Deutsche Telekom Security GmbH
Trust Center Certificate Practice Statement Public

Deutsche Telekom Security GmbH

Öffentlich

Version: 01.00

Gültig ab: 01.10.2021

Status: Freigegeben

Letztes Review: 23.09.2021

IMPRESSUM

Tabelle 1: Dokumenteneigenschaften

Eigenschaft	Wert
Herausgeber	Deutsche Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Deutschland
Dateiname	Telekom Security CPS Public DE V01.00.docx
Gültig ab	01.10.2021
Titel	Trust Center Certificate Practice Statement Public
Version	01.00
Letztes Review	23.09.2021
Status	Freigegeben
Ansprechpartner	Telekom Security Leiter Trust Center Betrieb
Kurzbeschreibung	Telekom Security CPS Public

ÄNDERUNGSHISTORIE

Tabelle 2: Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.9	01.08.2021	Telekom Security	Initialversion nach RFC 3647 Struktur
0.91	09.09.2021	Telekom Security	Korrektur von Auditfindings
01.00	24.09.2021	Telekom Security	Freigabe

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 eine Erklärung zum Zertifizierungsbetrieb (CPS) des Trust Centers der Telekom Security. Es beschreibt in der Struktur des RFC3647 die Umsetzung der Anforderungen aus

- der Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42),
- ETSI EN 319 401
- ETSI EN 319 411-1, ETSI EN 319 411-2
- den unter http://www.cabfourm.org veröffentlichten
    - „CA/Browser-Forum Baseline Requirements“ [BR],
    - „CA/Browser-Forum EV-Guidelines“ [EVCG],
    - “CA/Browser-Forum Network and Certificate System Security Requirements“,
- diversen Root Store Policies

an den Telekom Security PKI-Betrieb der neuen Generation und stellt somit eine Ergänzung zur Telekom Security Root CPS dar. Derzeit werden ausschließlich domainvalidierte TLS-Serverzertifikate angeboten.

Im Falle eines Widerspruchs zwischen dieser CPS, der Telekom Security CP und den oben referenzierten Quellen haben die Regelungen aus der Telekom Security CP und den oben referenzierten Quellen Vorrang.

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument trägt den Namen „Telekom Security CPS Public“ und wird durch die OID 1.3.6.1.4.1.7879.13.43 gekennzeichnet. Die OID ist wie folgt zusammengesetzt:

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Telekom Security CPS Public (43)}

Die verbindlichen Angaben zu Version, Gültigkeitsdatum und Status sind auf dem Deckblatt aufgeführt.

1.3 PKI-Teilnehmer

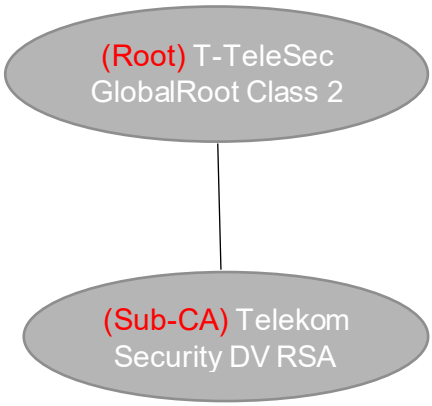
1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

Die folgenden Zwischenzertifizierungsstellen (Sub-CAs) sind im Gültigkeitsbereich dieser CPS:

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

Name	Schlüssel-typ	Seriennummer	Gültigkeitszeit-raum	Fingerprint
Telekom Security DV RSA CA 21	RSA 2048	2cf3c72f3f7d0f b31fc362d6b8 69558e	2021-04-21 bis 2031-04-21	99cc84f820818cf 0eefe81ddf572ca ce4b3acb78

Die Zwischenzertifizierungsstellen im Gültigkeitsbereich dieser CPS ordnen sich in folgende PKI-Hierarchien ein:



Die angegebenen Root CAs liegen im Geltungsbereich der Telekom Security Root CPS.

1.3.2 Registrierungsstellen (Registration Authorities, RA)

Das Trust Center der Telekom Security agiert selbst als die einzige RA für alle Zertifikate im Gültigkeitsbereich dieser CPS.

1.3.3 Endteilnehmer

Endteilnehmer sind alle natürlichen und juristischen Personen, welche EE-Zertifikate unter den oben genannten Zwischenzertifizierungsstellen beantragen oder besitzen.

1.3.4 Vertrauende Dritte

Vertrauende Dritte sind Personen oder IT-Prozesse, welche den unter dieser CPS ausgestellten 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

CA-Zertifikate werden ausschließlich zur Signatur von OCSP-Signer- und EE-Zertifikaten sowie Sperrlisten verwendet. Dabei werden die Zertifikatserweiterungen gemäß Kapitel 7.1.2 berücksichtigt.

Die zulässige Verwendung von EE-Zertifikaten wird durch die Zertifikatserweiterungen KeyUsage und ExtendedKeyUsage vorgegeben. Darüber hinaus hat der Endteilnehmer geltende gesetzliche Vorgaben einzuhalten.

1.4.2 Unzulässige Verwendung von Zertifikaten

CA-Zertifikate werden nicht für andere als den in Kapitel 1.4.1 aufgeführten Anwendungsfällen verwendet.

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

- Nukleare Einrichtungen
- Flugzeugnavigations- oder -kommunikationssysteme
- Luftverkehr-Kontrollsysteme
- Waffenkontrollsysteme

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-Programm 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 unter

https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

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

1.5.3 Person für die Feststellung der Konformität dieser CPS zur CP

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

1.5.4 Genehmigungsverfahren dieses CPS

Diese CPS wurde von der Leitung des Trust Centers freigegeben und behält seine Gültigkeit für neu ausgestellte Zertifikate sowie, soweit anwendbar, für bereits bestehende Zertifikate, solange sie nicht widerrufen oder durch eine neue Version ersetzt wird.

Diese CPS wird bei Bedarf, z.B. aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, mindestens aber einmal pro Jahr einem Review 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

Die Telekom Security betreibt zu allen CA-Zertifikaten ein Repository mit Informationen und Dokumenten (siehe Kap. 2.2) sowie Zertifikatsstatusdienste (siehe Kap. 4.9 bzw. 4.10).

2.2 Veröffentlichung von Informationen zu Zertifikaten

Die Telekom Security veröffentlicht im PKI-Repository auf den Web-Seiten des Trust Centers (https://www.telesec.de/de/service/downloads/pki-repository/) folgende Informationen bzw. Dokumente:

- Telekom Security CP
- Certificate Practice Statements (CPS, beinhaltet dieses Dokument)
- PKI Disclosure Statements (PDS)
- alle noch gültigen öffentlichen Root-CA-Zertifikate der Telekom Security
- alle von den öffentlichen Root-CAs der Telekom Security ausgestellten und noch gültigen Sub-CA-Zertifikate
- die Audit-Bestätigungen zu den öffentlichen Root-CA-Zertifikaten der Telekom Security (Verlinkung zu den Web-Seiten des Auditors).
- Leistungsbeschreibungen
- Allgemeine Geschäftsbedingungen (AGB)

Sowohl die CP als auch die Telekom Security CPS Public sind konform zum RFC3647 und werden in deutscher und englischer Sprache veröffentlicht, sowohl die jeweils gültige Version als auch alle relevanten abgelösten Versionen. Die deutschen und englischen Versionen eines Dokuments haben immer die gleiche Versionsnummer und werden inhaltlich synchronisiert. Im Streitfall ist jedoch die deutsche Version autoritativ.

Ergänzend zur Veröffentlichung im eigenen Repository veröffentlicht die Telekom Security alle erforderlichen Informationen zu CA-Zertifikaten in der „Common CA Database“ (CCADB) gemäß der CCADB-Policy (siehe https://www.ccadb.org).

Zu allen öffentlichen Root-CAs, unter denen TLS-Server-Zertifikate 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.

Die zugehörigen Links einer jeden Root-CA können auf der Webseite des Trust Centers eingesehen werden.

Alle ausgestellten EE-Zertifikate für TLS-Server-Authentifizierung werden vor ihrer endgültigen Ausstellung in einer den Anforderungen genügenden Anzahl an CTLogs veröffentlicht.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

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

- Die öffentlichen Root-CA-Zertifikate werden zu Beginn einer Root-Inklusion sowohl im eigenen Repository als auch in der CCADB veröffentlicht.
- Die 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.
- Die Audit-Bestätigungen werden innerhalb von 7 Tagen nach ihrer Ausstellung sowohl in der CCADB als auch im eigenen Repository veröffentlicht bzw. verlinkt.
- CP und CPS werden nach Freigabe einer neuen Version so bald wie möglich im Repository des Trust Centers veröffentlicht und an die CCADB kommuniziert.

2.4 Zugang zu den Verzeichnissen

Sowohl das o.g. Repository als auch die Zertifikatsstatusdienste sind für den lesenden Zugriff ohne Zugriffsbeschränkung 7x24 aus dem Internet 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

Siehe Kapitel 7.1.2 und 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 verdeutlicht.

Alle Zertifikate enthalten einen IssuerName, welcher identisch zum Subject Distinguished Name des ausstellenden CA-Zertifikats ist.

Alle TLS-Server-Zertifikate enthalten einen SubjectAlternativeName mit FQDNs, welche zu diesem Zertifikat gehören.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Domainvalidierte Zertifikate enthalten keinerlei Informationen zum Zertifikatsinhaber, wodurch grundsätzlich eine Anonymität des Zertifikatsnehmers gegeben ist.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Siehe Kapitel 7.1.2 und 7.1.4.

3.1.5 Eindeutigkeit von Namen

Alle unter einer jeweiligen Root-CA ausgestellten Sub-CA-Zertifikate erhalten einen einzigartigen CommonName und damit Subject Distinguished Name.

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

Für die Ausstellung eines Zertifikats ist ein mit dem privaten Schlüssel signierter Zertifikatsantrag notwendig.

3.2.2 Authentifizierung der Organisations -und Domain-Identität

Für die Ausstellung von domainvalidierten Zertifikaten ist die Authentifizierung von Organisationen nicht notwendig.

Die Validierung der Kontrolle eines Antragstellers über eine entsprechende Domain wird mithilfe der Funktionen des ACME-Protokolls überprüft. Diese sind:

1. (Methode nach CABF Baseline Requirements Kapitel 3.2.2.4.7)
   DNS Change
   Der Antragsteller weist die Kontrolle über einen FQDN durch Bestätigung des Vorhandenseins eines eindeutigen Zufallswert in einem DNS TXT oder CAA-Eintrag für den angeforderten FQDN mit der vorangestellten Bezeichnung „_acme_challenge“ nach. Diese Methode wird auch zur Validierung von Wildcard-Zertifikaten verwendet.

2. (Methode nach CABF Baseline Requirements Kapitel 3.2.2.4.19)
   Agreed-Upon Change to Website – ACME
   Der Antragsteller weist die Kontrolle über einen FQDN durch Nutzung der ACME http Challenge nach, wie in RFC 8555 Kapitel 8.3 definiert und durch die Anforderungen der Baseline Requirements ergänzt.

Für Wildcard-Zertifikate wird geprüft, ob das Wildcard-Zeichen „*“ (Stern, Asterisk) im ersten Label links eines „registry-controlled“ Label oder „public suffix“ (bspw. „.com“, Definition nach RFC 6454 Section) enthalten ist. In einem solchen Fall wird eine Zertifikatsausstellung abgelehnt, sofern der Antragsteller nicht seine rechtmäßige Kontrolle über den gesamten Domain Namespace nachweist.

3.2.3 Authentifizierung von natürlichen Personen

Für die Ausstellung von domainvalidierten Zertifikaten ist die Authentifizierung von natürlichen Personen nicht notwendig.

3.2.4 Nicht überprüfte Informationen

Keine Bestimmungen.

3.2.5 Validierung der Bevollmächtigung

Die Validierung der Bevollmächtigung geschieht im Rahmen von domainvalidierten Zertifikaten über den Nachweis der Domain-Kontrolle (siehe Kapitel 3.2.2) sowie die Berücksichtigung vorhandener CAA-Records.

3.2.6 Kritierien für Interoperabilität

Es werden keine Cross-Zertifikate ausgestellt.

3.3 Identifizierung und Authentifizierung für Zertifikatserneuerungen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Zertifikatserneuerungen

Zertifikatserneuerungen domainvalidierter Zertifikate werden wie Neu-Beauftragungen gehandhabt.

3.3.2 Identifizierung und Authentifizierung für Zertifikatserneuerungen nach einer Sperrung

Zertifikatserneuerungen domainvalidierter Zertifikate werden wie Neu-Beauftragungen gehandhabt.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Authentisierung von Sperranträgen zu TLS-Server-Zertifikaten geschieht über die Funktionen des ACME-Protokolls. Eine Identifizierung des Zertifikatsinhabers als berechtigter Sperrantragsteller kann zudem über die externe Account-Bindung und den zum Account gehörenden privaten Schlüssel erfolgen.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Zertifikatsanträge können grundsätzlich von allen natürlichen und juristischen Personen bzw. deren autorisierten Vertretern gestellt werden, sofern sie ein Kundenkonto beim Trust Center registriert haben.

4.1.2 Antragsprozess und -verantwortlichkeiten

Der Antragsprozess für Endteilnehmer-Zertifikate beinhaltet

- die Erstellung eines Accounts am ACME-Server mit Verknüpfung zum jeweiligen Kundenaccount (über ExternalAccountBinding-Schlüssel),
- die Generierung eines sicheren Schlüsselpaars,
- die Akzeptanz der Datenschutzhinweise, der Allgemeinen Geschäftsbedingungen, der Nutzungsbedingungen, des CPS sowie der Leistungsbeschreibung,
- die Bereitstellung eines Zertifikatsantrags inkl. öffentlichen Schlüssel durch den Antragsteller (bspw. über das ACME-Protokoll),
- die Bestätigung des Antragstellers, dass die im Zertifikatsauftrag angegebenen Informationen wahr und korrekt sind sowie die Schlüssel sicher generiert wurden.

4.2 Bearbeitung der Zertifikatsanträge

4.2.1 Durchführung der Identifizierung und Authentifizierung

Identifizierung und Authentifizierung werden im Kontext von Zertifikatsanträgen gemäß den in Kapitel 3.2 beschriebenen Verfahren durchgeführt. Damit verbundene manuelle Tätigkeiten werden ausschließlich von Personal in vertrauenswürdigen Rollen des Trust Centers der Telekom Security durchgeführt.

Darüber hinaus werden für TLS-Server-Zertifikate alle FQDN-Einträge im subjectAltName unmittelbar vor der Ausstellung eines Zertifikats gegen CAA-Einträge im DNS geprüft. Sollte kein CAA Ressource Record hinterlegt sein oder dessen issue bzw. issuewild-Property „telesec.de“ enthalten, wird die Ausstellung des Zertifikats fortgeführt. „iodef“-Einträge werden ausgewertet, jedoch nicht weiterverfolgt. Weitere Einträge des CAA Records werden nicht unterstützt.

Telekom Security pflegt für die Identifikation von High Risk Certificate Requests eine Datenbank mit Organisationsnamen und Domainnamen bzw. IP-Adressen, welche aufgrund ihrer Attraktivität ein erhöhtes Risiko besitzen, Ziel von Phishing-, Missbrauchs- oder Betrugsangriffen zu sein. Identifizierte High Risk Certificate Requests werden individuell betrachtet.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Ein Antrag zur Ausstellung von Zertifikaten wird vom Trust Center abgelehnt, wenn

- eine Validierung gemäß Kapitel 4.2.1 nicht vollständig abgeschlossen werden kann,
- im Falle eines High Risk Certificate Requests die Gefahr eines Missbrauchs nicht hinreichend ausgeschlossen werden kann,
- der Antrag für eine IP-Adresse aus einem reservierten Adressraum bzw. für einen internen Server-/Hostnamen gestellt wurde,
- der verwendete Schlüssel nicht den Qualitätskriterien entspricht oder kompromittiert ist,
- die CAA-Prüfung negativ ausfällt,
- ICANN die gTLD nicht freigegeben hat (die Liste der freigegebenen und gekündigten gTLD wird regelmäßig, spätestens jedoch alle 30 Tage über die ICANN-Webseite aktualisiert).

Telekom Security ist zudem berechtigt Zertifikatsanträge auch ohne Angabe von Gründen zu verweigern.

Wenn alle Validierungsschritte gemäß Kapitel 4.2.1 erfolgreich durchgeführt wurden und keiner der oben genannten Punkte zutrifft, wird die Zertifikatsausstellung genehmigt.

Im Falle einer Zurückstellung oder Ablehnung eines Auftrags wird der Zertifikatsantragsteller benachrichtigt.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Bestimmungen.

4.3 Ausstellung von Zertifikaten

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

Telekom Security stellt sicher, dass bei der Ausstellung der Zertifikate die Integrität und Authentizität der ins Zertifikat gelangenden Daten durch technische, organisatorische und personelle Maßnahmen gewährleistet wird.

4.3.2 Benachrichtigung des Antragstellers über die Ausstellung eines Zertifikats

Nach der Ausstellung eines Zertifikats wird der Antragsteller darüber informiert und das Zertifikat ist unmittelbar über das ACME-Protokoll verfügbar.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Keine Bestimmungen.

4.4.2 Veröffentlichung des Zertifikats durch die TSP

Siehe Kap. 2.2.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP

Siehe Kap. 2.2.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Antragsteller

Endteilnehmer werden über Allgemeine Geschäftsbedingungen verpflichtet, Zertifikate ausschließlich gemäß dieser CPS und den für das Zertifikat vorgesehenen Verwendungszwecken zu nutzen sowie die privaten Schlüssel über ihren gesamten Lebenszyklus zu schützen.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte

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

4.6 Zertifikatserneuerung unter Beibehaltung der Schlüssel (Renewal)

4.6.1 Umstände für ein Renewal

Ein Renewal von Zertifikaten wird wie eine Neu-Beauftragung gehandhabt.

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 Zertifikats-Neuausstellung

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 Zertifikatsausstellung 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 Zertifikaten wird wie eine Neu-Beauftragung gehandhabt.

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 Zertifikats-Neuausstellung

Nicht anwendbar.

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

Nicht anwendbar.

4.7.6 Veröffentlichung von Re-Key-Zertifikaten durch die TSP

Nicht anwendbar.

4.7.7 Information Dritter über die Zertifikatsausstellung durch den TSP

Nicht anwendbar.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Änderung von Zertifikatsdaten

Änderungen von Zertifikatsdaten werden wie Neu-Beauftragungen gehandhabt.

4.8.2 Antragsberechtigte für eine Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.3 Verarbeitung von Anträgen auf eine Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.4 Benachrichtigung des Endteilnehmers über die Zertifikats-Neuausstellung

Nicht anwendbar.

4.8.5 Verhalten, das die Annahme eines geänderten Zertifikats bestätigt

Nicht anwendbar.

4.8.6 Veröffentlichung geänderter Zertifikate durch die TSP

Nicht anwendbar.

4.8.7 Information Dritter über die Zertifikatsausstellung durch den TSP

Nicht anwendbar.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Sperrgründe

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 zum Telekom Security CPS Root herausgegeben wurde oder der Betreiber der Sub-CA nicht konform zum Root CPS 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.

Ein Endteilnehmer-Zertifikat wird innerhalb einer sehr kurzen Frist (24 Stunden für TLS-Server- Zertifikate) gesperrt, wenn

- ein schriftlicher Sperrantrag, auch ohne Angabe von Gründen, vom Endteilnehmer gestellt wurde,
- festgestellt wird, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- festgestellt wird, dass der private Schlüssel des Endteilnehmer-Zertifikats kompromittiert wurde oder einer unautorisierten Person oder einer nicht mit dem Endteilnehmer verbundenen Organisation übergeben wurde,
- festgestellt wird, dass es eine praktisch anwendbare Methode gibt, mit welcher der private Schlüssel aus dem öffentlichen Schlüssel berechnet werden kann (bspw. Debian Weak Key),
- wenn festgestellt wird, dass der Validierung der Domainautorisierung oder der Kontrolle über einen FQDN oder eine IP-Adresse im Zertifikat nicht vertraut werden kann.

Ein Endteilnehmer-Zertifikat wird möglichst innerhalb einer sehr kurzen Frist (24 Stunden für TLS-Server- Zertifikate), spätestens jedoch innerhalb einer mittleren Frist (5 Tage für TLS-Server -Zertifikate) gesperrt, wenn

- festgestellt wird, dass das Zertifikat nicht in Übereinstimmung mit der CPS der Sub-CA ausgestellt wurde,
- der private Schlüssel nicht mehr den Anforderungen aus Kap. 6.1.5 und 6.1.6 genügt, oder Methoden bekannt geworden sind, die den privaten Schlüssel des Zertifikatinhabers gefährden oder die Berechnung des privaten Schlüssels aus dem öffentlichen Schlüssel ermöglichen oder dass es eindeutige Beweise dafür gibt, dass die für die Generierung des privaten Schlüssels verwendete Methode mangelhaft war.
- festgestellt wird, dass das Zertifikat missbräuchlich eingesetzt wurde,
- festgestellt wird, dass der Endteilnehmer gegen eine oder mehrere wesentliche Vereinbarungen oder Nutzungsbedingungen verstoßen hat,
- festgestellt wird, dass die Informationen im Zertifikat nicht korrekt sind oder es wesentliche Änderungen gegeben hat,

- das Recht des TSP zur Ausstellung von Zertifikaten gemäß den Baseline Requirements des CA/Browser-Forums erloschen ist oder widerrufen oder gekündigt wurde und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden,
- festgestellt wird, dass die Verwendung eines FQDN oder einer IP-Adresse im Zertifikat nicht mehr gesetzlich zulässig ist,
- festgestellt wird, dass ein Wildcard-Zertifikat zur Authentifizierung eines betrügerisch irreführenden sub-FQDN verwendet wurde.

Gesperrte Zertifikate werden nicht wieder entsperrt.

4.9.2 Berechtigte Sperrantragsteller

Die Sperrung eines Zertifikats kann grundsätzlich durch den Zertifikatsinhaber bzw. einen berechtigten Vertreter des Zertifikatsinhabers beantragt werden.

Darüber hinaus kann die Sperrung eines Zertifikats durch jede Person ausgelöst oder beantragt werden, wenn sie dem Trust Center nachweisen kann, dass einer der in Kapitel 4.9.1 aufgeführten Sperrgründe vorliegt.

4.9.3 Verfahren zur Beantragung von Sperrungen

Die Beantragung von Sperranträgen kann grundsätzlich über die vom ACME-Protokoll bereitgestellten Funktionen erfolgen. Dazu ist die Signatur eines Sperrantrags mit dem zum Zertifikat gehörenden privaten Schlüssel oder dem privaten Schlüssel des mit dem Zertifikat assoziierten Account notwendig. Alternativ kann ein Sperrantrag durch Nachweis der Kontrolle über die im Zertifikat angegebene Domain autorisiert werden.

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

4.9.4 Fristen zur Beantragung einer Sperrung

Wenn ein Sperrgrund gemäß Kapitel 4.9.1 festgestellt wird, ist schnellstmöglich ein Sperrantrag zu stellen bzw. das Trust Center zu informieren.

4.9.5 Fristen zur Verarbeitung von Sperranträgen durch die TSP

Liegt für ein Endteilnehmer-Zertifikat ein berechtigter Sperrantrag vor, so wird die Sperrung innerhalb weniger Minuten durch das System durchgeführt. Sollte einer der in Kapitel 4.9.1 aufgeführten Gründe für ein Endteilnehmer-Zertifikat festgestellt werden, so wird die Sperrung schnellstmöglich unter Berücksichtigung der Umstände durchgeführt. Für TLS-Server-Zertifikate werden innerhalb von 24 Stunden nach Eingang einer Problemmeldung die Fakten und Umstände untersucht und es werden dem Endteilnehmer sowie der meldenden Person eine erste Rückmeldung zu den bis dahin vorliegenden Erkenntnissen gegeben. Anschließend

werden mit dem Endteilnehmer und der meldenden Person die Analyseergebnisse besprochen und es wird entschieden, ob eine Sperrung erforderlich ist. Falls eine Sperrung erforderlich ist, wird unter Beachtung der zeitlichen Vorgaben aus Kap. 4.9.1 und Berücksichtigung der folgenden Aspekte der Zeitpunkt der Sperrung festgelegt:

- die Art des mutmaßlichen Problems (Umfang, Kontext, Schweregrad, Ausmaß, Schadensrisiko)
- die Auswirkungen einer Sperrung (direkte und kollaterale Auswirkungen auf Endteilnehmer vertrauende Dritte)
- die Anzahl der Problemmeldungen zu einem Zertifikat oder Endteilnehmer
- die Entität, welche die Meldung eingestellt hat
- die einschlägigen Rechtsvorschriften

Die Sperrung eines Zertifikats 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, welche Auskunft über gesperrte Endteilnehmer-Zertifikate geben (Certificate Revocation List (CRL)), werden innerhalb weniger Minuten nach einer durchgeführten Sperrung sowie regelmäßig alle 24 Stunden aktualisiert. Der Wert des nextUpdate-Felds liegt maximal 5 Tage nach dem Wert des thisUpdate-Felds.

4.9.8 Maximale Latenzzeit von Sperrlisten

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

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Es werden Online-Statusinformationen zu allen Zertifikaten per OCSP bereitgestellt.

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 beabsichtigen eine Schlüsselkompromittierung zu melden, können die unter 4.9.3 genannten Funktionen des ACME-Protokolls oder die in Abschnitt 1.5.2 beschriebenen Kontaktmöglichkeiten nutzen. Für letzteres 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 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 Zertifikate werden sowohl von den CAs signierte Sperrlisten als auch von delegierten OCSP-Respondern signierte OCSP-Auskünfte bereitgestellt, deren Authentizität und Integrität durch technische sowie organisatorische Maßnahmen sichergestellt wird.

4.10.1 Betriebliche Vorgaben

Alle Zertifikatsstatusauskünfte (Sperrlisten und OCSP) werden regelmäßig vor der Generierung (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 erhalten einen Wert im nextUpdate-Feld, der 5 Tage nach dem thisUpdate-Wert liegt, werden jedoch für maximal 2 Stunden für weitere Anfragen wiederverwendet, sofern es zu keinen Statusänderungen in einer geringeren Frist kommt.

OCSP-Anfragen zu nicht vergebenen Seriennummern werden überwacht.

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

Gesperrte Zertifikate sind auch nach ihrem Gültigkeitsende noch in mindestens der nächsten regulären 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 12 Stunden gewährleisten. Darüber hinaus werden größtmögliche Bemühungen unternommen, Störungen so schnell wie möglich zu beheben.

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

4.10.3 Optionale Merkmale

Keine Bestimmungen.

4.11 Kündigung durch Zertifikatsinhaber

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

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und-Praktiken

Nicht anwendbar.

4.12.2 Richtlinien und Praktiken für die Kapselung und Wiederherstellung von Sitzungsschlüsseln

Nicht anwendbar.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE REGELUNGEN

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

Das ISMS selbst sowie weitere Sicherheitsrichtlinien, Sicherheitskonzepte und andere Dokumente stellen die Einhaltung der in der 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 getrennt und nach „Trusted Site Infrastructure TSI V3.2 Dual Site“ auditiert und zertifiziert.

5.1.2 Physikalischer Zutritt

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

5.1.3 Stromversorgung und Klimatisierung

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

5.1.4 Wassereinwirkung

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

5.1.5 Brandvorsorge und Brandschutz

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

5.1.6 Aufbewahrung von Medien

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

5.1.7 Abfallentsorgung

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

5.1.8 Off-Site-Sicherung

Sicherungen werden georedundant vorgehalten.

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

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

- Leiter TSP: trägt die gesamte Verantwortung für die bereitgestellten Dienste des Trust Centers
- Informationssicherheitsbeauftragter: plant und überwacht die Implementierung von Sicherheitsmaßnahmen, leitet das ISMS

- ISMS-Teammitglied: unterstützt den Informationssicherheitsbeauftragten in seinen Aufgaben
- Administrator: konfiguriert und wartet die IT-Infrastruktur (Netzwerke, Datenbanken, Server, Applikationen etc.)
- CA Operator: generiert CA-Schlüssel und -Zertifikate
- Interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten Zertifikate, Prozesse, Dokumentationen und begutachtet die Konformität von Schlüssel- bzw. Root-Zeremonien
- Root-Programm/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
- RA-Mitarbeiter (Validierungsspezialist): validiert Zertifikatsanträge, veranlasst die Ausstellung oder manuelle Sperrung von Zertifikaten

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

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, sodass ein Mitarbeiter nur die unter einem Auflistungspunkt geführten Rollen gleichzeitig besetzen darf:

- Management/Leiter Trust Center
- IT-Sicherheitsbeauftragter/Compliance-Team/Interner Auditor
- RA-Mitarbeiter/Validierungsspezialist
- Administrator/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. Vor der Erstbeschäftigung werden zudem relevante Abschlüsse und Referenzen überprüft, um die Eignung für die Tätigkeit festzustellen.

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 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 kontinuierlich 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 der Lebenszyklus der HSM) sowie EE-Zertifikaten (Validierung der Antragsdaten sowie Ausstellung, Erneuerung und Sperrung der Zertifikate etc.) 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 grundsätzlich kontinuierlich protokolliert (in den Systemen der Offline-CA nur während des Betriebs):

- 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 aufgeführten Ereignisse werden kontinuierlich protokolliert.

Die in Kap. 5.4.1.2 aufgeführten Ereignisse werden kontinuierlich durch die Systeme protokolliert.

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 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

Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten werden für mindestens 7 Jahre nach Gültigkeitsende oder Sperrung des letzten zu einem Public Key ausgestellten Zertifikats und, im Falle von CA-Zertifikaten, der Zerstörung des Schlüssels aufbewahrt.

Aufzeichnungen zu den in Kapitel 5.4.1.2 aufgeführten Ereignissen werden für mindestens 2 Jahre nach dem Eintreten des Sicherheitsereignisses aufbewahrt.

5.4.4 Schutz der Audit-Protokolle

Die Aufzeichnungen zu den in Kap. 5.4.1.1 aufgeführten Aktivitäten werden vertraulich und integritätsgesichert und vor Zerstörung sowie Löschung geschützt aufbewahrt. Bei Papieranträgen bzw. Protokollen erfolgt dies im sicheren Papierarchiv des Trust Centers, bei elektronischen Anträgen (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 Ereignis-auslösenden Person

Keine Bestimmungen.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Bestimmungen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Art der archivierten Datensätze

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.

Sicherheitsvorfälle mit signifikanten Auswirkungen auf den bereitgestellten Vertrauensdienst oder auf personenbezogene Daten werden innerhalb von 24 Stunden an das BSI, die

Bundesnetzagentur oder den Landes-Datenschutz gemeldet, je nach Art und Kontext des Vorfalls.

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

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

5.7.2 Wiederherstellung bei Beschädigung von Computern, Software oder Daten

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

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

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

Im Falle einer Kompromittierung eines CA-Schlüssels wird das CA-Zertifikat gesperrt und alle betroffenen Endteilnehmer sowie weitere Instanzen, mit denen entsprechende Vereinbarungen abgeschlossen wurden, informiert.

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, welcher unter anderem die nachfolgenden Punkte abdeckt.

Im Falle einer Beendigung des Betriebs sieht die Telekom Security vor, alle betroffenen Zertifikatnehmer frühzeitig zu informieren, sodass diese möglichst vor Einstellung des CA-Betriebs zu einer anderen CA der Telekom Security oder eines anderen Betreibers migrieren können und damit mögliche Störungen für die Endteilnehmer vermieden werden.

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

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

Zur Außerbetriebnahme werden die privaten Schlüssel der 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 Vertrauensdiensteanbieter (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

Es werden keine Schlüssel für Endteilnehmer generiert. Die Endteilnehmer werden jedoch über die zulässigen Schlüsselalgorithmen informiert.

Die Schlüssel einer CA der Telekom Security werden in einem HSM gemäß Kap. 6.2.1 in der sicheren Umgebung des Trust Centers im Rahmen einer Schlüssel-Zeremonie generiert. Voraussetzung für die Generierung der Schlüssel istein freigegebener Antrag auf Ausstellung eines CA-Zertifikats.

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

- die Aktivierung des HSMs mittels geteilter Aktivierungsdaten,
- das Backup der Schlüssel auf mehrere Backup-HSM unter Verwendung geteilter Token („n von m“),
- getrennte Aufbewahrung der Token zur Widerherstellung der Schlüssel aus dem Backup („n von m“).

Alle Zeremonien werden von einem qualifizierten internen Auditor und, im Falle von Sub-CAs zur Ausstellung von TLS-Server-Zertifikaten, von einem qualifizierten externen Auditor einer Konformitätsbewertungsstelle (siehe Kapitel 8.2) überwacht. Die erfolgreiche Durchführung einer Zeremonie wird durch die entsprechenden Auditoren in den Protokollen bestätigt.

6.1.2 Bereitstellung der privaten Schlüssel an Antragsteller

Nicht anwendbar.

6.1.3 Übergabe öffentlicher Schlüssel an Zertifikataussteller

Öffentliche Schlüssel werden von den Antragstellern mittels PKCS#10-Requests über gesicherte TLS-Verbindungen eingereicht.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

Alle CA-Zertifikate werden wie in Kap. 2.2 beschrieben veröffentlicht. Darüber hinaus werden alle EE-Zertifikate mit den dazugehörigen Sub-CA-Zertifikaten der Vertrauenskette an die Endteilnehmer ausgegeben.

6.1.5 Schlüssellängen

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

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

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Bei RSA-Schlüsseln wird geprüft, dass der Wert des Exponenten eine ungerade Zahl größer oder gleich 3 ist und im Bereich von 2^{16} und 2^{256}-1 liegt sowie dass der 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 unendliche ferne Punkt der Kurve ist.

6.1.7 Schlüsselverwendung

Private Sub-CA-Schlüssel werden ausschließlich zur Signatur von weiteren Sub-CA- bzw. Endteilnehmer-Zertifikaten, delegierten OCSP-Signer-Zertifikaten und Sperrlisten verwendet.

Alle Endteilnehmer-Zertifikate erhalten eine gemäß Kapitel 7.1.2 definierte keyUsage- und ExtendedKeyUsage-Erweiterung, welche die zulässige Verwendung der mit dem Zertifikat verbundenen Schlüssel vorgibt.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

CA-Schlüssel werden ausschließlich in HSMs 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 privater CA-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 CA-Schlüsseln außerhalb des Trust Centers der Telekom Security findet nicht statt.

6.2.4 Sicherung privater Schlüssel

Die privaten CA-Schlüssel werden im Rahmen der Zeremonie zur Schlüsselgenerierung (siehe Kap. 6.1.1) ausschließlich auf Backup-HSM kopiert, welche unter einem vergleichbaren Sicherheitsniveau wie die originalen Instanzen der Schlüssel 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 CA-Schlüsseln findet nicht statt.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Die privaten CA-Schlüssel 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

Private CA-Schlüssel 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 CA-Schlüsseln können aufgrund der Aufteilung der Aktivierungsdaten auf zwei Personen in unterschiedlichen Rollen ausschließlich im Vier-Augen-Prinzip aktiviert werden. Dies wird durch den internen Auditor überwacht und protokolliert.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

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

6.2.10 Methoden zur Zerstörung privater Schlüssel

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

Die Zerstörung von Schlüsseln erfolgt wie die Generierung in einer Zeremonie im Beisein von 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

Zertifikate werden im Rahmen regelmäßiger Sicherungsmaßnahmen archiviert.

6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Für alle Schlüssel gilt, dass diese nur so lange genutzt werden, wie diese inkl. der zur Zertifikatssignatur verwendeten Algorithmen als hinreichend sicher gemäß Kapitel 6.1.5 und 6.1.6 angesehen werden.

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

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

TLS-Server-Zertifikate werden mit einer Gültigkeitsdauer von maximal 397 Tagen ausgestellt.

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

Schlüsselpaare können für Folgezertifikate wiederverwendet werden, soweit sie nicht kompromittiert oder anderweitig unbrauchbar sind.

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

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

6.6.1 Steuerung der Systementwicklung

Die Telekom Security steht im regelmäßigen und engen Austausch mit dem Software-Lieferanten der CA sowie OCSP-Systeme, 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
- 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

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

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

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

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

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

7.1.1 Versionsnummer

Alle X509-Zertifikate werden in der Version 3 (mit dem Wert „2“) ausgestellt.

7.1.2 Zertifikatserweiterungen

Im Folgenden werden die Zertifikatserweiterungen für die jeweiligen Zertifikatstypen angegeben. Nicht aufgeführte Zertifikatserweiterungen werden nicht gesetzt.

In Sub-CA-Zertifikaten werden ausschließlich die folgenden Zertifikatserweiterungen gesetzt:

- authorityKeyIdentifier: enthält Wert des subjectKeyIdentifier des ausstellenden CA-Zertifikats
- subjectKeyIdentifier: enthält „keyIdentifier“ gem. RFC5280 #4.2.1.1.
- keyUsage (kritisch): „keyCertSign“, „cRLSign“
- basicConstraints (kritisch):
  - „cA“: „true“
  - „pathLenConstraint“: gemäß RFC5280
- CertificatePolicies:
  - In Sub-CA-Zertifikaten zur Ausstellung von TLS-Server- Zertifikaten wird die entsprechende Policy-OID der Baseline Requirements gesetzt (siehe Kapitel 7.1.6).
  - In allen anderen Sub-CA-Zertifikaten ist diese Erweiterung optional.
- extendedKeyUsage:
  - In Sub-CA-Zertifikaten zur Ausstellung von TLS-Server-Zertifikaten werden „id-kp-serverAuth“ und ggf. „id-kp-clientAuth“ gesetzt.
- cRLDistributionPoints: enthält http-URL der zugehörigen CRL
- authorityInfoAccess: enthält http-URL des zugehörigen OCSP-Responders (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)). In Sub-CA-Zertifikaten zur Ausstellung von TLS-Server-Zertifikaten wird zusätzlich eine http-URL gesetzt, die einen Downloadpunkt des zugehörigen übergeordneten CA-Zertifikats enthält (accessMethod 1.3.6.1.5.5.7.48.2 (calssuers)).

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

In EE-Zertifikaten werden ausschließlich die folgenden Zertifikatserweiterungen gesetzt:

- authorityKeyIdentifier: <Wert des subjectKeyIdentifier des ausstellenden CA-Zertifikats>
- subjectKeyIdentifier: <enthält „keyIdentifier“ gem. RFC5280 #4.2.1.1.>
- keyUsage (kritisch): <enthält einen Wert konsistent zur extendedKeyUsage gem. RFC5280 #4.2.1.12>
- basicConstraints (kritisch):
  - „cA“: „false“
  - „pathLenConstraint“: <wird nicht gesetzt>
- CertificatePolicies:
  - In TLS-Server-Zertifikaten wird die entsprechende Policy-OID der Baseline Requirements gesetzt (siehe Kapitel 7.1.6).
  - In allen anderen EE-Zertifikaten wird mindestens eine OID einer entsprechenden Policy gesetzt.
- subjectAltName: enthält mindestens einen Eintrag mit einem FQDN oder einer IP-Adresse (bei Wildcard-Zertifikaten ist das erste Zeichen ein „*“)
- extendedKeyUsage:
  - In TLS-Server-Zertifikaten werden „id-kp-serverAuth“ und ggf. „id-kp-clientAuth“ gesetzt.
  - In S/MIME-Zertifikaten wird ausschließlich „id-kp-emailProtection“ gesetzt.
  - In Client-Authentication-Zertifikaten wird ausschließlich „id-kp-clientAuth“ gesetzt.
- cRLDistributionPoints: enthält http-URL der zugehörigen CRL
- authorityInfoAccess: enthält http-URL des zugehörigen OCSP-Responders (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)) und zusätzlich eine http-URL, die einen Downloadpunkt des zugehörigen übergeordneten CA-Zertifikats enthält (accessMethod 1.3.6.1.5.5.7.48.2 (calssuers)).

7.1.3 Algorithmen-OID

Telekom Security verwendet zur Signatur von Zertifikaten ausschließlich die folgenden Algorithmen:

- 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)

7.1.4 Namensformen

In CA-Zertifikaten werden ausschließlich folgende Attribute gesetzt:

- commonName
- organizationName
- countryName

Telekom Security setzt im subjectDN von domainvalidierten EE-Zertifikaten ausschließlich das Attribut commonName mit einen im SubjectAlternativeName enthaltenen FQDN.

7.1.5 Namensbeschränkungen

Es werden keine Namensbeschränkungen gesetzt.

7.1.6 OIDs der Erweiterung „CertificatePolicies“

In Sub-CA- und EE-Zertifikaten wird mindestens eine OID einer entsprechenden Certificate Policy gesetzt. TLS-Server- Zertifikate und zu deren Ausstellung genutzte Sub-CA-Zertifikate enthalten jeweils eine der folgenden OIDs der Baseline Requirements:

- 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)

Der Qualifier „cPSuri“ enthält einen Verweis auf das Repository der Telekom Security, in welchem dieses CPS hinterlegt ist.

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

7.2 Sperrlistenprofile

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

7.2.1 Versionsnummer(n)

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

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Alle Sperrlisten 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), privilegeWithdrawn (9).

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 CA ausgestellt wurde. Alle OCSP-Signer-Zertifikate enthalten die Erweiterung id-pkix-ocsp-nocheck. Von Sub-CAs ausgestellte OCSP-Signer-Zertifikate besitzen eine Gültigkeitsdauer von 1 Monat.

In OCSP-Antworten für 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 CP fallenden CA-Zertifikate werden auf den Webseiten des Trust Centers sowie in der CCADB und mehreren CTLogs veröffentlicht 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 sowie für diejenigen Sub-CAs, welche im Geltungsbereich der [BR] liegen, 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 die zugehörige Schlüsselgenerierung mindestens von einem internen Auditor überwacht und für konform befunden wurde.

Durch interne Auditoren werden zudem monatliche Selbstüberprüfungen durchgeführt, welche stichprobenartig eine zufällige Auswahl von mindestens 3% der seit der letzten Prüfung ausgestellten TLS-Server-Zertifikate betreffen.

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

Alle in Kapitel 1.3.1 aufgeführten Sub-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. ETSI EN 319 411-2. Die folgenden Policies werden angewandt:

- Telekom Security DV RSA CA 21: DVCP

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, Erneuerung und Verwaltung von Zertifikaten ist in den jeweiligen Leistungsbeschreibungen geregelt.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Es werden keine Entgelte für den Zugriff auf Zertifikate erhoben.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

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

9.1.4 Entgelte für andere Leistungen

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

9.1.5 Erstattung von Entgelten

Die Erstattung von Entgelten erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts und sind in den Allgemeinen Geschäftsbedingungen konkretisiert.

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 nach folgenden Schutzklassen eingestuft:

- offen
- intern
- vertraulich
- vertraulich (Kunde)

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

9.3.2 Umfang an nicht vertraulichen Informationen

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

- die in Zertifikaten enthaltenen Informationen
- 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.

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 PKI-Dienste 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, die öffentlich zugänglich oder aus öffentlichen Informationen ableitbar sind. Hierzu zählen z.B. Informationen in Zertifikaten.

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 Telekom Security als Zertifizierungsstellenbetreiber

Die Telekom Security sichert einen zuverlässigen, vertrauenswürdigen, diskriminierungsfreien und legalen Betrieb der Dienstleistung sowie die Einhaltung der Konformität zur Telekom Security CP zu. Die den Endteilnehmern angebotenen Dienste und Produkte werden soweit möglich auch Menschen mit Behinderungen zugänglich gemacht. Sollten Maßnahmen nicht ausreichen, bietet das Trust Center darüber hinaus behinderten Menschen zur Unterstützung bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten kostenlosen telefonischen Support.

Vor Abschluss eines Vertragsverhältnisses mit einem Endteilnehmer wird dieser über die Nutzungsbedingungen zur Verwendung der Zertifikate gemäß Kap. 9.6.3 informiert.

Telekom Security sichert die in der Telekom Security CP Kapitel 9.6.1 geforderten Zusicherungen und Gewährleistungen der TSP zu.

Die Akzeptanz der Verträge mit den Endteilnehmern inkl. Nutzungsbedingungen können, sofern rechtlich durchsetzbar, elektronisch erfolgen und für mehrere Zertifikate gelten.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Die Telekom Security nutzt ausschließlich eigene Mitarbeiter für die Registrierungstätigkeiten und sichert die in der Telekom Security CP geforderten Zusicherungen und Gewährleistungen zu.

9.6.3 Zusicherungen und Gewährleistungen der Antragsteller

Telekom Security legt die Nutzungsbedingungen für die Endteilnehmerzertifikate gegenüber den Endteilnehmern fest und lassen deren Akzeptanz vor der Ausstellung der Zertifikate von den Endteilnehmern bestätigen. Diese Nutzungsbedingungen berücksichtigen die in der Telekom Security CP geforderten Zusicherungen und Gewährleistungen.

Die Nutzungsbedingungen werden den Endteilnehmern dauerhaft auf integre Art und Weise über die Webseiten des Trust Centers sowie die Service Portale für Endkunden bereitgestellt.

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 sowie den Allgemeinen Geschäftsbedingungen 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 sowie den Allgemeinen Geschäftsbedingungen geregelt und entsprechen grundsätzlich geltendem Recht.

9.9 Schadensersatz

Etwaige Schadenersatzansprüche gegenüber der Telekom Security werden in den internen und externen Vereinbarungen sowie den Allgemeinen Geschäftsbedingungen 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 Zertifikatsinhaber 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

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

9.14 Geltendes Recht

Es gilt deutsches Recht.

9.15 Einhaltung geltenden Rechts

Die Telekom Security sichert zu, geltendes Recht einzuhalten.

9.16 Verschiedene Bestimmungen

9.16.1 Gesamte Vereinbarung

Keine Bestimmungen.

9.16.2 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

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

9.17 Sonstige Bestimmungen

Keine Bestimmungen.