Schadensersatz

Etwaige Schadenersatzansprüche der TSP gegenüber der Telekom Security werden in den internen und externen Vereinbarungen geregelt.

9.10 Laufzeit und Terminierung

9.10.1 Laufzeit

Dieses CPS gilt ab dem auf dem Deckblatt angegebenen Gültigkeitsdatum für alle neu ausgestellten und, falls anwendbar, bereits bestehende Zertifikate, solange es nicht widerrufen oder durch eine neue Version ersetzt wird.

9.10.2 Terminierung

Siehe 9.10.1.

9.10.3 Effekt einer Terminierung und Fortführungen

Siehe 9.10.1.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Bestimmungen.

9.12 Änderungen

Die Telekom Security informiert die TSP und, sofern anwendbar, Bewertungsstellen und Aufsichts- oder andere Regulierungsbehörden über relevante Änderungen, siehe dazu auch Kap. 1.5.4, 9.6.1 und 9.6.3.

9.12.1 Verfahren für Änderungen

Keine Bestimmungen.

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Keine Bestimmungen.

9.12.3 Umstände, unter denen der OID geändert werden muss

Keine Bestimmungen.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Etwaige Bestimmungen zwischen den Betreibern der Sub-CAs und der Telekom Security als Betreiber der Root-CAs werden in den internen und externen Vereinbarungen geregelt.

9.14 Geltendes Recht

Es gilt deutsches Recht.

9.15 Einhaltung geltenden Rechts

Die Telekom Security sichert zu, geltendes Recht einzuhalten.

9.16 Verschiedene Bestimmungen

9.16.1 Gesamte Vereinbarung

Keine Bestimmungen.

9.16.2 Abtretung

Keine Bestimmungen.

9.16.3 Salvatorische Klausel

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

9.16.4 Rechtsdurchsetzung

Keine Bestimmungen.

9.16.5 Höhere Gewalt

Keine Bestimmungen.

9.17 Sonstige Bestimmungen

Keine Bestimmungen.