Deutsche Telekom Security GmbH
Certification Practice Statement Public

Version: 03.00

Gültig ab: 22.08.2022

Status: Freigegeben

Letztes Review: 17.08.2022

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License (https://creativecommons.org/licenses/by-nd/4.0/).

Copyright ©2022 Deutsche Telekom Security GmbH, Bonn

ÄNDERUNGSHISTORIE

Tabelle 1: Änderungshistorie

Version	Stand	Änderungen / Kommentar
01.00	24.09.2021	Initialversion nach RFC 3647 Struktur
02.00	15.03.2022	Aufnahme neues CA-Zertifikat
03.00	13.08.2022	Erweiterung um OV, Generelle Überarbeitung

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 Überblick

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

Bei dem vorliegenden Dokument handelt es sich um ein Certification Practice Statement (CPS) des Trust Centers der Telekom Security. Es beschreibt in der Struktur des RFC3647 die Einhaltung und die Umsetzung der Anforderungen aus

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

an den Telekom Security PKI-Betrieb der Public Certificate Service Platform. Diese CPS wird durch die Telekom Security CPS Root ergänzt.

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

1.2 Name und Kennzeichnung des Dokuments

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

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

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

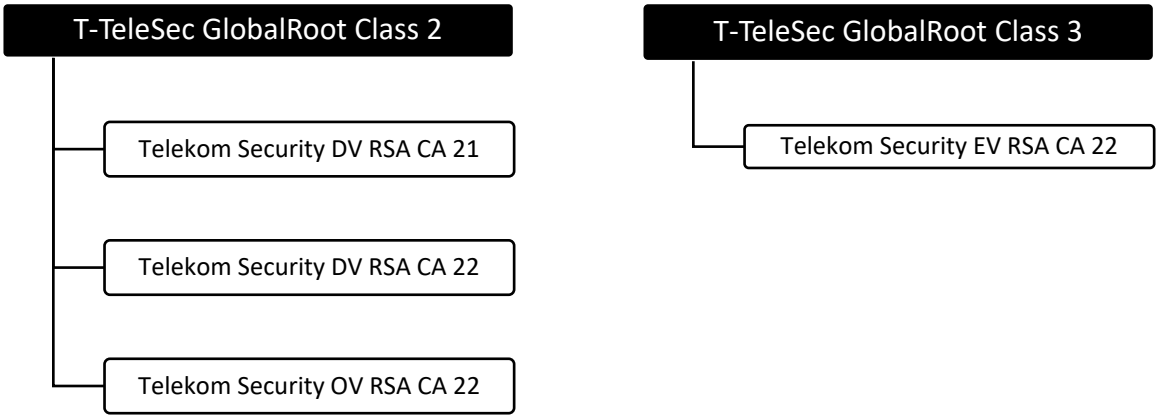
Die folgenden Sub-CA-Zertifikate sind im Gültigkeitsbereich dieser CPS:

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

Name	Schlüssel-typ	Seriennummer	Gültigkeitszeit-raum	Fingerprint (SHA1)
Telekom Security DV RSA CA 21	RSA 2048	2cf3c72f3f7d0fb31fc 362d6b869558e	2021-04-21 bis 2031-04-21	99cc84f820818cf0eefe81d df572cace4b3acb78
Telekom Security DV RSA CA 22	RSA 4096	2103be2c2aa30a5b 5b1f0e1a4456239a	2022-02-22 bis 2032-02-22	01648268a45f9e0990acb5 d391ad1876ccee0bed
Telekom Security OV RSA CA 22	RSA 4096	343262b23269e3db 202a1478136ac1af	2022-06-21 bis 2032-06-21	32cd823131f8abb068fAa0 e2f495ad9fbc89afa4
Telekom Security EV RSA CA 22	RSA 4096	1cd786631ec0cfba0 b52fa9b5e0287b1	2022-06-21 bis 2032-06-21	578fc66913edC923f12df29 c5993e6f25f9965dc

Die Telekom Security EV RSA CA 22 ist derzeit noch nicht in Betrieb. Die Sub-CA-Zertifikate gliedern sich in folgende PKI-Hierarchien ein:

PKI-Hierarchie der Public Certificate Services Platform



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

1.3.2 Registrierungsstellen (Registration Authorities, RA)

Das Trust Center der Telekom Security agiert selbst als RA.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind alle natürlichen oder juristischen Personen, welche Zertifikate von den in dieser CPS genannten CAs bzw. Trust Services beziehen. Zertifikatsnehmer benötigen daher einen registrierten Account bei Telekom Security, bspw. über ein entsprechendes Service-Portal.

Subjekte der Endteilnehmerzertifikate sind Domains bzw. Webserver, ggf. auch in Assoziation mit juristischen Personen.

1.3.4 Vertrauende Dritte

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

1.3.5 Andere Teilnehmer

Keine Bestimmungen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

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 Endteilnehmer-Zertifikaten wird durch die Zertifikatsprofile bzw. Zertifikatserweiterungen KeyUsage und ExtendedKeyUsage vorgegeben. Darüber hinaus hat der Zertifikatsnehmer geltende gesetzliche Vorgaben einzuhalten.

1.4.2 Unzulässige Verwendung von Zertifikaten

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

1.5 Verwaltung des Dokuments

1.5.1 Verwaltende Organisation dieses Dokuments

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

1.5.2 Ansprechpartner

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

TrustCenter-Roots@telekom.de

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

Vorfälle können an diese Mail-Adresse gesendet werden. Bezüglich der Meldung von Schlüsselkompromittierungen sind die Instruktionen gemäß Kapitel 4.9.12 zu berücksichtigen.

1.5.3 Person für die Feststellung der Konformität dieser CPS zur CP

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

1.5.4 Genehmigungsverfahren dieses CPS

Jede Version dieses CPS wird nach Feststellung der Konformität zur Telekom Security CP von der Leitung des Trust Centers freigegeben und behält seine Gültigkeit für neu ausgestellte Zertifikate sowie für bereits bestehende Zertifikate, bis sie widerrufen oder durch eine neue Version ersetzt wird.

1.6 Definitionen und Abkürzungen

Siehe Telekom Security CP.

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

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

2.2 Veröffentlichung von Informationen zu Zertifikaten

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

- Telekom Security CP
- Certification Practice Statements (CPS, beinhaltet dieses Dokument)
- PKI Disclosure Statements (PDS)
- alle im Geltungsbereich dieser CPS befindlichen CAs
- Audit Attestations zu öffentlichen Root-CA-Zertifikaten der Telekom Security (Verlinkung zu den offiziellen Web-Seiten des Auditors).
- Nutzungsbedingungen, Leistungsbeschreibungen und Allgemeine Geschäftsbedingungen (AGB)

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

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

Zu allen öffentlichen Root-CAs, unter denen TLS-Server-Zertifikate ausgestellt werden, werden jeweils Test-Web-Seiten mit einem gültigen, einem abgelaufenen und einem gesperrten TLS-Serverzertifikat betrieben. Die Links zu diesen Test-Webseiten einer jeden Root-CA können auf der Webseite des Trust Centers eingesehen werden.

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

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

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

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

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

2.4 Zugang zu den Verzeichnissen

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

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

3.1.1 Namensformen

Es werden in alle Zertifikate die Namen der Zertifikatsinhaber in Form eines Distinguished Names gemäß [x500] aufgenommen. Darüber hinaus enthalten TLS-Server-Zertifikate immer einen subjectAltName. Siehe Kapitel 7.1.4 für Details.

3.1.2 Aussagekraft von Namen

Keine Bestimmungen.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Nicht anwendbar.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

Ein SubjectDN ist in der Zuordnung zu den Zertifikatsnehmern eindeutig, wird also nicht an unterschiedliche Zertifikatsnehmer vergeben. Sollten die Daten von mehreren Zertifikatsnehmern übereinstimmen, so werden weitere Identifier hinzugenommen, um Eindeutigkeit der SubjectDN herzustellen.

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

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Keine Bestimmungen.

3.2 Initiale Validierung der Identität

Zur initialen Validierung der Identität einer natürlichen oder juristischen Person werden ausschließlich direkte Nachweise oder Bescheinigungen von angemessenen und autorisierten Quellen verwendet. Die Nachweise können dabei in Papierform oder elektronisch erfasst werden und es werden nur solche Nachweise angefordert, welche für die Identifizierung notwendig sind.

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

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Für den Besitznachweis ist ein mit dem privaten Schlüssel signierter PKCS#10-Request notwendig.

3.2.2 Authentifizierung der Organisationsidentität

Es werden die nachfolgenden Methoden zur Validierung einer Organisationsidentität verwendet.

(QGIS – Qualified Government Information Source) Existenz und Identität einer Organisation werden über staatlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert. Beispiele für QGIS sind Handelsregister, berufsständige Körperschaften öffentlichen Rechts und das Bundeszentralamt für Steuern. Für eine Prüfung werden die vom Antragsteller bereitgestellten Informationen für eine automatisierte oder manuelle Suche in den entsprechenden Registern verwendet. Daraus resultierende Ergebnisse werden mit den bereitgestellten Informationen abgeglichen.

(QIIS – Qualified Independent Information Source) Existenz und Identität einer Organisation werden über privatrechtlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert. Diese Quellen werden hinsichtlich ihrer Aktualität und Zuverlässigkeit evaluiert, bevor sie von Telekom Security als QIIS eingestuft werden. Beispiele für QIIS sind Wirtschaftsauskunfteien. Für eine Prüfung werden die vom Antragsteller bereitgestellten Informationen für eine automatisierte oder manuelle Suche in den Datenbanken der QIIS verwendet. Daraus resultierende Ergebnisse werden mit den bereitgestellten Informationen abgeglichen.

(Bescheinigungsschreiben) Der Antragsteller weist die Existenz und Identität einer Organisation durch Vorlage eines durch einen Notar ausgestelltes Bescheinigungsschreiben nach. Voraussetzung für die Akzeptanz eines solchen Nachweises ist, dass der Notar in einem entsprechend anerkannten Notarverzeichnis geführt wird.

(Sekundärquelle) Der Antragsteller weist die Adresse einer Organisation durch Vorlage eines staatlich ausgestellten Steuerbescheids, eines Kontoauszugs, einer Rechnung oder ähnlichem nachgewiesen werden. Die Aktualität, Zuverlässigkeit und Relevanz der vorgelegten Nachweise wird durch die Registrierungskräfte individuell bewertet und ggf. zum Nachweis einzelner Attribute akzeptiert oder abgelehnt.

3.2.3 Authentifizierung von natürlichen Personen

Eine Authentifizierung von natürlichen Personen findet im Kontext domainvalidierter oder organisationsvalidierter Zertifikate nicht statt.

3.2.4 Nicht überprüfte Informationen

Es werden ausschließlich gemäß Kapitel 3.2.2 oder 3.2.7 validierte Informationen in ein Zertifikat aufgenommen.

3.2.5 Validierung der Bevollmächtigung

Für organisationsvalidierte TLS-Server-Zertifikate wird die Authentizität des Zertifikatsantrags über den Nachweis der Bevollmächtigung des Antragstellers, im Namen der Organisation (des Zertifikat-Subjekts) Zertifikate zu beantragen, validiert.

3.2.6 Kriterien für Interoperabilität

Nicht anwendbar.

3.2.7 Validierung der Kontrolle über eine Domain

Es werden die folgenden Methoden zur Validierung der Domain-Kontrolle angewendet:

DNS Change (Methode nach [BR#3.2.2.4.7]):

Der Antragsteller weist die Kontrolle über einen FQDN durch Hinterlegung eines eindeutig vorgegebenen Zufallswerts im DNS TXT Record der mit einem vorgegebenen Präfix-Label versehenen Domain nach. Das Präfix beginnt mit einem Unterstrich. Die Anforderungen der [BR] zu dieser Methode werden eingehalten.

Diese Methode wird auch zur Validierung von Wildcard-Zertifikaten verwendet.

Validating Applicant as a Domain Contact (Methode nach [BR#3.2.2.4.12]):

Die Kontrolle über einen FQDN wird durch den Domain-Kontakt validiert.

Diese Methode wird nur für Domains (inkl. Wildcard-Zertifikate) des Konzerns Deutsche Telekom AG verwendet.

Es werden die Anforderungen der [BR] zu dieser Methode eingehalten.

Agreed-Upon Change to Website v2 (Methode nach [BR#3.2.2.4.18]):

Der Antragsteller weist die Kontrolle über einen FQDN durch Hinterlegung eines eindeutig vorgegebenen Zufallswerts in einer Datei im „/.well-known/pki-validation“-Verzeichnis nach. Es werden die Anforderungen der [BR] zu dieser Methode eingehalten.

Agreed-Upon Change to Website – ACME (Methode nach [BR#3.2.2.4.19]):

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 [BR] ergänzt.

Für Wildcard-Zertifikate werden die Anforderungen der [BR] Kapitel 3.2.2.6 auf Basis der ICANN-Domains der Public Suffix List eingehalten.

3.3 Identifizierung und Authentifizierung für Zertifikatserneuerungen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Zertifikatserneuerungen

Die Identifizierung und Authentifizierung geschieht, unter Berücksichtigung der Gültigkeitsdauer von Validierungen und Nachweisen gemäß Kapitel 4.2.1, durch die erfolgreiche Anmeldung am Kundenaccount, bspw. mit Username und Passwort oder einer anderen Form von Geheimnis.

3.3.2 Identifizierung und Authentifizierung für Zertifikatserneuerungen nach einer Sperrung

Eine Erneuerung gesperrter Zertifikate wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Zertifikatsantragsteller können eine Sperrung der eigenen Zertifikate auch über ihren eigenen Kundenaccount autorisieren.

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 mit einer gültigen E-Mailadresse verknüpftes Kundenkonto beim Trust Center der Deutschen Telekom Security GmbH registriert haben. Davon ausgenommen sind jedoch Entitäten, mit denen aufgrund rechtlicher oder konzern-interner Bestimmungen keine Geschäfte erlaubt sind.

4.1.2 Antragsprozess und -verantwortlichkeiten

Der Antragsprozess beinhaltet in Abhängigkeit des Zertifikatstyps folgende Punkte:

- Generierung eines Schlüsselpaars gemäß den geltenden Vorgaben dieses CPS
- Bereitstellung der ins Zertifikat aufzunehmenden Informationen in Form eines Zertifikatsantrags inklusive eines signierten Certificate Signing Requests zum zuvor generierten Schlüsselpaar, welcher mindestens eine der gewünschten Domains enthält
- Bereitstellung einer durch einen Zeichnungsberechtigten der Organisation handschriftlich oder elektronisch unterschriebenen Vollmacht
- Akzeptanz der Datenschutzhinweise, Allgemeinen Geschäftsbedingungen, Nutzungsbedingungen
- Bestätigung der Korrektheit der im Zertifikatsantrag gemachten Angaben und der korrekten Generierung des Schlüsselpaars
- Ggf. zusätzliche Nachweisdokumente

4.2 Bearbeitung der Zertifikatsanträge

4.2.1 Durchführung der Identifizierung und Authentifizierung

Zertifikatsanträge werden durch Automatismen sowie Registrierungsmitarbeiter auf Vollständigkeit, Korrektheit und Echtheit überprüft. Insbesondere werden die Angaben gemäß Kapitel 3.2 validiert. Auf bereits durchgeführte Validierungen und Nachweise darf zurückgegriffen werden, sofern die in Kapitel 4.2.2 genannten Fristen erfüllt werden.

Für TLS-Server-Zertifikate wird die Kontrolle über jegliche im Zertifikatsantrag enthaltenen Domains mittels einer der in Kapitel 3.2.7 beschriebenen Methoden validiert.

Für OV-Zertifikate wird zusätzlich die Identität der Organisation mittels der in Kapitel 3.2.2 beschriebenen Methoden validiert. Konkret werden für die jeweiligen Attribute die folgenden Methoden verwendet:

- OrganizationName: QGIS, QIIS, Beglaubigungsschreiben
- Country: QGIS, QIIS, Beglaubigungsschreiben

- Locality: QGIS, QIIS, Beglaubigungsschreiben,
- PostalCode: QGIS, QIIS, Beglaubigungsschreiben,
- StreetAddress (optional): QGIS, QIIS, Beglaubigungsschreiben, Sekundärquelle
- StateOrProvinceName (optional): QGIS, QIIS, Beglaubigungsschreiben, Sekundärquelle

Für organisationsvalidierte TLS-Server-Zertifiakte wird die Autorisierung des Antragstellers im Namen einer Organisation Zertifikate zu beantragen gemäß Kapitel 3.2.5 validiert.

Mit der Identifizierung und Authentifizierung verbundene manuelle Tätigkeiten werden ausschließlich von Personal in vertrauenswürdigen Rollen des Trust Centers der Telekom Security durchgeführt.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

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

Zertifikatsanträge für Internal Names (gemäß Definition der Baseline Requirements [BR]) werden abgelehnt.

Für TLS-Server-Zertifikate werden zu Beginn einer Antragstellung als auch unmittelbar vor der Ausstellung eines Zertifikats für alle im Antrag enthaltenen FQDN-Einträge die CAA-Records im DNS geprüft. Ein Zertifikatsantrag wird abgelehnt, falls in „issue“ oder „issuewild“ ein Eintrag vorhanden ist, welcher nicht „telesec.de“ ist. „iodef“-Einträge werden ausgewertet, jedoch nicht weiterverfolgt. Weitere Einträge des CAA Records werden nicht unterstützt. Die CAA-Prüfung ist für 8 Stunden gültig. Sollte die Abfrage eines CAA-Records fehlschlagen, wird mit der Ausstellung des Zertifikats dennoch fortgefahren, sofern

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

Zertifikatsanträge werden abgelehnt, wenn der verwendete Schlüssel als kompromittiert gilt oder die Qualitätskriterien gemäß Kapitel 6.1.5 und Kapitel 6.1.6 nicht erfüllt.

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

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

Wenn alle Validierungsschritte gemäß Kapitel 4.2.1 erfolgreich durchgeführt wurden und keiner der in diesem Kapitel genannten Prüfschritte zu einer Ablehnung führt, wird die Zertifikatsausstellung genehmigt. Unabhängig davon behält sich Telekom Security vor, Zertifikatsanträge auch ohne Angabe von Gründen abzulehnen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Bestimmungen.

4.3 Ausstellung von Zertifikaten

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

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

Alle TLS-Server-Zertifikate werden vor der eigentlichen Ausstellung in einer hinreichenden Anzahl von CT-Log-Servern (Certificate Transparency gemäß RFC 6962) als „Pre-Zertifikate“ veröffentlicht und die Signed Certificate Timestamps (SCTs) im tatsächlichen Zertifikat aufgenommen. Die Anzahl der SCTs hängt vom Zertifikatstyp ab (siehe Kapitel 7.1.2).

4.3.2 Benachrichtigung des Antragstellers über die Ausstellung eines Zertifikats

Nach der Ausstellung eines Zertifikats wird dieses über die gewählten Schnittstellen bereitgestellt. Es findet keine gesonderte Benachrichtigung des Antragstellers statt.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Keine Bestimmungen.

4.4.2 Veröffentlichung des Zertifikats durch die TSP

Zertifikatsnehmer können die für sie ausgestellten Zertifikate über die bereitgestellten Kundenschnittstellen beziehen. Darüber hinaus wird keine Veröffentlichung der Zertifikate vorgenommen.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP

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

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den 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.

Insbesondere gilt für TLS-Server-Zertifikate, dass diese ausschließlich auf Servern installiert werden dürfen, welche unter den in subjectAltName gelisteten Domainnamen erreichbar sind.

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-Key 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 Endteilnehmer-Zertifikat wird innerhalb 24 Stunden 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,
- wenn festgestellt wird, dass der Validierung der Domainautorisierung oder der Kontrolle über einen FQDN im Zertifikat nicht vertraut werden kann.

Ein Endteilnehmer-Zertifikat wird möglichst innerhalb 24 Stunden, spätestens jedoch innerhalb von 5 Tagen 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 [BR] erloschen ist oder widerrufen oder gekündigt wurde und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden,
- festgestellt wird, dass die Verwendung eines FQDN 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 Telekom Security oder durch den Zertifikatsinhaber bzw. einen berechtigten Vertreter des Zertifikatsinhabers beantragt werden.

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

4.9.3 Verfahren zur Beantragung von Sperrungen

Autorisierte Sperranträge können gestellt werden, indem über das ACME-Protokoll die Kontrolle über eine im Zertifikat enthaltene Domain, die Kompromittierung des Schlüssels oder die Identität des Sperrantragstellers als ACME-Accountinhaber des zu sperrenden Zertifikats nachgewiesen werden können.

Zertifikatsantragsteller können eine Sperrung der eigenen Zertifikate auch über ihren Kundenaccount autorisieren.

Darüber hinaus bietet das Trust Center eine E-Mail-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

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

4.9.5 Fristen zur Verarbeitung von Sperranträgen

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 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 regelmäßig alle 24 Stunden aktualisiert.

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 (siehe Telekom Security CP).

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine Bestimmung.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Alle Parteien können eine Schlüsselkompromittierung über die in 4.9.3 genannte Funktion des ACME-Protokolls oder über die in Abschnitt 1.5.2 beschriebene Kontaktmöglichkeit melden. Für letzteres müssen ausreichende Informationen oder Verweise auf Informationen angegeben werden, die das Vorliegen einer Schlüsselkompromittierung beweisen. Sofern möglich, sollte ein mit dem kompromittierten privaten Schlüssel signierter CSR mit commonName "Compromised Key" im Base64-Format bereitgestellt werden. Darüber hinaus sollte das betroffene Zertifikat selbst referenziert werden.

Zertifikatsinhaber können eine Schlüsselkompromittierung auch über die Sperrfunktion ihres Accounts mit Angabe „Schlüsselkompromittierung“ als Sperrgrund melden.

4.9.13 Umstände für eine Suspendierung

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, spätestens jedoch alle 24 Stunden zeitsynchronisiert.

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

4.10.1.1 Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

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

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

OCSP-Anfragen zu nicht vergebenen Seriennummern werden überwacht.

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

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

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 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
- (Informations-)Sicherheitsbeauftragter: 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-Team/Compliance-Team (PKI): koordiniert die Umsetzung von Anforderungen, überwacht Anforderungsquellen (Mailing-Listen, Root-Store-Policies, ETSI), übernimmt Außenkommunikation zu Root-Store-Betreibern und „Bugzilla“, berät bei Vorfällen und Änderungen, verantwortet CP, bearbeitet Anträge für CA-Ausstellungen
- 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 vorhanden, wodurch sicherheitsrelevante oder -kritische Tätigkeiten nur durch Personen in vertrauenswürdigen Rollen und nur im Vier-Augen-Prinzip durchgeführt werden. Die Anzahl der Mitarbeiter, die solche sicherheitsrelevanten oder -kritischen Tätigkeiten ausüben, ist unter Berücksichtigung von Vertreterregelungen und arbeitstechnischen Umständen auf ein Minimum beschränkt.

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

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

5.3 Personelle Maßnahmen

5.3.1 Qualifikationen, Erfahrung und Berechtigungen

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

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

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

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.

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

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Keine Bestimmungen.

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.

5.3.8 Dem Personal zur Verfügung gestellte Dokumentation

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

- (minimalen) Berechtigungen,
- Aufgabentrennungen,

- Vier-Augen-Prinzipien sowie
- Schulungs- und Sensibilisierungsmaßnahmen

enthalten.

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

5.4 Protokollierungsverfahren

5.4.1 Zu protokollierende Ereignisse

Die in Telekom Security CP Kapitel 5.4.1 geforderten Ereignisse, d.h.

- alle wesentlichen Ereignisse der Zertifikats- und Schlüsselmanagementsysteme sowie Statusdienste,
- alle sicherheitsrelevanten Ereignisse an den PKI- und Sicherheitssystemen,
- Installation, Update und Deinstallation von Software auf den PKI-Systemen
- Physikalische Ein- und Austritte in bzw. aus den Sicherheitszonen,

werden kontinuierlich inkl. einer Beschreibung des Ereignisses, des präzisen Zeitpunkts und, sofern anwendbar, der Identität des Auslösers protokolliert. Die Zeit der protokollierenden Systeme wird mehrfach pro Tag mit einer zentralen und vertrauenswürdigen Quelle synchronisiert.

5.4.2 Häufigkeit der Log-Verarbeitung

Logdaten werden wie folgt ausgewertet:

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

5.4.3 Aufbewahrungszeitraum für Logdaten

Alle in 5.4.1 erfassten Logdaten werden für zwei Jahre nach ihrem Eintreten bzw. bis zwei Jahre nach Ablauf oder Sperrung der zugehörigen Zertifikate bzw. Löschung der CA-Schlüssel aufbewahrt.

5.4.4 Schutz der Audit-Protokolle

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

5.4.5 Backup-Verfahren für Audit-Protokolle

Logdaten werden im Rahmen der regelmäßigen System-Backups mitgesichert.

5.4.6 Audit-Sammelsystem

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

5.4.7 Benachrichtigung der Ereignis-auslösenden Person

Keine Bestimmungen.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Bestimmungen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Art der archivierten Datensätze

Es werden die in Telekom Security CP Kapitel 5.5.1 genannten Aufzeichnungen archiviert:

- Antrags-/Zertifikatshistorie mit Angabe von Datum, Uhrzeit und Identität der handelnden Person
- Die im Rahmen der Beantragung einer Ausstellung, Erneuerung, Änderung oder Sperrung vom Antragsteller vorgelegten oder dem Antragsteller übermittelten relevanten Informationen und Dokumente („Registrierungsinformationen“)
- Die verwendete Methode zur Validierung der Domain-Kontrolle
- Alle veröffentlichten CP, CPS und Nutzungsbedingungen
- Zertifizierungsunterlagen und Auditberichte
- Relevante Dokumentation bzgl. der Sicherheit der Systeme

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Aufzeichnungen über den Lebenszyklus von CA-Schlüsseln werden für mindestens 7 Jahre nach Ablauf der korrespondierenden Zertifikate aufbewahrt. Außerdem werden die Nutzungsbedingungen

Alle weiteren Aufzeichnungen werden für zwei Jahre aufbewahrt, wobei für die Zertifikatshistorie und die Registrierungsdaten diese Frist mit Ablauf bzw. Sperrung des jeweiligen Zertifikats beginnt.

5.5.3 Schutz von Archiven

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

5.5.4 Backup-Verfahren für Archive

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

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Siehe Kap. 6.8.

5.5.6 Archivsystem (intern oder extern)

Es kommen ausschließlich interne Archivsysteme zum Einsatz.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

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

5.6 Schlüsselwechsel

Vor Ablauf eines Sub-CA-Zertifikats wird rechtzeitig ein neues CA-Zertifikat gemäß den aktuellen Versionen der CP und CPS Root ausgestellt. Dabei wird der Zeitraum zwischen der Veröffentlichung des neuen CA-Zertifikats und der Außerbetriebnahme des alten CA-Zertifikats hinreichend groß gewählt, so dass für Endteilnehmer keine Unterbrechung in deren Betrieb entsteht.

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

Die Geschäftsfortführung bzw. die Bereitstellung der für einen konformen Weiterbetrieb benötigten Dienste und Systeme wird durch technische und organisatorische Maßnahmen gesichert. Dazu gehören neben einem geo-redundanten Betrieb auch entsprechend Telekom Security CP Kapitel 5.7.1 aufgebaute Notfalldokumentation bzw. Notfallmanagement.

5.8 Einstellung des CA- oder RA-Betriebs

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

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

Alle betroffenen Zertifikatsnehmer, Trusted Root Stores und Unterauftragnehmer werden frühzeitig informiert. Für alle weiteren vertrauenden Dritten werden entsprechende Informationen auf den Webseiten des Trust Centers bereitgestellt.

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

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

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.

Schlüsselpaare für CAs werden mit HSMs gemäß Kap. 6.2.1 in der sicheren Umgebung des Trust Centers und im Rahmen einer Schlüssel-Zeremonie generiert. Die Generierung setzt die Freigabe des Managements voraus. Die an der Zeremonie beteiligten vertrauenswürdigen Rollen und deren Aufgaben vor, während und nach der Schlüsselzeremonie sind in einer Arbeitsanweisung beschrieben. Dies beinhaltet u.a. die Arbeitsschritte zur Aktivierung der HSMs mittels geteilter Aktivierungsdaten, Schlüsselgenerierung und Backup im Mehr-Personen-Prinzip mit unterschiedlichen Rollen.

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 Auditoren in den Protokollen bestätigt.

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

Schlüsselpaare für RA-Mitarbeiter werden in entsprechend zertifizierten Smartcards generiert.

6.1.2 Bereitstellung der privaten Schlüssel an Antragsteller

Nicht anwendbar.

6.1.3 Übergabe öffentlicher Schlüssel an Zertifikatausssteller

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

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

Alle CA-Zertifikate werden wie in Kap. 2.2 beschrieben veröffentlicht. 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 generiert (CA, RA) bzw. akzeptiert (Endnutzer), welche mindestens eine Länge von 2048 Bit und eine durch 8 teilbare Länge des Modulo aufweisen. Für Schlüsselpaare, welche über das Jahr 2025 hinaus verwendet werden, gilt eine Mindestlänge von 3072 Bit.

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 Modulo eine ungerade Zahl ist, die nicht die Potenz einer Primzahl ist und keine Faktoren hat, die kleiner als 752 sind.

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

6.1.7 Schlüsselverwendung

Alle Zertifikate 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.

RA-Schlüssel werden in zertifizierten und kryptographisch sicheren SmartCards generiert und verwendet.

6.2.2 Mehrpersonenkontrolle über private Schlüssel (n von m)

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

6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung 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 in Betrieb befindlichen HSMs aufbewahrt werden.

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

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

6.2.7 Speicherung privater Schlüssel in kryptografischen Modulen

Private CA-Schlüssel werden ausschließlich in HSMs generiert, gespeichert und angewendet.

Eine Aufbewahrung außerhalb der operativen HSM oder Backup-HSM findet nicht statt.

6.2.8 Methoden zur Aktivierung privater Schlüssel

HSMs mit 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 Schlüssel-Zeremonie (siehe Kap. 6.1.1) und berücksichtigt alle Kopien der Schlüssel. Die Schlüssel werden mit den Bordmitteln der HSMs zerstört.

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

privaten Schlüssel, sofern die Schlüssel in anderen bzw. neuen kryptografischen Modulen noch weiter genutzt werden sollen.

6.2.11 Bewertung kryptografischer Module

Siehe Kap. 6.2.1.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des öffentlichen Schlüssels

Keine Bestimmungen.

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.

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“).

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

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

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

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.

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

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

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

Accounts werden mit Multi-Faktor-Authentifizierung oder starken Passwörtern gemäß aktueller Best Practices geschützt, wobei u.a. die Anforderungen der CAB-Forum Network Security Guidelines [NSG] eingehalten werden.

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.

6.5.2 Sicherheitsbewertung von Computern

Keine Bestimmungen.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Steuerung der Systementwicklung

Es sind konzernweite Prozesse etabliert, welche die Berücksichtigung von Sicherheitsanforderungen an die Entwicklung von PKI-Komponenten sicherstellt.

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

6.6.2 Maßnahmen des Sicherheitsmanagements

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

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

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.

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
- 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.

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 oder SOGIS.

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 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. 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 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.

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

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

6.8 Zeitstempel

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

7.1.1 Versionsnummer

Alle X509-Zertifikate werden in der Version 3 ausgestellt.

7.1.2 Zertifikatserweiterungen

TLS-Server-Zertifikate enthalten folgende Zertifikatserweiterungen:

- **authorityKeyIdentifier:** enthält den subjectKeyIdentifier der ausstellenden CA
- **subjectKeyIdentifier:** enthält „keyIdentifier“ gem. RFC5280 #4.2.1.1.
- **keyUsage:** (*kritisch*) „digitalSignature“ und für RSA (optional) „keyEncipherment“
- **basicConstraints:** (*kritisch*)
  - **„cA“:** „false“
  - **„pathLenConstraint“:** wird nicht gesetzt
- **CertificatePolicies:** gemäß Kapitel 7.1.6
- **subjectAltName:** enthält mindestens einen FQDN
- **extendedKeyUsage:** „id-kp-serverAuth“ und (optional) „id-kp-clientAuth“
- **cRLDistributionPoints:** enthält http-URL der zugehörigen CRL
- **authorityInfoAccess:** enthält entsprechende http-URLs für accessMethod 1.3.6.1.5.5.7.48.1 (ocsp) und accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)

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)

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

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

Die in der Mozilla Root Store Policy [MOZ] genannten Encodings werden eingehalten.

7.1.4 Namensformen

Domainvalidierte TLS-Server-Zertifikate enthalten folgende Namen:

- **commonName:** enthält genau einen im subjectAltName enthaltenen FQDN

Organisationsvalidierte TLS-Server-Zertifikate enthalten folgende Namen:

- **commonName:** enthält genau einen im subjectAltName enthaltenen FQDN
- **organizationName:** gemäß Validierung
- **country:** gemäß Validierung und ISO-3166-1
- **localityName:** gemäß Validierung
- **postalCode:** gemäß Validierung
- (Optional) **stateOrProvinceName:** gemäß Validierung und ISO-3166-2
- (Optional) **streetAddress:** gemäß Validierung

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 [BR]:

- 2.23.140.1.2.1 (Domain Validation)
- 2.23.140.1.2.2 (Organizational Validation)

Bei EE-Zertifikaten enthält der Qualifier „cPSuri“ 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“

Der Policy Qualifier wird 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 vertrauenden Dritten 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

Sperrlisten enthalten folgende CRL-Erweiterungen:

- AuthorityKeyIdentifier
- cRLNumber
- expiredCertsOnCRL

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

- unspecified (0)
- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- privilegeWithdrawn (9)

Die CRLReason keyCompromise (1) hat Vorrang gegenüber allen anderen Sperrgründen. Sollte kein Sperrgrund bekannt sein, also CRLReason unspecified (0) zutreffen, so wird die Sperrlisteneintragserweiterung reasonCode nicht gesetzt.

7.3 OCSP-Profil

Alle OCSP-Antworten werden gemäß den Anforderungen des 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.

7.3.1 Versionsnummer(n)

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

7.3.2 OCSP-Erweiterungen

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

8 AUDITS UND ANDERE BEWERTUNGS-KRITERIEN

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 und attestiert.

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 und Mitglied des Accredited Conformity Assessment Bodies‘ Council (ACAB’c).

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

Der Trust Service Public Certificate Services Platform wird inklusive aller dazugehörigen CAs gemäß ETSI EN 319 411-1 in der jeweils aktuellen Version geprüft. Die angewandten Policies sind:

- LCP in Verbindung mit DVCP und OVCP

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 konzerninterne sowie, im Falle von Audits nach ETSI, die je Finding vorgegeben Fristen eingehalten.

8.6 Mitteilung der Ergebnisse

Die von externen Prüfern erstellten Audit-Bescheinigungen aller CAs werden unverzüglich, spätestens jedoch innerhalb von 3 Monaten nach Ende der Prüfung in der „Common CA Database“ (CCADB) veröffentlicht. Im Falle einer Verzögerung 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. **Fehler! Verweisquelle konnte nicht g efunden werden.** 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

9.3.1 Umfang an vertraulichen Informationen

Alle Informationen im Kontext des Trust Services gelten als vertrauliche Informationen, sofern sie nicht gemäß Kapitel 9.3.2 explizit als nicht vertrauliche Informationen eingestuft wurden.

9.3.2 Umfang an nicht vertraulichen Informationen

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

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

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

Auftragnehmer oder Dritte werden ebenfalls vertraglich zur Einhaltung der 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 datenschutzrechtliche Freigabe des Betriebs.

9.4.2 Als privat zu behandelnde Informationen

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

9.4.3 Nicht als privat zu behandelnde Informationen

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

9.4.4 Verantwortung für den Schutz personenbezogener Informationen

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

9.4.5 Hinweis und Zustimmung zur Verwendung privater Informationen

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

9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

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

9.4.7 Andere Umstände der Offenlegung von Informationen

Nicht anwendbar.

9.5 Urheberrecht

Es gelten die gesetzlichen Vorschriften.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Telekom Security als Zertifizierungsstellenbetreiber

Telekom Security sichert die in der Telekom Security CP geforderten Zusicherungen und Gewährleistungen der Zertifizierungsstellenbetreiber zu. Insbesondere sichert Telekom Security 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 zusätzlich einen kostenlosen telefonischen Support an, um behinderte Menschen bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten zu unterstützen.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Telekom Security sichert die in der Telekom Security CP geforderten Zusicherungen und Gewährleistungen der RAs zu.

9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsnehmer

Telekom Security legt die Nutzungsbedingungen für die Endteilnehmerzertifikate gegenüber den Endteilnehmern fest und lässt deren Akzeptanz vor Ausstellung der Zertifikate von den Endteilnehmern bestätigen. Diese Nutzungsbedingungen berücksichtigen die in der Telekom Security CP Kapitel 9.6.3 geforderten Zusicherungen, Gewährleistungen und anzugebenen Informationen.

9.6.4 Zusicherungen und Gewährleistungen vertrauender Dritter

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

9.6.5 Zusicherungen und Gewährleistungen sonstiger Teilnehmer

Keine Bestimmungen.

9.7 Gewährleistungsausschlüsse

Etwaige Gewährleistungsausschlüsse werden in den Allgemeinen Geschäftsbedingungen 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 Nutzungsbedingungen beschrieben und entsprechen geltendem Recht.

9.9 Schadensersatz

Etwaige Schadenersatzansprüche gegenüber der Telekom Security werden in 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 bestehenden Zertifikate, bis es durch eine neue Version ersetzt wird.

9.10.2 Terminierung

Siehe 9.10.1.

9.10.3 Effekt einer Terminierung und Fortführungen

Keine Bestimmungen.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Bestimmungen.

9.12 Änderungen

9.12.1 Verfahren für Änderungen

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

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

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

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Neue Versionen dieses CPS werden gemäß Kapitel 2 veröffentlicht.

Neue Versionen der Nutzungsbedingungen, die sich auf die Akzeptanz des Dienstes durch die Zertifikatsnehmer oder die Zertifikatsnutzer auswirken könnten, werden rechtzeitig den Zertifikatsnehmern, den Zertifikatsnutzern und, sofern anwendbar, Bewertungsstellen und Aufsichts- oder anderen Regulierungsbehörden bekannt gegeben.

9.12.3 Umstände, unter denen der OID geändert werden muss

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

9.13 Bestimmungen zur Beilegung von Streitigkeiten

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

Keine Bestimmungen.

9.16.3 Salvatorische Klausel

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

9.16.4 Rechtsdurchsetzung

Keine Bestimmungen.

9.16.5 Höhere Gewalt

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

9.17 Sonstige Bestimmungen

Keine Bestimmungen.