Telekom Security PKI - Certificate Policy

Zertifizierungsrichtlinie für die Telekom Security Trust Center Public Key Infrastruktur

Deutsche Telekom Security GmbH

Öffentlich

Version: 12.00

Gültig ab: 01.07.2020

Status: Freigabe

Letztes Review: 05.06.2020

IMPRESSUM

Tabelle 1 – Impressum

Angaben	Ausprägung
Herausgeber	Deutsche Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Deutschland
Dateiname	Telekom-Security-PKI-CP-DE-v12.00-20200605.docx
Gültig ab	01.07.2020
Titel	Telekom Security PKI - Certificate Policy Zertifizierungsrichtlinie für die Telekom Security Trust Center Public Key Infrastruktur
Version	12.00
Letztes Review	05.06.2020
Status	Freigabe
Ansprechpartner	Deutsche Telekom Security Leiter Trust Center Betrieb
Kurzbeschreibung	Zertifizierungsrichtlinie für Telekom Security PKI

ÄNDERUNGSHISTORIE

Tabelle 2 – Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
8.0	15.05.2018	T-Systems	Initialversion nach RFC 3647 Struktur und Auftrennung zwischen CP und CPS. Aus diesem Grund wurde eine neue Änderungshistorie begonnen. Ältere Versionen des CP/CPS basieren auf einer abweichenden Struktur.
9.0	12.10.2018	T-Systems	Einarbeitung Änderungen in Kapitel 1.5.2, 4.9 und 5
10.0	10.10.2019	T-Systems	Einarbeitung BR-Änderungen gemäß BR 1.5.7 bis BR 1.6.6 Einarbeitung EV-Änderungen gemäß EV 1.6.9 bis 1.7.0
10.1 10.2 10.3	04.02.2020	T-Systems	- Änderung Dokumentenvorlage auf Barrierefreiheit - Einarbeitung Mozilla 2.7 Anforderungen - Einarbeitung BR-Änderungen gemäß BR 1.6.7 - Einarbeitung EV-Änderungen gemäß EV 1.7.1
10.3	04.02.2020	T-Systems	Bereitstellung zur Prüfung
10.4	03.03.2020	T-Systems	Anpassungen
11.00	13.03.2020	T-Systems	Freigabe
11.01	05.06.2020	T-Systems	Änderung von T-Systems International GmbH zu Deutsche Telekom Security GmbH
11.02	05.06.2020	T-Systems	Review
11.03	05.06.2020	T-Systems	QS
12.00	08.06.2020	T-Systems	Freigabe

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS

ABBILDUNGSVERZEICHNIS

In der aktuellen Version sind keine Abbildungen vorhanden.

1 EINLEITUNG

1.1 Überblick

Die Telekom Security Trust Center Public Key Infrastruktur (Telekom Security PKI) wird durch die Konzerneinheit Deutsche Telekom Security GmbH in der Deutschen Telekom AG im Trust Center betrieben. Das Trust Center unterhält eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Stammzertifizierungsstellen (Root-CAs).

Bei dem vorliegenden Dokument handelt es sich um die Zertifizierungsrichtlinie (engl. Certification Policy, kurz CP) für alle innerhalb der Telekom Security PKI betriebenen Zertifizierungsstellen, wobei der Fokus auf der Root-CA liegt. Es orientiert sich an dem internationalen Standard für Zertifizierungsrichtlinien RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) der Internet Engineering Task Force (IETF).

Das Trust Center sichert weiterhin zu, dass alle Zertifizierungsstellen innerhalb der Telekom Security PKI die Anforderungen und Regelungen der jeweils aktuellen veröffentlichten Version der „CA/Browser-Forum Baseline Requirements“ [CAB-BR] (http://www.cabforum.org/documents.html) zu erfüllen und einzuhalten. Im Falle eines Widerspruchs zwischen dem vorliegenden Dokument und den [CAB-BR], haben die Regelungen aus den [CAB-BR] Vorrang.

1.2 Dokumentenidentifikation

Tabelle 3 – Dokumenteneigenschaften

Name	Version	Gültig ab	Objektbezeichnung (Object Identifier)
Telekom Security PKI - Certificate Policy	12.00	01.07.2020	1.3.6.1.4.1.7879.13.38

1.2.1 Revisionen

Siehe Änderungshistorie zu Anfang des Dokuments.

1.2.2 Relevante Daten

Siehe Änderungshistorie zu Anfang des Dokuments.

1.3 PKI Beteiligte

1.3.1 Zertifizierungsstellen (CA)

Neben dem Betrieb von Zertifizierungsstellen für eigene interne Produkte und Dienstleistungen stellt das Trust Center CA-Zertifikate für Zertifizierungsstellen anderer Betreiber aus.

1.3.2 Registrierungsstellen (RA)

Jeder Zertifizierungsstelle sind eine oder mehrere Registrierungsstellen zugeordnet. Es gibt keine Begrenzung hinsichtlich der Anzahl der zugeordneten Registrierungsstellen. Eine Registrierungsstelle ist der zugeordneten Zertifizierungsstelle unterstellt, und agiert als

vorgelagerte Schnittstelle zu den Teilnehmern der PKI. Die Registrierungsstellen sind daher ebenso dieser CP untergeordnet.

Bei der Mehrzahl der Zertifizierungsstellen gibt es eine Hierarchiebildung innerhalb der zugeordneten Registrierungsstellen in eine oder mehrere übergeordnete und eine oder mehrere nachgeordnete Registrierungsstellen. Jede nachgeordnete Registrierungsstelle ist genau einer übergeordneten Registrierungsstelle zugeordnet.

Aufgaben von übergeordneten Registrierungsstellen sind:

- die Zulassung und der Widerruf nachgeordneter Registrierungsstellen,
- die Zuordnung des jeweiligen Verantwortungsbereiches einer nachgeordneten Registrierungsstelle (für welche Teilmenge der Teilnehmeraufträge ist die Registrierungsstelle verantwortlich?),
- die Sperrung bzw. Suspension von Teilnehmerzertifikaten über alle Verantwortungsbereiche.
- Aufgaben von nachgeordneten Registrierungsstellen sind:
- die Registrierung von Teilnehmern innerhalb des definierten Verantwortungsbereiches,
- Prüfung von Teilnehmeraufträgen innerhalb des definierten Verantwortungsbereiches gemäß den Richtlinien der jeweiligen Zertifizierungsstelle (ggf. unter Zuhilfenahme beglaubigter oder mit Dienstsiegeln versehener Identifikationsdokumente),
- nach erfolgreicher Prüfung die Freigabe oder andernfalls die Ablehnung dieser Teilnehmeraufträge,
- in Folge der Freigabe eines Teilnehmerauftrags den Auftrag an die Zertifizierungsstelle zur Ausstellung und Auslieferung des Teilnehmerzertifikats übermitteln,
- die Entgegennahme und Prüfung von Aufträgen auf Zertifikatssperrung oder –suspension innerhalb des definierten Verantwortungsbereiches (falls Suspension im Rahmen der jeweiligen Zertifizierungsstelle vorgesehen ist),
- in Folge der Freigabe eines Sperr- oder Suspensionsauftrags den Auftrag an die Zertifizierungsstelle zur Sperrung bzw. Suspension des Teilnehmerzertifikats übermitteln.

Wird keine Hierarchiebildung der Registrierungsstellen vorgenommen, erfüllen die Registrierungsstellen gleichrangig die Aufgaben der nachgeordneten Registrierungsstellen, ohne dass eine Trennung in Verantwortungsbereiche vorliegt.

Die Registrierungsstellen werden mit der notwendigen Technologie ausgestattet. Die Mitarbeiter der Registrierungsstellen authentifizieren sich sicher gegenüber der jeweiligen Zertifizierungsstelle.

1.3.3 Zertifikatsnehmer (Subscriber)

Zertifikatsnehmer der Root-CAs sind ausschließlich unmittelbar nachgeordnete Zertifizierungsstellen. Es werden keine Endteilnehmer Zertifikate ausgestellt.

Der Zertifikatsnehmer:

- beantragt das Zertifikat (vertreten durch eine berechtigte natürliche Person)
- wird im Rahmen der Registrierung von der zuständigen CA authentifiziert
- wird durch das Zertifikat identifiziert, d.h. es wird bestätigt, dass der im Zertifikat enthaltene öffentliche Schlüssel dem Zertifikatsnehmer gehört
- ist im Besitz des privaten Schlüssels, der zum öffentlichen Schlüssel im Zertifikat gehört

1.3.4 Vertrauender Dritter (Relying parties)

Ein vertrauender Dritter (Relying Party) ist eine natürliche Person oder Subjekt, die/das sich auf die Vertrauenswürdigkeit des von Telekom Security ausgestellten Zertifikats und/oder digitalen Signatur verlässt.

1.3.5 Andere Teilnehmer

Es werden keine Funktionen und/oder Aufgaben an externe Stellen ausgelagert (Delegated Third Party), welche den Betrieb der CA-Infrastruktur, die Prüfung, Genehmigung, Bearbeitung oder Verwaltung von Zertifikaten oder Zertifikatsaufträgen betreffen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Zertifikate werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Attribute zur Key Usage und den Festlegungen des CPS der jeweiligen Zertifizierungsstelle eingesetzt.

Der Zertifikatsnehmer ist dafür verantwortlich, Zertifikate so zu verwenden, dass die Verwendung den anwendbaren gesetzlichen Bestimmungen entspricht. Dies gilt insbesondere für die Einhaltung der jeweils anwendbaren Ausfuhr- oder Einfuhrbestimmungen.

1.4.2 Unzulässige Verwendung von Zertifikaten

Zertifikate sind nicht zur Verwendung oder zur Weitergabe vorgesehen, ausgelegt oder zugelassen für:

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

Es ist außerdem nicht zulässig ein ausgestelltes Zertifikat für ein MitM- Szenario zu verwenden oder wenn die Nutzung gesetzlich verboten ist.

1.5 Verwaltung des Dokuments

1.5.1 Organisatorische Zuständigkeit für dieses Dokument

Dieses Dokument (CP) wird herausgegeben von Deutsche Telekom Security GmbH, Trust Center & ID-Solutions.

1.5.2 Kontaktinformationen

Adresse:

Deutsche Telekom Security GmbH

Trust Center & ID Solutions

Leiter Trust Center Betrieb

Untere Industriestraße 20

57250 Netphen, Deutschland

Telefon:

+49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)

WWW: https://www.telesec.de

E-Mail: telesec_support@t-systems.com

Die Meldung von Missbrauch, Kompromittierung von Zertifikaten und Schlüsseln des Trust Center müssen unter einer URL für jedermann 7x24h abgesetzt werden können. Die Webseite muss eine Prozessbeschreibung/Instruktionen für den Nutzer enthalten und dies muss zusätzlich im Kapitel 1.5.2 des CPS dargestellt werden.

1.5.3 Pflege der Richtlinie und Konformität des CPS

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

Das CPS ist konform zur vorliegenden CP zu erstellen.

1.5.4 Genehmigungsverfahren dieses Dokuments (CP)

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

Die vorliegende CP wird unabhängig von weiteren Änderungen einem jährlichen Review unterzogen. Verantwortlich für die Durchführung bzw. die Koordination des Reviews ist die in Kapitel 1.5.1 benannte Stelle.

Das jährliche Review ist in der Änderungshistorie des CP zu vermerken. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden.

1.6 Definitionen und Abkürzungen

1.6.1 Glossar

Tabelle 4 - Glossar

Begriff	Erläuterung
Antrag auf ein Zertifikat mit erhöhtem Risiko	Ein Antrag, für den die CA eine Zusatzprüfung im Hinblick auf interne Kriterien und Datenbanken vorsieht, die von der CA geführt werden. Dies kann Namen betreffen, die in Bezug auf Phishing oder eine andere betrügerische Nutzung einem höheren Risiko ausgesetzt sind, Namen, die in zuvor abgelehnten Zertifikatsanträgen oder widerrufenen (gesperrten) Zertifikaten enthalten sind, Namen, die auf der MillerSmiles-Phishing-Liste oder auf der Safe-Browsing-Liste von Google stehen bzw. Namen, die die CA anhand ihrer eigenen Risikominderungskriterien identifiziert.

Begriff	Erläuterung
Antragsteller	Die natürliche oder juristische Person, die ein Zertifikat (oder dessen Erneuerung) beantragt. Ist das Zertifikat einmal ausgestellt, wird der Antragsteller als Zertifikatnehmer bezeichnet. Bei für Geräte ausgestellten Zertifikaten ist der Antragsteller die Organisation, die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt, auch wenn das Gerät den eigentlichen Antrag auf das Zertifikat sendet.
Anwendungssoftwareanbieter	Ein Anbieter von Internetbrowser-Software oder anderer Anwendungssoftware der vertrauenden Seite, die Zertifikate anzeigt oder verwendet und Stammzertifikate (Root) beinhaltet.
Ausstellende Zertifizierungsstelle (CA)	Die Zertifizierungsstelle (CA), die ein bestimmtes Zertifikat ausgestellt hat. Dabei kann es sich um eine Stammzertifizierungsstelle (Root-CA) oder eine untergeordnete Zertifizierungsstelle (Sub-CA) handeln.
Authentifizierung	Prüfung einer Identität an Hand behaupteter Merkmale.
Authority Revocation List (ARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (außer Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
Beauftragte Drittpartei	Eine natürliche oder juristische Person, die nicht identisch mit der Zertifizierungsstelle (CA) ist, jedoch von dieser bevollmächtigt ist, den Zertifikatsverwaltungsprozess zu unterstützen, indem sie Aufgaben zur Erfüllung einer oder mehrerer Anforderungen erfüllt. Dies kann z.B. eine externe Registrierungsstelle oder auch eine interne enterprise Registrierungsstelle sein.
Berechtigungsdokument	Die Dokumentation, die die Berechtigung eines Antragstellers belegt, ein oder mehrere Zertifikat(e) für eine bestimmte natürliche Person, Personen- und Funktionsgruppen, juristische Personen oder Gerät zu beantragen. Es kann sich auch um ein Dokument der Zertifizierungsstelle über eine Kommunikation mit der betreffenden Person oder Organisation handeln.
Bezugsvertrag (Subscriber Agreement)	Eine Vereinbarung zwischen der Zertifizierungsstelle (CA) und dem Antragsteller/Zertifikatnehmer, in der die Rechte und Verpflichtungen der Parteien festlegt werden.
Bulk	Funktion einer CA mit der der Sub-Registrator Soft-PSE per Massengenerierung erzeugen kann.
Certificate Management Protocol (CMP)	Das Zertifikat-Verwaltungsprotokoll, ist ein von der IETF entwickeltes Protokoll, zur Verwaltung von X.509-Zertifikaten innerhalb einer Public-Key-Infrastruktur (PKI).
Certificate Policy (CP)	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Signing Request (CSR) [TC]	Von einem Gerät (z.B. Server) elektronisch erstellt und mit dem privaten Schlüssel signierter Zertifikatsantrag, der in kodierter Form den öffentlichen Schlüssel und die Zertifikatsdaten enthält. Die Syntax wird durch den Standard PKCS#11 beschrieben.
Certificate Revocation List (CRL)	Siehe Sperrliste
Certification Authority (CA)	Siehe Zertifizierungsstelle.
Certification Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
Change Advisory Board	Gremium innerhalb der Telekom Security, das über PKI-Funktionalitäten entscheidet.
Chipkarte	Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.

Begriff	Erläuterung
Dezentrales Registrierungsmodell	Der Benutzer stellt über die Benutzer-Webseite oder per Mail-Request oder das Gerät stellt über seine SCEP-Schnittstelle den Zertifikatsantrag, den der Sub-Registrator bearbeitet (Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage)).
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Domain-Berechtigungs-dokument	Die Dokumentation, die von der Domain-Namen-Registrierungsstelle (Domain Name Registrar), einem registrierten Domain-Inhaber (Domain Name Registrant) oder der Person bzw. Organisation bereitgestellt wird, die in WHOIS als registrierter Domain-Inhaber aufgeführt ist (einschließlich aller privaten, anonymen oder Proxy-Registrierungsservices), und die Berechtigung eines Antragstellers belegt, ein Zertifikat für einen bestimmten Domain-Namensraum zu beantragen. Es kann sich auch um ein Dokument der Zertifizierungsstelle über eine Kommunikation mit der betreffenden Person oder Organisation handeln.
Domain-Name	Die Bezeichnung, die einem Knoten im Domain Name System (DNS) zugeordnet ist.
Dual-Key-Zertifikat	Variante, bei der für Verschlüsselung und Signatur getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt zwei korrespondierende Zertifikate.
Endteilnehmer	Siehe auch Zertifikatnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Endteilnehmer-Zertifikat	Ein Zertifikat, welches nicht die Basiseinschränkung (basic constraints) „Zertifizierungsstelle“ verwendet, daher selber keine Zertifikate signieren kann.
Erklärung zum Zertifizierungsbetrieb (CPS)	Eines von mehreren Dokumenten, die allgemeine und spezifische Rahmenbedingungen vorgibt. Das beninhaltet insbesondere eine Beschreibung der Verfahrensweise, wie die Zertifizierungsstelle (CA) Zertifikate ausstellt, verwaltet, sperrt und erneuert.
Erlaubte Internet-Domänen	Ein Domänenname, der aus der Top-Level-Domain und weiteren Sub-Domains besteht, und nach erfolgreicher Prüfung durch die interne Registrierungsstelle als „erlaubte Internet-Domäne“ in die PKI-Konfiguration des Mandanten (Master-Domäne) aufgenommen wird.
ETSI-Zertifizierung	Überprüfung und Bestätigung für Zertifizierungsstellen durch einen unabhängigen Gutachter, das die PKI nach den ETSI-Kriterien „ETSI TS 102 042“ betrieben werden. Ziel der ETSI-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken.
Externe Registrierungsstelle	Ein Mitarbeiter (Beschäftigter) oder Vertreter eines der Zertifizierungsstelle (CA) nicht verbundenen Unternehmens (non Affiliate), der die Ausstellung von Zertifikaten für Dritte genehmigt. Diese Rollen (Trusted Roles) werden z.B. vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen.
Gerät	Komponente wie beispielsweise Router, Server, Gateway, Applikation, die zertifikatsbasierende Funktionen unterstützen, selbst aber nicht oder nur begrenzt selbst Zertifikate beantragen können. Häufig werden Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.
Geräte-Zertifikat	X.509 V3 Zertifikat, welches im commonName-Feld (CN) des distinguishedName des Zertifikatnehmers (Subject) und/oder in mindestens einer subjectAltName-Erweiterung entweder einen Hostname, IP-Adresse oder Mail-Adresse enthält.
Gültiges Zertifikat	Ein Zertifikat, das dem in RFC 5280 dargelegten Validierungsverfahren besteht.

Begriff	Erläuterung
Gültigkeitsdauer	Der Zeitraum vom Ausstellungsdatum (not before) des Zertifikats bis zum Ablaufdatum (not after).
Hardware Security Modul (HSM)	Hardware zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hashwert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
Identifizierung	Der Prozess der Mitteilung der Identität eines Subjekts oder Objekts (z.B. Benutzer, Gerät) an ein System. Die Identifizierung ist ein Bestandteil der Validierung.
Interface	Schnittstelle als Teil eines Systems, dass zur Kommunikation (Ein- und Ausgabe) dient.
Interne Registrierungsstelle	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer der CA, der die vom PKI-Mandanten benannten „Domain“ prüft und diesem zur Zertifikatsbeantragung zur Verfügung stellt. Diese Rolle (Trusted Role) wird z.B. vom Trust-Center-Operator der Telekom Security wahrgenommen.
Interner Server-Name	Ein Server-Name (der einen nicht registrierten Domain-Namen enthalten kann oder nicht), der nicht mit dem öffentlichen Domain Name System (DNS) aufgelöst werden kann.
Issuer-Distinguished-Name (Issuer-DN)	Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Issuer-DN bezeichnet eindeutig die Zertifizierungsstelle.
Juristische Person	Eine Gesellschaft, ein Konzern, eine Partnerschaft, Einzelfirma, Treuhandgesellschaft, Regierungsbehörde oder eine andere klagebefugte Rechtspersönlichkeit innerhalb des Rechtssystems eines Landes.
Key-Back-Up	Mechanismus zur Schlüsselsicherung. Um beispielsweise verschlüsselte E-Mails bei Schlüsselverlust wieder herstellen zu können empfiehlt sich das Key-Back-Up des Schlüsselmaterials des Verschlüsselungsschlüssels. Key-Back-Up wird auch als Synonym für Key-Archiving benutzt.
Key-Recovery	Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert.
Kompromittierung	Ein privater Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
Land	Entweder ein Mitglied der Vereinten Nationen oder eine geographische Region, die von mindestens zwei Mitgliedsländern der UNO als souveräner Staat anerkannt wird.
Latenzzeit	Zeitraum zwischen einer Aktion und dem Eintreten einer verzögerten Reaktion (Verzögerungszeitraum). Bei der Latenzzeit erfolgt die Aktion im Verborgenen und wird erst durch die Reaktion festgestellt.
LDAP-Server	Server, der Informationen speichert, die über LDAP abrufbar sind.
Lightweight Directory Access Protocol (LDAP)	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Mail-Security	Security-Funktionen wie Digitale Signatur und Verschlüsselung, die Standard-Mail-Anwendungen unterstützen.

Begriff	Erläuterung
Managementsystem für Informationssicherheit (ISMS)	Das „Managementsystem für Informationssicherheit“ (ISMS) ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Der Begriff wird im Standard ISO/IEC 27002 verwendet, ISO/IEC 27001 definiert ein ISMS.
Mandant	Der Mandant stellt eine eigene logische abgeschlossene Einheit mit eigener Rechte-, Organisations- und Datenverwaltung innerhalb des Systems dar. Der Mandant strukturiert somit die Nutzung des Systems. Als Mandant wird z.B. die Master-Domäne bezeichnet. Innerhalb der Master-Domäne bestehen weitere Untergliederungen in Form von Zuständigkeitsbereichen (auch als Sub-Domänen bezeichnet).
Mandantenfähigkeit	Als Mandantenfähigkeit bezeichnet man in der Informationstechnik (IT) die Eigenschaft einer Software bzw. Server, auf einer Installation mehrere logisch voneinander vollständig getrennte Mandanten abzubilden. Die jeweiligen Mandanten, etwa unterschiedliche rechtliche Einheiten oder Firmen, haben dabei keinerlei gegenseitigen Einblick in die Daten, Benutzerverwaltung oder Ähnliches der anderen Parteien/Mandanten.
Master-Domäne	Eigenständiger, mit einem eindeutigen Namen festgelegter Verwaltungsbereich, der ausschließlich für eine beauftragte Drittpartei (Delegated Third Party) eingerichtet wird. Innerhalb des Mandanten kann die beauftragte Drittpartei Zertifikate genehmigen und verwalten. Der Mandant wird mit dem Master-Registrator-Zertifikat verwaltet. Weitere Informationen finden Sie auch unter: Mandant.
Master-Registrator	Natürliche Person (Trusted Role) der die Master-Domäne verwaltet.
Nicht registrierter Domain-Name	Ein Domain-Name, der kein registrierter Domain-Name ist.
Nutzungsbedingungen (Terms of Use)	Bestimmungen bezüglich der Verwahrung und zugelassenen Verwendungszwecke eines ausgestellten Zertifikats in Übereinstimmung mit den gegebenen Anforderungen, wenn der Antragsteller/Zertifikatnehmer beispielsweise ein verbundenes Unternehmen der Zertifizierungsstelle (CA) ist.
Object Identifier (OID)	Ein eindeutiger alphanumerischer oder numerischer Bezeichner, der unter dem jeweiligen Standard für ein bestimmtes Objekt oder eine Objektklasse der Internationalen Organisation für Normung (ISO) registriert ist.
Online Certificate Status Protocol (OCSP) [BR]	Ein Protokoll zur Online-Zertifikatsvalidierung, mit dessen Hilfe die Anwendungssoftware der vertrauenden Seite den Status eines identifizierten Zertifikats bestimmen kann. Siehe auch OCSP-Responder.
OCSP-Responder	Ein Online-Server, der der Zertifizierungsstelle (CA) untersteht und mit deren zentrale Datenablage (Repository) zur Bearbeitung von Zertifikatsstatusanfragen verbunden ist. Siehe auch Online Certificate Status Protocol (OCSP).
Öffentlicher Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Inhaber des entsprechenden privaten Schlüssels offen gelegt werden darf und der von der vertrauenden Seite verwendet wird, um digitale Signaturen zu verifizieren, die mit dem privaten Schlüssel des Inhabers erstellt wurden, und/oder um Mitteilungen zu verschlüsseln, die nur mit dem zugehörigen privaten Schlüssel des Inhabers entschlüsselt werden können.
Öffentliches Geräte-Zertifikat	Ein Geräte-Zertifikat, welches in der CA-Hierarchie von einer Sub-CA unterhalb eines öffentlichen Root-Zertifikates ausgestellt ist.
Personal Identification Number (PIN)	Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.
Personal Security Environment (PSE)	In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.

Begriff	Erläuterung
Privater Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Schlüsselpaarinhaber geheim gehalten und verwendet wird, um digitale Signaturen zu erstellen und/oder elektronische Daten und Dateien zu entschlüsseln, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
Public Key Service (PKS)	Service des Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Policy	Richtlinien bzw. Erklärung, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
Personal Security Environment (PSE)	In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Public Key Infrastruktur	Hardware, Software, Personen, Verfahren, Regeln, Richtlinien und Verpflichtungen, mit denen die vertrauenswürdige Generierung, Ausstellung, Verwaltung und Verwendung von Zertifikaten und Schlüsseln auf der Basis der Public-Key-Kryptographie ermöglicht wird.
Qualifizierter Auditor	Eine natürliche oder juristische Person, welche die an sie gestellten Anforderungen erfüllt.
Registrierter Domain-Name	Ein Domain-Name, der bei einer Domain-Namen-Registrierungsstelle (Registrar) registriert wurde.
Registrierungsstelle (RA)	Eine juristische Person, die für die Identifizierung und Authentifizierung von Zertifikatssubjekten zuständig ist. Sie ist jedoch keine CA und signiert somit keine Zertifikate und stellt diese nicht aus. Eine RA kann bei der Beantragung oder beim Widerruf eines Zertifikats oder in beiden Fällen Unterstützung leisten. Wenn „RA“ als Adjektiv verwendet wird, um eine Rolle oder eine Funktion zu beschreiben, ist nicht zwangsläufig von einer eigenständigen Stelle die Rede. Sie kann jedoch Teil der CA sein.
Registrierungsmodell	Es wird zwischen Zentralem Registrierungsmodell (siehe dort) und Dezentralem Registrierungsmodell (siehe dort) unterschieden.
Registrierungs-stelle eines Unternehmens (Enterprise RA)	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der nicht der Zertifizierungsstelle (CA) angegliedert ist (non Affiliate), der die Ausstellung von Zertifikaten für diese Organisation genehmigt. Diese Rollen (Trusted Roles) können z.B. vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen werden.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, dass nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
Root-CA	Siehe Wurzelzertifizierungsstelle.
Schlüssel-kompromittierung	Ein privater Schlüssel (Private Key) gilt als kompromittiert, wenn sein Wert einer nicht autorisierten Person offengelegt wurde, eine nicht autorisierten Person Zugriff auf ihn hatte oder es eine praktische Methode gibt, mit der eine nicht autorisierte Person seinen Wert a usfindig machen kann.
Schlüsselpaar	Der private Schlüssel und der dazugehörige öffentliche Schlüssel.
Schlüsselverantwortlicher	Eine durch die beauftragte Drittpartei (Delegated Third Party) autorisiert natürliche Person, die verantwortlich ist für die ordnungsgemäße Verwendung (Verteilung, Nutzung und ggf. Sperrung) des Schlüsselpaars und Zertifikat, dass für eine Personen- und Funktionsgruppe, juristische Person oder Gerät ausgestellt wurde.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Erweiterung des E-Mail-Formats MIME, die Zusätze für kryptografische Dienste beschreibt, welche Authentizität, Integrität und Vertraulichkeit von Nachrichten sicherstellen.

Begriff	Erläuterung
Secure Socket Layer (SSL)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet, inzwischen durch das neuere Verfahren TLS abgelöst. Kann ihn vielen Fällen statt dem komplexeren IPSec verwendet werden.
Service Desk	Das Service Desk ist eine organisatorische Einheit innerhalb eines Unternehmens, das für den Mandanten bzw. beauftragte Drittpartei (Delegated Third Party) als zentrale Anlaufstelle für alle Service- und Supportanfragen dient und diese innerhalb des Unternehmens entsprechend den vereinbarten Geschäftsprozessen vermittelt.
Simple Certificate Enrollment Protocol (SCEP)	Simple Certificate Enrollment Protocol. Protokoll zur Beauftragung und zum Laden von Zertifikaten in IPSec Devices.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP stellt einen einfachen Mechanismus zum Austausch von strukturierter Information zwischen Anwendungen in einer dezentralisierten, verteilten Umgebung zur Verfügung.
Single-Key-Zertifikat	Variante, bei der für Verschlüsselung und Signatur das gleiche Schlüsselpaar verwendet wird. D. h. ein Benutzer besitzt ein Zertifikat.
Software-PSE (Soft-PSE)	Eine verschlüsselte Datei zur Speicherung des Zertifikats und den zugehörigen privaten und öffentlichen Schlüssel.
Smartcard	Spezielle Plastikkarte mit integriertem Computerchip, die auch für kryptografische Anwendungen eingesetzt werden kann.
Sperrberechtigte(r)	Person, die von einem Zertifikatnehmer oder Schlüsselverantwortlichen autorisiert ist, ein Zertifikat für eine Personen- und Funktionsgruppe, juristische Person oder Gerät sperren zu dürfen. Die Autorisierung erfolgt über das Zertifikatssperrpasswort.
Sperrinstanz	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der Zertifikatssperrungen durchführt.
Stammzertifizierungsstelle (Root-CA)	Die oberste Zertifizierungsstelle, deren Stammzertifikat von Anwendungssoftwareanbietern verteilt wird und die untergeordnete CA-Zertifikate (Sub-Zertifikate) ausstellt.
Subject Alternative Name	Zusätzliche Felder in einem Zertifikat. Die Felder können zusätzliche Namen des Zertifikatsnehmers enthalten und ist eine Standarderweiterung des X509 Standards.
Subject-Distinguished-Name (Subject-DN)	Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Subject-DN bezeichnet eindeutig die Person oder Gerät.
Subjekt	Die natürliche Person, das Gerät, System, die Einheit oder juristische Person, die in einem Zertifikat als Subjekt benannt wird. Das Subjekt ist entweder der Zertifikatnehmer oder ein Gerät, das der Kontrolle des Zertifikatnehmers untersteht oder von diesem betrieben wird.
Subjektidentitätsdaten	Daten, die das Zertifikatssubjekt identifizieren. Subjektidentitätsdaten beinhalten keinen Domain-Namen, der in der Erweiterung subjectAltName oder im Feld Subject commonName aufgeführt ist.
Sub-Registrator	Natürliche Person (Trusted Role) der den Zuständigkeitsbereich verwaltet.
Suspension	Im Zusammenhang von PKI ist unter Suspendierung die vorläufige bzw. temporäre Sperrung zu verstehen. Das Zertifikat erscheint zunächst in der Zertifikatssperrliste kann aber durch den Sub-Registrator wieder aktiv geschaltet werden.
Transport-Layer Security (TLS)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet.
Triple-Key-Zertifikat	Variante, bei der für Verschlüsselung, Signatur und Microsoft Smartcard-LogOn getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt drei entsprechende Zertifikate.
Untergeordnete Zertifizierungsstelle (Sub-CA)	Eine Zertifizierungsstelle, deren Zertifikat von der Stammzertifizierungsstelle (Root-CA) oder einer anderen untergeordneten Zertifizierungsstelle (CA) signiert wird.

Begriff	Erläuterung
Validierung	Ein Nachweis der Reproduzierbarkeit eines Ergebnisses aus einer beschriebenen Vorgehensweise unter definierten Bedingungen. Je exakter eine Vorgehensweise beschrieben ist und je weniger unbekannte Einflussfaktoren bestehen, desto sicherer ist es, übereinstimmende Resultate zu erzeugen. Für eine Validierung benötigt man die Beschreibung des Zieles und des Weges. Valide bedeutet in diesem Zusammenhang, dass der Weg wiederholbar zum Ziel führt. Im Kontext einer PKI besteht ein Validierungsprozess an folgenden Stellen: Mitteilung und Prüfung einer Identität (z.B. natürliche Person, Gerät) gegenüber dem Zertifikatsantrag. Algorithmus zur Überprüfung eines Zertifikats auf Gültigkeitsdauer (Gültigkeitszeitraum), ausstellende Zertifizierungsstellen und Zertifikatsstatus (gültig, gesperrt).
Validierungsspezialist	Jemand, der die Datenüberprüfungsaufgaben gemäß den jeweiligen Anforderungen wahrnimmt. Im Kontext des Trust-Centers sind dies die Rolleninhaber: Trust-Center-Operator, Master-Registrator, Sub-Registrator
Verbundenes Unternehmen (Affiliate)	Beispielsweise ein Unternehmen, eine Partnerschaft, ein Joint Venture, Körperschaft, (Kapital) Gesellschaft, Verband, Stiftung oder eine andere Organisation (juristische Person), welche eine andere Organisation (juristische Person), Einrichtung, Abteilung, Gebietskörperschaft oder eine Einheit, die einer Regierungsbehörde direkt unterstellt ist, beaufsichtigt, von dieser beaufsichtigt wird oder mit dieser einer gemeinsamen Kontrolle untersteht.
Vertrauende Dritte (Relying Parties)	Eine natürliche oder juristische Person, die sich auf ein gültiges Zertifikat verlässt. Ein Anbieter von Anwendungssoftware gilt nicht als vertrauender Dritter, wenn die von diesem Anbieter vertriebene Software lediglich Informationen zu einem Zertifikat anzeigt.
Vertrauenswürdiges Zertifikat	Ein Zertifikat, dem aufgrund der Tatsache vertraut wird, dass sein entsprechendes Stammzertifikat als Vertrauensanker in weit verbreiteter Anwendungssoftware verteilt ist
Vertreter des Antragstellers	Falls abweichend vom Antragsteller, eine natürliche Person oder Kostenträger, ein Beschäftigter des Antragstellers oder ein Handlungsbevollmächtigter ist, der die ausdrückliche Befugnis besitzt, den Antragsteller zu vertreten: (i) die im Namen des Antragstellers einen Antrag auf ein Zertifikat unterzeichnet, einreicht oder genehmigt, und/oder (ii) die im Namen des Antragstellers eine Bezugsvertrag (Subscriber Agreement) unterzeichnet und einreicht, und/oder (iii) die im Namen des Antragstellers die Nutzungsbestimmungen des Zertifikats anerkennt und ihnen zustimmt, wenn der Antragsteller eine verbundene Unternehmen (Affiliate) der Zertifizierungsstelle (CA) ist.
Verzeichnisdienst	Datenspeicher zum Abruf von Zertifikaten und Zertifikats-Validierungsinformationen (Sperrlisten).
Vollmacht	Unter einer Vollmacht versteht man die durch ein Rechtsgeschäft begründete Vertretungsmacht. Die Vollmacht entsteht durch einseitige empfangsbedürftige Willenserklärung des Vollmachtgebers gegenüber dem Vollmachtnehmer.
Voll qualifizierter Domain-Name (FQDN)	Korrekter und vollständiger Domain-Name, d.h. Verkettung aller Labels eines Pfades im Domain-Namensraum (weitere Informationen siehe RFC 2181).
WHOIS	Informationen die (a) direkt von dem Domain-Namen Registrator oder dem Registrierungsstellenmitarbeiter mittels RFC 3912 Protokoll abgefragt wurden, (b) die anhand des Registry Data Access Protokolls (RFC 7482) ermittelt wurden oder (3) die über eine HTTPS Webseite ermittelt wurden.
Wildcard-Zertifikat	Ein Zertifikat, das ein Sternchen (*) in der äußersten linken Position eines in dem Zertifikat enthaltenen voll qualifizierten Domain-Namens (Fully-Qualified Domain Names) des Subjekts aufweist.

Begriff	Erläuterung
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zentrale Datenablage (Repository)	Eine Online-Datenbank, die öffentliche PKI-Dokumente (z.B. Zertifizierungsrichtlinie, Erklärung zum Zertifizierungsbetrieb, CA-Zertifikate) sowie Zertifikatsstatusinformationen, entweder in Form einer CRL- oder OCSP-Antwort, enthält.
Zentrales Registrierungsmodell	Nach erfolgreicher Registrierung beantragt der Sub-Registrator über die Sub-RA-Webseite das Zertifikat (per Webformular oder Bulk) und erhält dieses bzw. das Schlüsselmaterial für den Endteilnehmer (außer Registrator-Zertifikat) direkt ausgestellt.
Zertifikat	Ein elektronisches Dokument, das eine digitale Signatur verwendet, um einen öffentlichen Schlüssel an eine Identität (z.B. Person, Gerät) zu binden.
Zertifikat einer Stammzertifizierungs-stelle (Root-Zertifikat)	Das selbstsignierte Zertifikat, das von der Stammzertifizierungsstelle (Root-CA) zur Eigenidentifizierung ausgestellt wurde. Ferner soll dieses Zertifikat auch bei der Prüfung (Validierung) ausgestellten Sub-Zertifikate unterstützen.
Zertifikatnehmer	Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die rechtlich durch einen Bezugsvertrag oder Nutzungsbedingungen gebunden ist.
Zertifikatsantrag	Ein in elektronischer oder schriftlicher Form erstellter Antrag, der Daten zu einem Antragsteller enthält.
Zertifikatsdaten	Zertifikatsanträge und damit verbundene Daten (vom Antragsteller oder anderweitig eingeholt), die sich im Besitz der Zertifizierungsstelle (CA) befinden, die der Kontrolle durch die CA unterliegen oder auf die die CA Zugriff hat.
Zertifikatsproblem-bericht	Beschwerde wegen des Verdachts der Gefährdung des Schlüssels, des Zertifikatsmissbrauchs oder hinsichtlich anderer Arten von Betrug, Gefährdung, Missbrauch oder eines Fehlverhaltens im Zusammenhang mit Zertifikaten.
Zertifikatssperrliste (CRL)	Eine regelmäßig aktualisierte, mit Zeitstempel versehene Liste gesperrter (widerrufener) Zertifikate, die von der ausstellenden Zertifizierungsstelle (CA) generiert und digital signiert wird. Die Authority Revocation List (ARL) ist ein Spezialfall der Zertifikatssperrliste (CRL), da sie nur Sub-CA-Zertifikate enthält.
Zertifikatsverwaltungsprozess	Prozesse, Praktiken und Verfahren im Zusammenhang mit der Verwendung von Schlüsseln, Software und Hardware, mit deren Hilfe die Zertifizierungsstelle (CA) Zertifikatsdaten prüft, Zertifikate ausstellt, eine zentrale Datenablage (Repository) unterhält und Zertifikate widerruft/sperrt.
Zertifizierungsrichtlinie (CP)	Ein Regelwerk, das die Verwendungsmöglichkeit eines genannten Zertifikats auf eine bestimmte Gemeinschaft (PKI-Beteiligte) und/oder eine PKI-Implementierung mit gängigen Sicherheitsanforderungen, vorgibt.
Zertifizierungsstelle (CA)	Eine Organisation, die für die Generierung, Ausstellung, die Sperrung und die Verwaltung von Zertifikaten zuständig ist. Die Bezeichnung bezieht sich sowohl auf Stammzertifizierungsstellen (Root-CA) als auch auf untergeordnete Zertifizierungsstellen (Sub-CA).
Zuständigkeitsbereich	Hierarchisch untergeordneter Teilbereich der Master-Domäne, der von einem Sub-Registrator verwaltet wird.
Zuverlässige öffentliche Datenquelle	Ein Authentifizierungsdokument oder eine Datenquelle (z.B. Identitätsdatenbank, Handelsregister), anhand der Subjektidentitätsdaten überprüft werden und die im Allgemeinen von kommerziellen Unternehmen und Behörde (öffentliche Verwaltung) als zuverlässig anerkannt wird und die von einer dritten Partei für einen anderen Zweck als der Zertifikatsausstellung durch den Antragsteller erstellt wurde.

1.6.2 Abkürzungsverzeichnis

Tabelle 5 - Abkürzungsverzeichnis

Überschrift	Definition
ARL	Authority Revocation List
BR	Baseline Requirements
DK	Dual Key
CA	Certification Authority
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
EDV	Elektronische Datenverarbeitung
eIDAS	electronic Identification and Signature
ERP	Enterprise-Resource-Planning
ETSI	European Telecommunications Standards Institute (deutsch: Europäisches Institut für Telekommunikationsnormen)
FQDN	Fully Qualified Domain Name
GRP	Kennzeichner für Gruppen, Funktions-, Rollenzertifikat
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
IPSec	Internet Protocol Security
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)
ISO	International Organization for Standardization
IV	Individual Validation
LB	Leistungsbeschreibung
LDAP	Lightweight Directory Access Protocol
NCP	"Normalized" Certificate Policy
NIC	Network Information Center
n.v.	nicht vorhanden
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
OV	Organizational Validated
OVCP	Organizational Validation” Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudonym
PSE	Personal Security Environment
PTC	Publicly-trusted certificate
RA	Registration Authority
RFC	Requests for Comments
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key
SLA	Service Level Agreement
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SigG	Signaturgesetz
SigV	Signaturverordnung

Überschrift	Definition
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TK	Triple Key
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language

1.6.3 Referenzen

Tabelle 6 - Referenzen

Kürzel	Referenz
[BDSG]	Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66.
[CAB-BR]	Zum jeweiligen Zeitpunkt gültige Version des vom CA/Browser-Forum unter http://www.cabforum.org/documents.html veröffentlichten Dokuments „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“
[EU-RL]	Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 1999/93/EG, EU, 1999
[Moz-2-7]	Mozilla Root Store Policy, Version 2.7, Stand 01.01.2020, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy
[PKCS]	RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“, http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
[RFC6962]	Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013.
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften, Bundesgesetzblatt I 2001, S. 876
[SigV]	Signaturgesetzverordnung, „Verordnung zur elektronischen Signatur“, BGBl. I S. 3074, 21.November 2001
[X.509]	Information technology - Open Systems Interconnection - The Directory:authentication framework, Version 3, ITU, 1997

1.6.4 Konventionen / Vorgaben

Keine Vorgabe.

2 VERÖFFENTLICHUNG UND VERANTWORTLICHKEIT FÜR INFORMATIONEN (REPOSITORIES)

Die eingeschlossenen CAs müssen eine CPS und/oder CP entwickeln, umsetzen, durchsetzen und jährlich anpassen. Die CPS muss im Detail beschreiben, wie die jeweils gültigen Anforderungen, insbesondere die der Baseline Requirements und des Mozilla Root-Programms, umgesetzt werden.

2.1 Informationsspeicher (Repositories)

Jede eingeschlossene CA muss durch den Verzeichnisdienst mindestens einen Zugriff auf die Sperrdaten zur Verfügung stellen.

Die eingeschlossenen CAs können darüber hinaus die Teilnehmerzertifikate im Verzeichnisdienst zugänglich machen. Falls dabei personenbezogene Daten publiziert werden, die dem Datenschutz unterliegen, muss eine Einwilligung der betroffenen Personen vorliegen.

2.2 Veröffentlichung von Zertifikaten und zugehörigen Informationen

Die eingeschlossenen CAs müssen den PKI-Beteiligten folgende Informationen zur Verfügung stellen:

Statusauskünfte

Den PKI-Beteiligten (siehe 1.3) müssen neben den Root- und Cross-Zertifikaten, die ARL, CRL und OCSP-Auskünfte den PKI Beteiligten 7x24h online-zur Verfügung gestellt werden.

CP / CPS

Weiterhin muss die zugehörige Certificate Policy / Certification Practice Statement allen PKI-Beteiligten über einen einfachen Weg mit einer Verfügbarkeit von 7x24h zugänglich machen.

Testwebseiten

Bei Webserver-Zertifikaten müssen die SubCAs Test-Webseiten mit Teilnehmerzertifikaten zur Verfügung stellen, die bis zu einer öffentlichen Root verkettet sind. Es müssen Webseiten mit einem gültigen, einem abgelaufenen und einem gesperrten Zertifikat bereitgestellt werden.

2.3 Zeitpunkt oder Intervall der Veröffentlichung

Root-CA- und Sub-CA-Zertifikate müssen nach ihrer Produktion öffentlich bereitgestellt werden. Die Sperrinformationen für Root-CA- und Sub-CA-Zertifikate müssen im Fall einer Sperrung aktualisiert werden. Die ARL für die Root-CA- und Sub-CA-Zertifikat muss mindestens halbjährlich aktualisiert werden. Werden Cross-Zertifikate verwendet, so muss die ARL alle 31 Tage aktualisiert werden.

Die CP/CPS-Dokumente müssen mindestens einmal im Jahr einem Review unterzogen werden. Bei relevanten Änderungen der im CPS beschriebenen Erklärungen, Maßnahmen oder Prozeduren ist das Dokument zu aktualisieren.

2.4 Zugang zu den Informationsdiensten

Die Informationsdienste unter 2.2 müssen öffentlich und ohne Zugriffsbeschränkung verfügbar sein. Die Informationsdienste müssen vor unbefugter Modifikation geschützt sein.

Der Zugriff aus dem öffentlichen Bereich darf nur als lesender Zugriff erfolgen.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

Keine Vorgabe.

3.1.1 Namensformen

Keine Vorgabe.

3.1.2 Aussagekraft von Namen

Keine Vorgabe.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Es dürfen keine anonyme oder pseudonyme Zertifikatsdaten verwendet werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Vorgabe.

3.1.5 Eindeutigkeit von Namen

Der CN in Root-CA Zertifikaten muss eindeutig sein.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Es liegt in der alleinigen Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Die Zertifizierungsstelle ist nicht verpflichtet, solche Rechte zu überprüfen.

Allein der Zertifikatnehmer ist für solche Überprüfungen verantwortlich. Falls eine Zertifizierungsstelle über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat widerrufen.

3.2 Identitätsprüfungen bei Erstbeauftragung

Das geforderte Prüfniveau ist an jeder Stelle der Vertrauenskette zu gewährleisten. Das Prüfniveau kann in der Vertrauenshierarchie stärker, jedoch in keiner Stufe schwächer werden.

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Der Zertifikatsnehmer muss bei einem Neuauftrag gegenüber der Zertifizierungsstelle in geeigneter Weise nachweisen, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist. Der Besitznachweis ist durch die Methode PKCS#10 erbracht. Diese Anforderung gilt nicht, wenn die Schlüsselerzeugung bei der Zertifizierungsstelle stattfindet.

3.2.2 Prüfung der Organisations- und Domain-Identität

Zertifikatsaufträge für Zertifikate, die ausschließlich Informationen im Feld „countryName“ enthalten, sind nicht zugelassen. Alle Auftragsinformationen sind anhand der nachfolgenden Prüfungen zu verifizieren.

3.2.2.1 Identität

Wenn die Informationen zur Subjektidentität den Namen oder die Anschrift einer Organisation enthalten sollen, MUSS die CA die Identität und Anschrift der Organisation verifizieren und prüfen. Hierzu ist zu überprüfen inwiefern die Anschrift die existierende oder gültige Anschrift des Auftraggebers ist. Die CA MUSS die Identität und Anschrift des Auftraggebers mithilfe der Dokumentation verifizieren, die durch mindestens eine der folgenden Stellen vorgelegt wird oder durch Kommunikation mit solchen Stellen beschafft wird:

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

Die CA KANN dieselbe Dokumentation oder Kommunikation, die in 1 bis 4 oben beschrieben ist, verwenden, um die Identität und die Anschrift des Auftraggebers zu verifizieren.

Alternativ KANN die CA die Anschrift des Auftraggebers (nicht jedoch die Identität des Auftraggebers) verifizieren, indem sie eine Rechnung eines Versorgungsunternehmens, eine Bankabrechnung, eine Kreditkartenabrechnung, ein vom Staat ausgegebenes Steuerdokument oder eine andere Form der Identifizierung heranzieht, deren Zuverlässigkeit die CA feststellt.

3.2.2.2 Firmierung/Handelsname

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

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

3.2.2.3 Überprüfung der Länderkennung

Wenn das Feld „subject:countryName“ existiert, MUSS die CA das zum Subjekt gehörende Land mithilfe einer der folgenden Methoden verifizieren:

a. die Zuweisung des IP-Adressenbereichs durch das Land für (i) die IP-Adresse der Webseite, wie durch den DNS-Eintrag für die Webseite angegeben, oder (ii) die IP-Adresse des Auftraggebers,
b. die ccTLD des beantragten Domain-Namens,
c. Informationen, die vom Domain-Name-Registrar vorgelegt werden, oder
d. eine in Abschnitt 3.2.2.1 identifizierte Methode.

Die CA SOLLTE ein Verfahren implementieren, um Proxy-Server zu überprüfen und damit den Rückgriff auf IP-Adressen zu verhindern, die in anderen Ländern als dem Land, in dem der Auftraggeber tatsächlich ansässig ist, zugewiesen wurden.

3.2.2.4 Überprüfung der Berechtigung oder der Kontrolle über die Domain

Für jeden vollqualifizierten Domain-Namen (FQDN), der in einem Zertifikat aufgeführt ist, MUSS die CA oder ein beauftragter Dritter (Delegated Third Party) bestätigen, dass der Auftraggeber (oder die Muttergesellschaft, die Tochtergesellschaft oder das verbundene Unternehmen des Auftraggebers, zum Zwecke dieses Abschnitts zusammen als „Auftraggeber“ bezeichnet) am Datum der Zertifikatsausstellung entweder der Domain-Name-Registrant ist oder die Kontrolle über den FQDN besitzt, und zwar durch mindestens eine der nachfolgenden Überprüfungen:

3.2.2.4.1 Überprüfung, ob der Auftraggeber der Domain Kontakt ist

Diese Methode ist zum 31.07.2018 abgelaufen und darf nicht mehr zur Überprüfung eingesetzt werden.

Validierungen, die zuvor anhand dieser Methode durchgeführt wurden, dürfen nicht zur Ausgabe neuer Zertifikate eingesetzt werden.

3.2.2.4.2 Kontakt per Email, Fax, SMS, oder Briefpost zum Domain Kontakt

Die CA sendet einen Zufallswert an den Domain-Kontakt per Email, Fax, SMS, oder Brief, der vom Domain Kontakt per Email, Fax, SMS, oder Brief bestätigt werden MUSS. Die Kontaktdaten müssen vom Domain-Name-Registrar abgefragt werden.

Jeder Zufallswert darf nur einmal benutzt werden und nicht älter als 30 Tage sein.

3.2.2.4.3 Telefonischer Kontakt zum Domain Kontakt

Die CA MUSS für einen telefonischen Kontakt die Rufnummer des Domain-Name-Registranten nutzen, die dem Domain-Name-Registrar vorgelegt wurde. In dem Telefonat muss sich die CA vom Domain-Name-Registranten den Zertifikatsantrag für jede FQDN bestätigen lassen.

Diese Validierungs-Methode durfte nur bis zum 31. Mai 2019 angewendet werden. Danach ist diese nicht mehr zulässig. Bereits durchgeführte Prüfungen sind für die Erneuerung von Zertifikaten im Rahmen der definierten Erneuerungsfristen gültig.

3.2.2.4.4 Konstruierte E-Mail zum Domain Kontakt

Die CA MUSS durch die Kommunikation mit dem Administrator der Domain unter Verwendung einer E-Mail-Adresse bestätigen, dass der Auftraggeber die Kontrolle über die Domain hat. Die E-Mail-Adresse ist durch Voranstellen von „admin“, „administrator“, „webmaster“, „hostmaster“ oder „postmaster“, gefolgt vom at-Zeichen („@“), gefolgt vom Domain-Namen zu bilden. Die E-Mail-Nachricht MUSS einen einzigartigen Zufallswert enthalten, der in der Antwortmail des Administrators enthalten sein MUSS.

Jeder Zufallswert darf nur einmal benutzt werden und nicht älter als 30 Tage sein.

3.2.2.4.5 Domainvollmacht

Diese Methode ist zum 31.07.2018 abgelaufen und darf nicht mehr zur Überprüfung eingesetzt werden.

Validierungen, die zuvor anhand dieser Methode durchgeführt wurden, dürfen nicht zur Ausgabe neuer Zertifikate eingesetzt werden.

3.2.2.4.6 Vereinbarte Änderung auf der Webseite

Für jeden im Zertifikat aufgelisteten FQDN MUSS der Auftraggeber die praktische Kontrolle nachweisen, indem er eine vereinbarte Änderung auf einer Webseite vornimmt.

3.2.2.4.7 Änderung im DNS

Die CA muss die Kontrolle des Antragstellers über den FQDN bestätigen. Die Kontrolle wird durch das Vorhandensein eines von der CA während der Beauftragung ausgestellten eindeutigen Zufallswert oder eines eindeutigen Anforderungstokens im DNS-CNAME-, TXT- oder CAA-Datensatz nachgewiesen.

3.2.2.4.8 IP Addresse

Die CA MUSS die Kontrolle des Antragstellers über den FQDN bestätigen. Dies kann vom Antragsteller nachgewiesen werden indem er eine IP-Adresse steuert, die von einer DNS-Suche nach A- oder AAAA-Datensätzen für den FQDN gemäß Abschnitt 3.2.2.5 zurückgegeben wird.

3.2.2.4.9 Testzertifikat

Keine Vorgabe.

3.2.2.4.10 TLS unter Verwendung einer Zufallszahl

Keine Vorgabe.

3.2.2.4.11 Beliebige andere Methode

Diese Methode darf nicht länger verwendet werden.

3.2.2.4.12 Validierung eines Antragstellers als Domain Kontakt

Die CA kann für eine Validierung eines Antragstellers und dessen Kontrolle über den FQDN prüfen inwiefern dieser der Domain Kontakt ist. Diese Methode kann nur dann eingesetzt werden, wenn die CA auch gleichzeitig Domänen-Namen-Registrators ist, oder eine Gesellschaft des Regristrators für den Basis Domain-Namen.

Wurde diese Methode zur Validierung des FQDNs eingesetzt, kann die CA weitere Zertifikate für andere FQDNs ausstellen die mit den Labels des validierten FQDNs enden.

Diese Methode kann zur Validierung von Wildcard Domain Namen eingesetzt werden.

3.2.2.4.13 E-Mail an einen DNS CAA Kontakt

Die CA muss für eine Validierung der Kontrolle des Antragstellers über einen FQDN einen Zufallswert via

E-Mail senden. Der Antragsteller verwertet den Zufallswert und sendet eine entsprechende Rückmeldung. Der Zufallswert muss dabei an einen DNS CAA Email Contact gesendet werden. Hierzu muss das CAA Resource Record Set unter Verwendung des in RFC 6844, Abschnitt 4 (angepasst durch Errata 5065) als Suchalgorithmus verwendet werden.

Jede E-Mail kann dabei die Kontrolle über mehrere FQDNs bestätigen, insofern die jeweilige E-Mail-Adresse ein DNS CAA E-Mail Kontakt für einen zu validierenden Authorization Domain

Namen ist. Dieselbe E-Mail kann an mehrere Empfänger gesendet werden, solange alle Empfänger DNS CAA E-Mail Kontakte für jeden zu validierenden Authorization Domain Namen sind.

Der Zufallswert muss dabei für jede E-Mail neu generiert und einmalig sein. Die E-Mail kann erneut verwendet werden, im Falle das die Empfänger sich nicht geändert haben. Der Zufallswert darf hierzu max. 30 Tage gültig bleiben. Das CPS kann eine kürzere Gültigkeitsdauer definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

Sollte der FQDN über diese Methode validiert worden sein, hat die CA die Möglichkeit weitere Zertifikate für andere FQDNs auszustellen. Diese müssen hierzu mit den Labels des geprüften FQDNs enden.

Diese Methode kann zur Validierung von Wildcard Domain Namen eingesetzt werden.

3.2.2.4.14 E-Mail an einen DNS TXT Kontakt

Die CA muss für eine Validierung eines Antragstellers und dessen Kontrolle über den FQDN prüfen inwiefern dieser ein DNS TXT Record E-Mail Kontakt ist. Hierzu muss eine E-Mail mit Zufallswert an diesen Kontakt gesendet werden. Der DNS TXT Record E-Mail Kontakt muss für den Authorization Domain Namen zuständig sein.

Jede E-Mail kann dabei die Kontrolle über mehrere FQDNs bestätigen, insofern jede E-Mail Adresse ein DNS TXT Record E-Mail Kontakt für den jeweils zu prüfenden Authorization Domain Namen ist. Dieselbe E-Mail kann an mehrere Empfänger versendet werden, insofern alle Empfänger DNS TXT Record E-Mail Kontakte für jeden zu prüfenden Authorization Domain Namen sind.

Der Zufallswert muss dabei für jede E-Mail neu generiert und einmalig sein. Die E-Mail kann erneut verwendet werden, im Falle das die Empfänger sich nicht geändert haben. Der Zufallswert darf hierzu max. 30 Tage gültig bleiben. Das CPS kann eine kürzere Gültigkeitsdauer definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

Sollte der FQDN über diese Methode validiert worden sein, hat die CA die Möglichkeit weitere Zertifikate für andere FQDNs auszustellen. Diese müssen hierzu mit den Labels des geprüfenten FQDNs enden.

Diese Methode kann zur Validierung von Wildcard Domain Namen eingesetzt werden.

3.2.2.4.15 Telefonischer Kontakt mit dem Domain Kontakt

Die CA muss für eine Validierung eines Antragstellers dessen Kontrolle über den FQDN prüfen. Hierzu ruft er telefonisch den Domain Kontakt anhand der benannten Telefonnummer an und überprüft dessen Antwort bzgl. der Zuständigkeit für den Authorization Domain Name (ADN). In jedem Telefonat kann die Kontrolle über mehrere Authorized Domain Names überprüft werden, wobei in diesem Falle der kontaktierte Domain-Kontakt für alle gelisteten ADNs zuständig sein muss.

Sollte ein anderer Mitarbeiter den Anruf annehmen, so kann die CA eine Weiterleitung an den korrekten Domain Kontakt fordern.

Meldet sich nur die Mobilbox des Domain Kontakts, kann die CA eine Nachricht mit einem Zufallswert und den zu validierenden ADNs hinterlassen. Der Zufallswert muss entsprechend durch den Domain Kontakt reflektiert und der CA genannt werden.

Der Zufallswert darf hierzu max. 30 Tage gültig bleiben. Das CPS kann eine kürzere Gültigkeitsdauer definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

Sollte der FQDN über diese Methode validiert worden sein, hat die CA die Möglichkeit weitere Zertifikate für andere FQDNs auszustellen. Diese müssen hierzu mit den Labels des geprüften FQDNs enden.

Diese Methode kann zur Validierung von Wildcard Domain Namen eingesetzt werden.

3.2.2.4.16 Telefonischer Kontakt mit dem DNS TXT Record Telefonkontakt

Die CA muss für eine Validierung eines Antragstellers dessen Kontrolle über den FQDN prüfen. Hierzu ruft er telefonisch den DNS TXT Record Telefonkontakt anhand der benannten Telefonnummer an und überprüft dessen Antwort bzgl. der Zuständigkeit für den Authorization Domain Name (ADN). In jedem Telefonat kann die Kontrolle über mehrere Authorized Domain Names überprüft werden, wobei in diesem Falle der kontaktierte DNS TXT Record Telefonkontakt für alle gelisteten ADNs zuständig sein muss.

Die CA kann nicht weitergeleitet werden, da speziell diese Telefonnummer als Kontakt für die Domain Validierung benannt wurde.

Meldet sich nur die Mobilbox des DNS TXT Record Telefonkontakts, kann die CA eine Nachricht mit einem Zufallswert hinterlassen. Der Zufallswert muss entsprechend durch den Kontakt reflektiert und der CA genannt werden.

Der Zufallswert darf hierzu max. 30 Tage gültig bleiben. Im CPS besteht die Möglichkeit eine kürzere Gültigkeitsdauer zu definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

Sollte der FQDN über diese Methode validiert worden sein, hat die CA die Möglichkeit weitere Zertifikate für andere FQDNs auszustellen. Diese müssen hierzu mit den Labels des geprüften FQDNs enden.

Diese Methode kann zur Validierung von Wildcard Domain Namen eingesetzt werden.

3.2.2.4.17 Telefonischer Kontakt mit DNS CAA Telefonkontakt

Die CA muss für eine Validierung eines Antragstellers dessen Kontrolle über den FQDN prüfen. Hierzu ruft er telefonisch den DNS CAA Telefonkontakt anhand der benannten Telefonnummer an und überprüft dessen Antwort bzgl. der Zuständigkeit für den Authorization Domain Name (ADN). In jedem Telefonat kann die Kontrolle über mehrere Authorized Domain Names überprüft werden, wobei in diesem Falle der kontaktierte DNS CAA Telefonkontakt für alle gelisteten ADNs zuständig sein muss. Zur Ermittlung des CAA Resource Record Sets muss der Suchalgorithmus aus RFC 6844, Abschnitt 4 Anwendung finden.

Die CA kann nicht weitergeleitet werden, da speziell diese Telefonnummer als Kontakt für die Domain Validierung benannt wurde.

Meldet sich nur die Mobilbox des DNS CAA Telefonkontakts, kann die CA eine Nachricht mit einem Zufallswert hinterlassen. Der Zufallswert muss entsprechend durch den Kontakt reflektiert und der CA genannt werden.

Der Zufallswert darf hierzu max. 30 Tage gültig bleiben. Im CPS besteht die Möglichkeit eine kürzere Gültigkeitsdauer zu definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

Sollte der FQDN über diese Methode validiert worden sein, hat die CA die Möglichkeit weitere Zertifikate für andere FQDNs auszustellen. Diese müssen hierzu mit den Labels des geprüften FQDNs enden.

Diese Methode kann zur Validierung von Wildcard Domain Namen eingesetzt werden.

3.2.2.5 Authentifizierung für eine IP Adresse

Für jede, in einem Zertifikat aufgelistete, IP-Adresse muss die CA bestätigen, dass der Antragsteller am Datum der Zertifikatsausstellung die Kontrolle über die IP-Adresse hatte. Hierzu muss die CA einen Prüfprozesse anhand der Methoden in den folgenden Unterkapiteln durchführen.

Nach einer erfolgreichen Prüfung bzw. Validierung der Berechtigung des Antragstellers, kann diese für die Ausgabe von weiteren Zertifikaten genutzt werden. Dies ist jedoch nicht dauerhaft möglich. Es muss vielmehr in allen Fällen eine Prüfung in der vorgegebenen Zeit initiiert werden (siehe Kapitel 4.2.1) bevor ein Zertifikat ausgestellt wird. Zum Zwecke der IP Adress-Validierung umfasst der Begriff Antragsteller die Firma des Antragstellers, ein Tochterunternehmen oder Gesellschaft.

Eine Vorgabe der Baseline Requirements besteht darin, dass die CA eine Tabelle bzw. Protokoll vorhalten muss, welche ab dem 01. August 2019 dokumentiert welche Methode zur jeweiligen IP Adress-Validierung eingesetzt wurde und auf welcher BR-Versionsnummer gearbeitet wurde.

Es sollte berücksichtigt werden, dass IP-Adressen die im Zusammenhang mit diesem Kapitel geprüft werden in Subscriber-Zertifikaten (siehe 7.1.4.2) oder in Sub-CA Zertifikaten gelistet werden können. Dies erfolgt durch die Listung der IP-Adressen in erlaubten Baumstrukturen (permitted Subtrees) im Rahmen der Name Constraints Erweiterung.

CAs müssen nicht IP-Adressen, die in Sub-CAs gelistet sind, prüfen. Konkret handelt es sich um IP-Adressen in ausgenommenen Baumstrukturen (excluded Subtrees) in der Name Constraints Erweiterung vor deren Einbindung in Sub-CA Zertifikate.

3.2.2.5.1 Abgestimmte Änderung an einer Webseite

Eine Methode zur Prüfung der Authorität über eine IP-Adresse ist die Ausführung einer abgestimmten Änderung auf der korrespondierenden Webseite.

Die CA muss die Kontrolle des Antragstellers über die IP-Adresse durch die Bestätigung eines Anforderungstokens oder Zufallswerts in einer Datei oder Webseite bestätigen. Dieser Token oder Zufallswert muss in die Webseite integriert werden. Hierzu ist ein Meta-Tag im „/.well-known/pki-validation“-Verzeichnis oder eines anderen bei der IANA registrierten Pfades zu verwenden. Auf diese Weise wird die Kontrolle über die IP-Adresse geprüft die durch die CA über http/https und einen authorisierten Port erreichbar ist.

Während des Vorgangs darf der Request-Token oder der Zufallswert nicht in dem Request angezeigt werden.

Für den Zufallswert muss die CA einen Prozess implementieren, der die Zufälligkeit des Wertes garantiert und sicherstellt, dass dieser nicht mehrfach für unterschiedliche Zwecke genutzt wird. Die CA muss dabei einen einmaligen Zufallswert für den Zertifikatsantrag verwenden. Der Zufallswert darf a) max. 30 Tage gültig sein oder b) falls der Antragsteller einen Zertifikatsrequest gestellt hat muss die Zeit für die Wiederverwendung von validierten Informationen mit Zertifikatsrelevanz (siehe Kapitel 4.2.1) berücksichtigt werden.

3.2.2.5.2 E-Mail, Fax, SMS, Brief an IP Adresskontakt

Eine zweite Option zur Prüfung der Autorität über eine IP-Adresse ist der Austausch einen Zufallswertes über

E-Mai, Fax, SMS oder Brief an den IP-Adresskontakt. Der Zufallswert muss über E-Mail, Fax, SMS, Brief an den identifizierten IP-Adresskontakt versendet werden.

Der Versand kann an mehr als einen Empfänger stattfinden, insofern die IP-Adressen-Registrierungsstelle die weiteren Personen als Kontakte für die angefragten IP-Adressen identifiziert. Der Antragsteller sendet die Antwort unter Verwendung des Zufallswertes zurück. Jede E-Mail, jedes Fax, jede SMS oder Brief kann die Kontrolle über mehrere IP-Adressen bestätigen. Der Zufallswert sollte einmalig für jede E-Mail, jedes Fax, jede SMS oder jeden Brief sein.

Die CA kann E-Mai/Fax/SMS/Brief unter Verwendung des Zufallswertes erneut versenden, insofern sich der Inhalt und die Empfänger nicht verändert haben.

Der Zufallswert muss hierzu 30 Tage gültig bleiben. Das CPS kann eine kürzere Gültigkeitsdauer definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

3.2.2.5.3 Adressauflösung (Reverse Address Lookup)

Als dritte Möglichkeit zur Validierung der Autorität über eine IP-Adresse, kann die CA eine Adressauflösung durchführen (Reverse Address Lookup). Die Kontrolle des Antragstellers über die IP-Adresse wird dadurch bestätigt, dass der Domain Name welcher mit der IP-Adresse verbunden ist über die Adressauflösung ermittelt werden kann. Der nächste Schritt bildet die Prüfung der Kontrolle über den FQDN mittels einer der Methoden in Kapitel 3.2.2.4.

3.2.2.5.4 Andere Methoden

Die CA kann zur Validierung der IP-Adresse eine beliebige andere Prüfmethode einsetzen, vorausgesetzt die CA erhält einen dokumentierten Nachweis das der Antragsteller die praktische Kontrolle über die IP-Adresse besitzt. Die gewählte Methode muss dabei min. den gleichen Prüflevel wie die zuvor in diesem Kapitel genannten Verfahren nachweisen.

Diese Methode darf nach dem 31. Juli 2019 nicht mehr eingesetzt werden. Bereits angeschlossene Validierungen dürfen für eine erneute Zertifikatsausgabe nach dem 31. Juli 2019 nicht mehr verwendet werden. Zuvor anhand dieser Methode ausgestellte Zertifikate können ohne erneute Prüfung bis zu ihrem natürlichen Ablaufdatum gültig bleiben.

3.2.2.5.5 Telefonischer Kontakt mit IP Adressen-Kontakt

Die CA kann zur Prüfung der Autorität über eine IP-Adresse den IP-Adress-Kontakt telefonisch anrufen. Der Angerufene muss eine entsprechende Antwort bzgl. seines Requests zur Validierung der IP-Adresse geben.

Die CA muss dabei die Telefonnummer anrufen, welche bei der IP-Adressen Registrierungsstelle für den

IP-Adressen-Kontakt angegeben ist. Jeder Anruf muss an eine eindeutige Nummer getätigt werden.

Für den Fall, dass die CA einen Kollegen des Kontaktes erreicht, kann sie um eine Weiterleitung an den korrekten IP-Adressen-Kontakt bitten.

Meldet sich nur die Mobilbox des IP-Adressen-Kontakts, kann die CA eine Nachricht mit einem Zufallswert und die zu prüfenden IP-Adressen hinterlassen. Der enthaltene Zufallswert muss entsprechend durch den Kontakt reflektiert und der CA genannt werden.

Der Zufallswert bleibt hierzu max. 30 Tage gültig. Das CPS kann eine kürzere Gültigkeitsdauer definieren. In diesem Fall muss den Vorgaben des CPS gefolgt werden.

3.2.2.5.6 ACME “http-01” Methode für IP-Adressen

Zur Prüfung der Kontrolle des Antragstellers über eine IP-Adresse kann die dokumentierte Methode „http-01“ in Entwurf 04 der „ACME IP Identifier Validation Extension“, verfügbar unter https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, eingesetzt werden.

3.2.2.5.7 ACME “tls-alpn-01” Methode für IP-Adressen

Zur Prüfung der Kontrolle des Antragstellers über eine IP-Adresse kann die dokumentierte Methode „tls-alpn-01“ in Entwurf 04 der „ACME IP Identifier Validation Extension“, verfügbar unter https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, eingesetzt werden.

3.2.2.6 Überprüfen einer Wildcard Domain

Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur im linken Label des CN oder „subjectAltName“ akzeptiert. Mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro CN oder „subjectAltName“ wird nicht akzeptiert.

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

Die Verwendung von Wildcard-Zeichen ist bei EV-Zertifikaten nicht zulässig.

3.2.2.7 Zuverlässigkeit der Datenquelle

Vor Verwendung einer Datenquelle als zuverlässige Datenquelle MUSS die Quelle im Hinblick auf ihre Zuverlässigkeit, Genauigkeit und Änderungs- oder Fälschungssicherheit beurteilt werden. Es muss folgendes berücksichtigt werden:

1. dass Alter der vorgelegten Informationen,
2. die Häufigkeit der Aktualisierungen der Informationsquelle,
3. der Datenanbieter und der Zweck der Datenerfassung,
4. die Verfügbarkeit der Daten und
5. die Integrität der Daten.

Datenbanken, die von der CA, ihrem Eigentümer oder ihren verbundenen Unternehmen gepflegt werden, gelten nicht als zuverlässige Datenquelle, wenn der Hauptzweck der Datenbank darin liegt, Informationen zur Erfüllung der Validierungsanforderungen unter diesem Abschnitt 3.2 zu sammeln.

3.2.2.8 CAA Records

Beim Ausstellen von Zertifikaten muss die Zertifizierungsstelle die CAA-Records für jeden dNSName im subjectAltName-Feld prüfen, wie in RFC 6844 (Errata 5065) beschrieben. Dies umfasst auch die Verarbeitung von issue, issuewild oder iodef Property Tags, wie in RFC 6844 definiert (insofern zutreffend).

Die CA muss dabei ein gesetztes „critical flag“ berücksichtigen und darf keine Zertifikate ausgeben, falls ein unbekanntes Feld (Property) als kritisch gekennzeichnet wurde. Die CA kann ein nicht leeres CAA Resource Record Set ohne Issue Property Tags (im Falle Wildcard Domain Name ohne Issuewild Property Tags) zur Ausstellung verwenden, es sei denn ein anderes CAA Resource Record Set steht dem entgegen.

Die Prüfung der CAA Records kann entfallen bei Zertifikaten:

- für die bereits ein Certificate Transparency-Pre-Zertifikat ausgestellt wurde, das in mindestens zwei CT-Logservern abgelegt ist und für das CAA Records geprüft wurden.
- die von einer technisch beschränkten Sub-CA entsprechend Kapitel 7.1.5 ausgestellt werden.
- die von einem Affiliate der ausstellenden CA beantragt wurden.

CAs müssen potentielle Probleme, die durch einen CAA Record ausgelöst wurden, ausreichend dokumentieren und ggf. für Reports bereitstellen.

3.2.3 Authentifizierung einer natürlichen Person

Bei der Ausstellung von Zertifikaten für natürliche Personen müssen geeignete Verfahren zur Prüfung der Identität herangezogen werden, z.B.:

- Personalausweis
- Reisepass mit amtlicher Meldebescheinigung

Prüfniveau Niedrig

Keine Vorgabe.

Prüfniveau Medium

Für die Identifizierung einer natürlichen Person, die Services mit Prüfniveau Medium beauftragt, gelten die folgenden Validierungsverfahren:

- Feststellung der Existenz der natürlichen Person anhand von nachprüfbaren Identifikationsmerkmalen

Um nachprüfbare Identifikationsmerkmale zu verifizieren KANN die CA oder RA auf einen von Telekom Security anerkannten Identitätsprüfungsservice oder eine Identitätsprüfungsdatenbank oder die von staatlicher Stelle oder Behörde ausgestellten Ausweisdokumente zurückgreifen.

Prüfniveau Hoch

Für die Identifizierung einer natürlichen Person, die Services mit Prüfniveau Hoch beauftragt, gelten die folgenden Validierungsverfahren:

- Prüfniveau Medium ist zu erfüllen
- Persönliche Vorsprache mit einem amtlich ausgestellten Ausweisdokuments mit Lichtbild, bei einer CA oder RA.

3.2.4 Nicht verifizierte Teilnehmerinformationen

Keine Vorgabe.

3.2.5 Überprüfung der Berechtigung

Die Autorisierung einer natürlichen Person als handlungsberechtigt im Namen einer Organisation oder natürlichen Person muss durch ein geeignetes Verfahren erfolgen.

3.2.6 Kriterien für Interoperabilität oder Zertifizierung

Es sind alle Cross-Zertifikate zu veröffentlichen, die von einer CA ausgestellt wurden.

3.3 Identitätsprüfung und Authentifizierung bei einer Schlüsselerneuerung

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Zur Zertifikatserneuerung einer untergeordneten Zertifizierungsstelle (Sub-CA) müssen die „Identitätsprüfungen bei Erstbeauftragung“ (siehe Kapitel 3.2) durchlaufen werden.

3.3.2 Identitätsprüfung bei Schlüsselerneuerung nach Zertifikatssperrung

Die Schlüsselerneuerung eines gesperrten Zertifikats ist nicht möglich.

3.4 Identifizierung und Authentifizierung bei Sperranträgen

Nur zur Sperrung autorisierte Personen und Institutionen können die Sperrung eines Zertifikates beauftragen.

Die Authentisierung einer Sperrung hat in geeigneter Art und Weise zu erfolgen. Es wird empfohlen, ein Sperrpasswort zu verwenden, das im Rahmen der Zertifikatsbeauftragung bzw. Auslieferung festgelegt und sicher an den Zertifikatsnehmer übermittelt wird.

Die zur Sperrung zu verwendenden Telefonnummern, Faxnummern, Webseiten oder Adressen sind zu veröffentlichen.

4 BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

Dieses Kapitel setzt sich mit betrieblichen Anforderungen im Lebenszyklus von Zertifikaten auseinander.

4.1 Zertifikatsbeauftragung

In den Unterkapiteln werden Anforderungen an den Zertifikatsbeauftragungsprozess definiert. Der Zertifikatsbeauftragungsprozess findet in der Regel in der Registrierungsstelle statt.

4.1.1 Wer kann ein Zertifikat beauftragen?

Die Root-CAs oder CA, die inkludiert werden sollen, müssen ihren Antragsprozess inklusive der Schlüsselgenerierung, der Antragsbearbeitung in der RA und der Weiterleitung an die CA im CPS darlegen. Weiterhin muss der Auftraggeber verpflichtet werden, dass dieser aktuelle und korrekte Informationen in den Beauftragungsprozess einbringt.

Eine Sub-CA muss eine interne Datenbank betreiben, die alle vorherigen gesperrten Zertifikate oder Zertifikatsauftragsvorgänge, die aus Sicherheitsgründen zurückgewiesen wurden, beinhaltet. Diese Datenbank soll im Antragsprozess zur Verhinderung von Missbrauch verwendet werden.

4.1.2 Beauftragungsprozess und Zuständigkeiten

Bevor ein Zertifikat erzeugt werden kann, müssen im Registrierungsprozess mindestens die folgenden Aktivitäten abgeschlossen sein

- Abschließen des Vertrages oder CA-internen Vereinbarung
- Vorlage des Zertifikatsauftrags unter Verwendung der von der Zertifizierungsstelle vorgegebenen Mechanismen (z.B. signierter Online Auftrag im Format PKCS#10) und dessen syntaktische/semantische Prüfung,
- ggf. Vorlage weiterer Dokumente des Auftraggebers zur Autorisierung und Identifizierung gemäß dem Prüfniveau für Organisationen oder natürliche Personen,
- Nachweis des Besitzes des privaten Schlüssels gemäß Kapitel 3.2.1,
- vollständige positive Überprüfung der Auftragsdaten durch den Bearbeiter i.d.R. die Registrierungsstelle,
- Archivierung der Auftragsdaten,
- Autorisierung durch das Management.

Der Zertifikatsauftrag muss eine Bestätigung erhalten, dass die Daten im Zertifikatsauftrag wahrheitsgemäß sind. Diese Bestätigung muss vom Auftraggeber selbst oder von einem Bevollmächtigen erfolgen.

Die Root-CA muss vom Auftragsgeber einen Zertifikatsauftrag und Zustimmung zu den vertraglichen Vereinbarungen oder den Benutzungshinweisen oder gleichwertigen vertraglichen Unterlagen erhalten, bevor ein Zertifikat erzeugt werden kann.

4.2 Bearbeitung des Zertifikatsauftrags

Diese Kapitel befasst sich mit den Anforderungen an die Bearbeitung eines Zertifikatsauftrages.

4.2.1 Durchführung der Identifikation und Authentifizierung

Der Auftraggeber muss alle Informationen, die für eine Zertifikatserstellung benötigt werden und/oder in diesem CP gefordert werden, bereitstellen. Wenn nicht alle Angaben enthalten sind, muss die Root-CA diese Angaben vom Auftraggeber nachfordern oder die Daten von einer vertrauenswürdigen und unabhängigen Datenquelle nach Bestätigung durch den Auftraggeber beziehen und verwenden.

Für die Validierung von Aufträgen dürfen nur Daten verwendet werden, die max. 825 Tage vor der Ausstellung des Zertifikates erstellt wurden. Es werden keine vorhergehenden Aufträge zur Auftragsbearbeitung herangezogen.

4.2.2 Annahme oder Abweisung von Zertifikatsaufträgen

CAs dürfen keine Zertifikate ausgeben, welche interne Namen beinhalten, siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**.

4.2.3 Bearbeitungsdauer

Das CPS sollte eine Aussage zur zu erwartenden Bearbeitungsdauer machen, wenn vertraglich keine Verarbeitungsdauer festgelegt ist.

4.3 Ausstellung von Zertifikaten

Bei erfolgreicher Prüfung wird das Zertifikat erzeugt

4.3.1 CA-Tätigkeiten während der Ausstellung von Zertifikaten

Alle Tätigkeiten während der Ausstellung von Root- und Sub-CA-Zertifikaten müssen vorher festgelegten Abläufen (Key Ceremony) unterliegen und protokolliert werden. Für Root-CA-Zertifikate müssen Zeugen z.B. externer Auditor hinzugezogen werden.

4.3.2 Benachrichtigung des Zertifikatsauftraggebers über die Ausstellung von Zertifikaten

Die CA muss den Auftraggeber nach erfolgter Zertifikatserstellung informieren.

4.4 Zertifikatsannahme

Der Auftraggeber nimmt das erzeugte Zertifikat an. Im Falle von Zertifikaten einer Root-CA- oder Sub-CA sollte eine explizite Erklärung der Annahme erfolgen.

4.4.1 Annahme durch den Antragssteller

Die CA sollte eine Annahmebestätigung durch den Auftraggeber innerhalb einer bestimmten Frist verlangen. Die Art der Annahme ist im CPS darzustellen.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die Zertifikate, die durch die Root-CA erzeugt werden, müssen veröffentlicht werden. Dies muss über öffentlich zugängliche Medien erfolgen z.B. Webseite.

4.4.3 Benachrichtigung weiterer Instanzen durch die CA

Keine Vorgabe.

4.5 Verwendung von Schlüsselpaar und Zertifikat

Die im Rahmen dieses CP ausgestellten Zertifikate werden ausschließlich für Zertifizierungsstellen ausgestellt.

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsauftraggeber

Die CA muss Regelungen für die Speicherung und Nutzung des privaten Schlüssels und des Zertifikates durch den Zertifikatsauftraggeber festlegen. Der Einsatz der Zertifikate darf nur in einer Zertifizierungsstelle erfolgen. Der Zertifikatsbesitzer muss insbesondere auf eventuelle Konsequenzen bei Fehlverhalten wie z.B. eine umgehende Sperrung hingewiesen werden.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Relying Parties

Die CA muss Regelungen und Hinweise zur Nutzung der Zertifikate und öffentlichen Schlüssel für potentielle Nutzer z.B. Softwareherstellern erstellen und öffentlich zugänglich machen.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Für Zertifikate, die von der Root-CA zertifiziert werden, sollte eine Zertifikatserneuerung nicht durchgeführt werden.

4.6.1 Bedingungen für eine Zertifikatserneuerung

Es müssen die Regelungen und Fristen der Erstbeauftragung eingehalten werden, dies gilt insbesondere für die Aktualität der vorliegenden Validierungen. Weiterhin müssen die Regelungen der zum Bearbeitungszeitpunkt gültigen Version dieser CP berücksichtigt werden.

Für kompromittierte Schlüssel darf keine Zertifikatserneuerung durchgeführt werden.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Es muss sichergestellt werden, dass die Zertifikatserneuerung nur von einer autorisierten Person beauftragt werden kann.

4.6.3 Ablauf der Zertifikatserneuerung

Die Zertifikatserneuerung MUSS in einer bestimmten Frist erfolgen, dies ist im CPS festzulegen.

4.6.4 Benachrichtigung des Zertifikatsauftraggebers

Keine Vorgabe.

4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.3

4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

Beim Re-Key wird ein neues Schlüsselpaar für ein bestehendes Zertifikat verwendet. Es müssen alle Anforderungen eingehalten und die jeweiligen Bestimmungen im CPS beschrieben werden.

4.7.1 Bedingungen für eine Schlüsselerneuerung

Es müssen die Regelungen und Fristen der Erstbeauftragung eingehalten werden, dies gilt insbesondere für die Aktualität der vorliegenden Validierungen. Weiterhin müssen die Regelungen der zum Bearbeitungszeitpunkt gültigen Version dieser CP berücksichtigt werden.

4.7.2 Wer darf eine Zertifizierung eines neuen öffentlichen Schlüssels beauftragen?

Es muss sichergestellt werden, dass die Schlüsselerneuerung nur von einer autorisierten Person beauftragt werden kann.

4.7.3 Ablauf einer Schlüsselerneuerung

Keine Vorgabe.

4.7.4 Benachrichtigung eines Zertifikatsauftraggebers über das neue Zertifikat

Keine Vorgabe.

4.7.5 Annahme eines neuen Zertifikates

Es gilt Kapitel 4.4.

4.7.6 Veröffentlichung des neuen Zertifikates durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.7.7 Benachrichtigung weiterer Instanzen über eine Schlüsselerneuerung.

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.8 Änderung von Zertifikatsdaten

Ändern sich Zertifikatsdaten während der Zertifikatslaufzeit, so muss geprüft werden, ob das Zertifikat noch den Anforderungen entspricht bzw. ob der Auftraggeber noch alle Vollmachten und Nutzungsrechte innehat. Ist das nicht der Fall, so muss das Zertifikat gesperrt werden.

In diesem Fall muss ein neuer Zertifikatsauftrag mit aktualisierten Daten gestellt werden.

Bei Anpassung von Daten gelten die gleichen Regeln, wie bei der Zertifikatserneuerung.

4.8.1 Bedingungen für die Änderung von Zertifikatsdaten

Keine Vorgabe.

4.8.2 Wer darf eine Änderung der Zertifikatsdaten beauftragen?

Keine Vorgabe.

4.8.3 Ablauf einer Änderung eines Zertifikats

Keine Vorgabe.

4.8.4 Benachrichtigung eines Zertifikatsauftraggebers über Ausgabe eines neuen Zertifikats

Keine Vorgabe.

4.8.5 Annahme des geänderten Zertifikats

Keine Vorgabe.

4.8.6 Veröffentlichung des Zertifikates durch die CA

Keine Vorgabe.

4.8.7 Benachrichtigung weiterer Instanzen über das geänderte Zertifikat

Keine Vorgabe.

4.9 Zertifikatssperrung und Suspendierung

Die Sperrung von Zertifikaten, die durch die Root-CA erstellt wurden, sind von besonderer Kritikalität und müssen meist unter Beteiligung der akkreditierten Zertifizierungsstelle durchgeführt werden.

Die Regeln zum Sperren von Zertifikaten müssen im CPS beschrieben werden. Eine Suspendierung darf für Root-CA und Sub-CA-Zertifikat nicht durchgeführt werden.

4.9.1 Sperrgründe

4.9.1.1 Gründe für die Sperrung eines EE-Zertifikats (Subscriber-Zertifikat)

Eine Sub-CA muss ein Endteilnehmer-Zertifikat (nicht S/MIME) innerhalb von 24 Stunden sperren, wenn einer oder mehrere der nachfolgend genannten Gründe vorliegen:

1. Der Zertifikatsinhaber fordert schriftlich an, dass die CA das Zertifikat sperrt.
2. Der Zertifikatsinhaber benachrichtigt die CA, dass die ursprüngliche Zertifikatanforderung nicht autorisiert wurde und keine rückwirkende Genehmigung erteilt.
3. Die CA erhält den Nachweis, dass der private Schlüssel des Zertifikatsinhabers kompromittiert wurde.
4. Die CA erhält den Nachweis, dass der Validierung der Domainautorisierung oder -kontrolle für einen FQDN oder eine IP-Adresse im Zertifikat nicht vertraut werden sollte.

Eine Sub-CA muss ein Endteilnehmer-Zertifikat innerhalb von fünf (5) Tagen sperren, wenn einer oder mehrere der nachfolgend genannten Gründe vorliegen:

1. Das Zertifikat entspricht nicht mehr den Anforderungen der Abschnitte 6.1.5 und 6.1.6. der Baseline Requirements.
2. Die Sub-CA erhält den Nachweis, dass das Zertifikat missbräuchlich verwendet wurde.

3. Der Sub-CA wird mitgeteilt, dass ein Zertifikatteilnehmer gegen eine oder mehrere wesentliche Vertragsvereinbarungen verstoßen hat.
4. Die Sub-CA wird über Umstände informiert, die darauf hindeuten, dass die Verwendung eines FQDN oder einer IP-Adresse im Zertifikat nicht mehr gesetzlich zulässig ist.
5. Die Sub-CA wird informiert, dass ein Wildcard-Zertifikat zur Authentifizierung eines betrügerisch irreführenden sub-FQDN verwendet wurde.
6. Die Sub-CA wird auf eine wesentliche Änderung der im Zertifikat enthaltenen Informationen hingewiesen.
7. Die Sub-CA wird darauf hingewiesen, dass das Zertifikat nicht in Übereinstimmung mit der CP bzw. CPS der CA ausgestellt wurde.
8. Die Sub-CA stellt fest oder wird darauf hingewiesen, dass die im Zertifikat enthaltenen Informationen nicht korrekt sind.
9. Das Recht der Sub-CA zur Ausstellung von Zertifikaten gemäß den Baseline Requirements erlischt oder wird widerrufen oder gekündigt, es sei denn, die CA hat Vorkehrungen getroffen, um das CRL / OCSP-Repository weiterhin zu verwalten.
10. Der Widerruf ist in der CP und / oder CPS der Sub-CA vorgeschrieben.
11. Die Sub-CA wird darauf aufmerksam gemacht, dass es Methoden gibt, die den privaten Schlüssel des Zertifikatinhabers gefährden oder die Berechnung des privaten Schlüssels aus dem öffentlichen Schlüssel ermöglichen, bzw. dass es eindeutige Beweise dafür gibt, dass die für die Generierung des privaten Schlüssels verwendete Methode mangelhaft war.

Von einer Sub-CA ausgestellte S/MIME-Zertifikate müssen gesperrt werden, wenn einer oder mehrere der nachfolgend genannten Gründe vorliegen:

1. Der Zertifikatsinhaber benachrichtigt die Sub-CA, dass die ursprüngliche Zertifikatanforderung nicht autorisiert wurde und keine rückwirkende Genehmigung erteilt.
2. Die Sub-CA erhält den Nachweis, dass der private Schlüssel des Zertifikatsinhabers kompromittiert wurde.
3. Die Sub-CA erhält den Nachweis, dass das Zertifikat missbräuchlich verwendet wurde.
4. Der Sub-CA wird mitgeteilt, dass ein Zertifikatteilnehmer gegen eine oder mehrere wesentliche Vertragsvereinbarungen verstoßen hat.
5. Die Sub-CA erhält Kenntnis davon, dass die in dem Zertifikat benannte E-Mail-Adresse rechtlich nicht länger genutzt werden darf.
6. Die Sub-CA erhält Kenntnis davon, dass sich zentrale Informationen im Zertifikat geändert haben.
7. Die Sub-CA wird darauf hingewiesen, dass das Zertifikat nicht in Übereinstimmung mit der CP bzw. CPS der Sub-CA ausgestellt wurde.
8. Die Sub-CA stellt fest oder wird darauf hingewiesen, dass die im Zertifikat enthaltenen Informationen nicht korrekt sind.
9. Die Sub-CA stellt den Betrieb ein und hat keine Regelungen getroffen, dass im Falle einer Betriebseinstellung der Sperrsupport durch eine andere CA weitergeführt wird.
10. Die Sub-CA hat den Verdacht, dass der eigene private Schlüssel kompromittiert wurde.
11. Der Widerruf ist in der CP und / oder CPS der Sub-CA vorgeschrieben.
12. Das Zertifikat wurde nicht in Übereinstimmung mit der zum Zeitpunkt der Ausstellung gültigen Mozilla Root Store Policy ausgestellt.

4.9.1.2 Gründe für die Sperrung eines Sub-CA Zertifikats

Die Herausgeber-CA muss ein Sub-CA-Zertifikat innerhalb von sieben (7) Tagen sperren, wenn einer oder mehrere der nachfolgend genannten Gründe vorliegen:

1. Die Sub-CA stellt schriftlich einen Sperrauftrag.
2. Die Sub-CA weist die herausgebende CA darauf hin, dass der ursprüngliche Zertifikatsrequest nicht autorisiert war und auch nicht rückwirkend autorisiert werden soll.
3. Der Herausgeber-CA liegen Beweise vor, dass der private Schlüssel der Sub-CA kompromittiert wurde oder nicht mehr den Anforderungen in Kapitel 6.1.5 und Kapitel 6.1.6 entspricht.
4. Der Herausgeber CA liegen Beweise vor, dass das Zertifikat missbräuchlich eingesetzt wurde.
5. Die Herausgeber-CA erhält Kenntnis davon, dass das Zertifikat nicht regelkonform herausgegeben wurde oder die Sub-CA nicht regelkonform arbeitet, wie es in diesem Dokument oder der anzuwendenden CP und CPS beschrieben ist.
6. Die Herausgeber-CA entscheidet, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist.
7. Die Herausgeber-CA oder die Sub-CA stellen den Betrieb ein und haben keine Regelungen getroffen, dass im Falle einer Betriebseinstellung der Sperrsupport durch eine andere CA weitergeführt wird.
8. Der Nachweis der CA-Browserforum-Konformität der Herausgeber-CA oder Sub-CA hat seine Gültigkeit verloren. Ein Sperrgebot gilt nicht, wenn die Herausgeber-CA Vorsorge getroffen hat, dass die CRL und der OCSP-Dienst weiter gepflegt und bereitgestellt werden.
9. Die Herausgeber-CA hat den Verdacht, dass der eigene private Schlüssel kompromittiert wurde.
10. Die CP oder CPS der herausgebenden CA sieht eine Sperrung vor.
11. Gesetzliche Vorschriften oder richterliche Urteile oder eine Weisung einer aufsichtsführenden Behörde liegen vor.

4.9.2 Wer kann eine Sperrung beauftragen?

Folgenden Personen und Institutionen MÜSSEN eine Sperrung einleiten können:

- der Zertifikatsauftraggeber oder eine andere autorisierte Person,
- die Zertifizierungsstelle aus den im vorherigen Abschnitt genannten Gründen.

Bei einer Meldung durch einen Dritten, der einen Mangel oder eine Abweichung gegenüber den genannten Standards erkennt, muss die Root-CA nach Prüfung des Sachverhalts eine Sperrung einleiten.

4.9.3 Ablauf einer Sperrung

Die Root-CAs müssen Sperrungsmöglichkeiten für die in 4.9.2 benannten Personen über gängige Kommunikationswege 7x24h bereitstellen und auf Problemreports reagieren. Der Prozess der Sperrung muss im CPS ausführlich beschrieben werden.

Weiterhin müssen die CAs Personen, die einen Zertifikatsmissbrauch, eine Schlüsselkompromittierung, Betrug oder ähnliche Sachverhalte melden wollen, eine verständliche Anweisung verfügbar machen, wie dies durchzuführen ist.

Die Informationen müssen online zugänglich sein, zusätzlich muss dies in Kapitel 1.5.2 des CPS beschrieben werden.

4.9.4 Fristen für einen Sperrauftrag

Nicht anwendbar.

4.9.5 Fristen für die Verarbeitung durch die Zertifizierungsstelle

Es ist innerhalb von 24 h nach Eingang einer Problemmeldung ein erster Bericht des Sachverhalts und der Analyseergebnisse zu erstellen und dem Zertifikatsnehmer sowie der Person, die das Problem gemeldet hat, eine Rückmeldung zu geben.

Nach Ansicht der Fakten und Umgebungsparameter wird die Zertifizierungsstelle mit dem Zertifikatsnehmer

oder der meldenden Person die Analyseergebnisse besprechen und entscheiden inwiefern eine Zertifikatssperrung notwendig wird. In diesem Zusammenhang wird das Datum der Sperrung festgelegt. Der Zeitraum zwischen Erhalt des Zertifikatsproblemreports bzw. Sperrwunsches bis zur veröffentlichten Sperrung darf die in Kapitel 4.9.1 geforderten Fristen für eine Sperrung nicht überschreiten. Bei der Festlegung des Sperrdatums sind folgende Punkte zu berücksichtigen:

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

Im Zuge einer Sperrung ist durch beteiligte Intermediate CAs innerhalb einer Woche ein Incidentreport zu erstellen und an die Root-CA zu übermitteln. Diese prüft den Report entsprechend.

4.9.6 Methoden zur Prüfung von Sperrinformationen durch Relying Parties

Sperrinformationen müssen in standardisierter Form z.B. ARL oder OCSP bereitgestellt werden, so dass Prüfungen mit standardkonformen Anwendungen durchgeführt werden können.

Die verwendeten Mechanismen müssen in der CPS beschrieben werden.

4.9.7 Frequenz der Veröffentlichung von Sperrinformationen

Die Sperrinformationen der Root-CA MÜSSEN nach einer Sperrung oder mindestens alle 6 Monate aktualisiert und öffentlich zur Verfügung gestellt werden. Bei der Nutzung von Cross-Zertifikaten muss eine Aktualisierung alle 31 Tage erfolgen.

Ein Eintrag darf nicht aus der CRL entfernt werden, bis er auf einer regelmäßig geplanten CRL erscheint, die nach Ablauf der Gültigkeitsdauer des Revoked-Zertifikats ausgestellt wird.

4.9.8 Maximale Latenzzeit von Sperrlisten

Die Sperrliste ARL darf nicht später als der „next update“-Eintrag eingestellt werden.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Sperrinformationen müssen für die Zertifikatsnutzer online, mit einem standard-konformen Verfahren bereitgestellt werden. Es müssen alle von dieser Zertifizierungsstelle gesperrten CA-Zertifikate enthalten sein.

Sowohl die Sperrlisten, als auch OSCP müssen 7x24h bereitgestellt werden.

Die OCSP-Antworten müssen den Vorgaben des RFC 6960 entsprechen.

4.9.10 Anforderungen an Online Überprüfungsverfahren

Die Root-CA muss die OCSP-Abfrage mit der GET-Methode unterstützen, wie in RFC 6960 und/oder RFC 5019 beschrieben. Die Root-CA muss die OCSP-Datenbank mindestens alle zwölf (12) Monate oder innerhalb von vierundzwanzig (24) Stunden nach einer Sperrung aktualisieren.

Bei Ausstellung von Subscriber-Zertifikaten soll die CA die OCSP-Informationen min. alle vier (4) Tage aktualisieren. OCSP-Antworten dürfen maximal eine Gültigkeit von 10 Tagen haben und werden danach ungültig.

Der OCSP-Responder darf bei einem Zertifikat, was nicht durch die CA ausgestellt wurde, oder einer Zertifikatsseriennummer im Status „unused“ keinen „good“-Status zurückgeben. Der OCSP-Responder sollte auf solche Anfragen gemonitort werden.

Der OCSP-Responder kann Antworten zu Zertifikatsseriennummern im Status „reserved“ geben, in der Form als ob ein korrespondierendes Zertifikat zu dem Pre-Zertifikat existiert. Die Zertifikatsstatus „assinged“, „reserved“ und „unused“ sollten den Vorgaben der [RFC 6962] entsprechen.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine Vorgabe.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Bei einer Kompromittierung eines privaten Schlüssels MUSS das entsprechende Zertifikat innerhalb von 24 Stunden nach Bekanntgabe gesperrt werden und der Schlüssel darf nicht mehr verwendet werden.

4.9.13 Suspendierung von Zertifikaten

Ein CA-Zertifikat darf NICHT suspendiert werden.

4.9.14 Wer kann eine Suspendierung beantragen?

Nicht anwendbar.

4.9.15 Ablauf einer Suspendierung

Nicht anwendbar.

4.9.16 Begrenzung der Suspendierungsperiode

Nicht anwendbar.

4.10 Statusauskunftsdienste für Zertifikate

Für CA-Zertifikate KANN ein OCSP-Dienst zur Verfügung gestellt werden. Eine Sperrliste ARL muss bereitgestellt werden.

4.10.1 Betriebliche Vorgaben

Die Einträge in der ARL dürfen erst herausgenommen werden, wenn das Zertifikat in mindestens einer nach dem Gültigkeitsende des Zertifikats ausgestellten Sperrliste enthalten ist.

4.10.2 Verfügbarkeit

Der Statusauskunftsdienst muss 7x24h zur Verfügung zu stehen. Es müssen ausreichende Kapazitäten zur Verfügung gestellt werden, so dass die Antwortzeit unter normalen Betriebsbedingungen 10 sec nicht überschreitet.

Bei einem Zertifikatsbeschwerdereport ist eine Möglichkeit bereitzustellen diesen innerhalb kurzer Zeit an eine rechtliche Stelle zu melden oder direkt ein Zertifikat zu sperren, zu welchem die Beschwerde eingegangen ist.

4.10.3 Optionale Merkmale

Keine Vorgabe.

4.11 Kündigung durch den Zertifikatsauftraggeber

Bei einer Kündigung des Vertrages oder Beendigung der internen Vereinbarung durch den Auftraggeber muss das Zertifikat gesperrt werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

Schlüsselhinterlegung und Wiederherstellung darf nur mit ausdrücklicher Genehmigung des Zertifikatsauftrages durchgeführt werden.

4.12.1 Richtlinien für Schlüsselhinterlegung und -wiederherstellung

Keine weiteren Anforderungen.

4.12.2 Sitzungsschlüsselkapselung und Richtlinien für die Wiederherstellung

Keine weiteren Anforderungen.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE MAßNAHMEN

Die eingeschlossenen CAs müssen vor Betriebsaufnahme jeweils ein umfangreiches Sicherheitskonzept entwickeln, einführen und aufrechterhalten, dass die folgenden Anforderungen erfüllt:

- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Zertifikatsdaten und des Zertifikatsmanagements-Prozesses.
- Schutz gegen mögliche Bedrohungen und Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses.
- Schutz gegen unautorisierten oder ungerechtfertigten Zugriff, Nutzung, Veröffentlichung, Auswechselung oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses.
- Schutz gegen Verlust oder mutwillige Zerstörung von Zertifikatsdaten oder Manipulationen im Zertifikatsmanagement-Prozess.
- Erhaltung der Einhaltung von gesetzlich geforderten Sicherheitsanforderungen (z.B. Vertrauensdienstegesetz).

Das Sicherheitskonzept muss administrative, organisatorische, technische und infrastrukturelle Maßnahmen enthalten, die der Sensibilität der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses angemessen sind. Das Sicherheitskonzept muss den aktuellen Stand der Technik und die Kosten bestimmter Maßnahmen berücksichtigen und ein angemessenes Sicherheitsniveau für die Schäden, die entstehen könnten und den Schutzbedarf der Daten, die geschützt werden sollen.

Das Sicherheitskonzept muss eine jährliche Risikoanalyse beinhalten, die die vorhersehbaren internen und externen Bedrohungen identifiziert, die zu einem unautorisierten Zugriff, Veröffentlichung, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können. Die Risikoanalyse muss die Wahrscheinlichkeiten und den potentiellen Schaden dieser Bedrohungen betrachten. Weiterhin muss die Sensibilität der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses berücksichtigt werden.

Das Sicherheitskonzept soll Tools und Produkte berücksichtigen, die bei der Erreichung eines angemessenen Sicherheitsniveaus unterstützen.

Das Sicherheitskonzept für den Zertifikatsmanagement-Prozess muss insbesondere folgende Aspekte beinhalten:

- Physikalische Sicherheit und umweltbezogene Maßnahmen.
- Systemintegritätsmaßnahmen, Konfigurationsmanagement, Erhaltung der Integrität von vertrauenswürdigem Code, Malware-Erkennung und Vorsichtsmaßnahmen.
- Netzwerksicherheit and Firewallmanagement, das Port-Beschränkungen und IP-Adressfilterung beinhaltet.
- Benutzermanagement, eine eigene Vergabe von vertrauenswürdigen Rollen, Ausbildung, Sensibilisierung und Fortbildung.
- Logische Zugriffskontrolle, Aktivitätsprotokollierung and sogenannte „inactivity time-outs“ um persönliche Verantwortlichkeit zu ermöglichen.

5.1 Trust Center Sicherheitsmaßnahmen (Physikalische Kontrollen)

Die eingeschlossenen CAs müssen die Maßnahmen beschreiben, die zum Schutz der Infrastruktur ergriffen werden.

5.1.1 Standort und bauliche Maßnahmen

Die eingeschlossenen CAs müssen die Standorte und die technischen und baulichen Maßnahmen insbesondere erforderliche Hochsicherheitszonen des CA-Betriebes beschreiben.

5.1.2 Physikalischer Zutritt

Es soll die Zutrittskontrolle der CA beschrieben werden. Dabei SOLLEN folgende Anforderungen berücksichtigt werden:

- Es sollen nur Zutrittsberechtigungen erteilt werden, die betrieblich notwendig sind.
- Diese Berechtigung sollten zeitlich begrenzt sein und regelmäßig überprüft werden.
- Der Zutritt für Gäste sollte nur im Ausnahmefall nach konkreter Prüfung der Notwendigkeit erteilt werden.
- Die Berechtigungserteilung darf nicht durch einen Mitarbeiter alleine autorisiert werden.
- Berechtigungsvergaben und Zutritte müssen protokolliert werden.

5.1.3 Stromversorgung und Klimatisierung

Es müssen die Maßnahmen der Stromversorgung und Klimatisierung beschrieben werden, die eine Versorgung entsprechend der geforderten Verfügbarkeit nach Stand der Technik sicherstellen.

5.1.4 Wasserschäden

Die Maßnahmen, die zum Schutz gegen Wasserschäden ergriffen wurden, müssen beschrieben werden. Befindet sich die Liegenschaft in der Nähe von Gewässern oder in einer Niederung MUSS die Hochwassergefahr bewertet und bei Bedarf Maßnahmen ergriffen werden.

5.1.5 Brandschutz

Es MUSS dargelegt werden, wie die Systeme der CA vor Brandgefahren geschützt werden d.h. welche Brandschutzmaßnahmen sind zum Erhalt der Hochverfügbarkeit implementiert.

In allen System- und Systemoperatorräumen, in Archiven und in USV-Räumen sowie weiteren ausgewählten Räumen sind Brandfrüherkennungssysteme (Ansaugsysteme) zu installieren. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder zu verbauen.

5.1.6 Aufbewahrung von Datenträgern

Datenträger mit kritischen Betriebsdaten sind gesichert und vor Umwelteinflüssen geschützt zu lagern. Die Maßnahmen sind zu beschreiben.

5.1.7 Entsorgung

Dokumente und Datenträger müssen so entsorgt werden, dass je nach Vertraulichkeitsstufe der Daten, diese jederzeit gewährleistet ist. Die Entsorgung muss lückenlos protokolliert werden.

5.1.8 Externe Sicherung

Von kritischen Daten müssen Sicherheitskopien erzeugt werden und an einem anderen Standort oder in einem zweiten Brandabschnitt gelagert werden.

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Alle Rollen, die innerhalb der CA kritische Funktionen wahrnehmen und die Vertrauenswürdigkeit der CA einschränken können, werden als vertrauenswürdige Rollen bezeichnet. Dies sind in der Regel die Gruppen Systemadministratoren, RA-Mitarbeiter, CA-Operatoren und interne Auditoren.

Diese Rollenbereiche müssen in der CPS abgebildet werden. Diese Rollen dürfen nur mit geeigneten und vertrauenswürdigen Personen besetzt werden. Die Besetzung darf nur nach Genehmigung durch das Senior-Management erfolgen und muss regelmäßig mindestens alle drei (3) Jahre überprüft werden.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Kritische Aufgaben, insbesondere Arbeiten mit dem privaten Schlüssel der CA, müssen im Vier-Augen-Prinzip durch Personen in einer vertrauenswürdigen Rolle durchgeführt werden.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Mitarbeiter, die vertrauenswürdige Rollen übernehmen, müssen identifiziert werden und entsprechend 5.3.2 überprüft werden.

Jeder Rolleninhaber einer vertrauenswürdigen Rolle muss sich vor seiner Tätigkeit authentifizieren. Es muss sichergestellt sein, dass der Rolleninhaber sicher identifiziert werden kann.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Eine Aufgabentrennung MUSS für die Bereiche RA-Mitarbeiter/CA-Operator, Systemadministrator und Interner Auditor gewährleistet sein. Eine Person darf nur innerhalb einer dieser Bereiches Aufgaben übernehmen.

5.3 Personelle Maßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Alle Personen in der Zertifikatsverwaltung müssen vertrauenswürdig sein und über die notwendige Fachkunde und Erfahrung verfügen. Dies ist durch eine Prüfung nachzuweisen. Diese Prüfung muss vor der Durchführung von Tätigkeiten in einer vertrauenswürdigen Rolle positiv abgeschlossen sein. Ist die Prüfung nicht abgeschlossen, so kann in Ausnahmefällen eine Tätigkeit unter Beobachtung eines anderen Mitarbeiters in einer vertrauenswürdigen Rolle erfolgen.

5.3.2 Sicherheitsüberprüfung

Personen, die eine vertrauenswürdige Rolle übernehmen sollen, müssen ein Führungszeugnis gemäß Bundeszentralregistergesetz BZRG § 30 oder vergleichbares vorlegen. Stehen Einträge einer Übernahme der Rolle entgegen, so muss die Rollenübernahme abgelehnt werden. Die CA kann weitere Prüfungen vornehmen. Die Überprüfung des Führungszeugnisses (oder vergleichbar) sollte alle drei Jahre erneuert werden.

5.3.3 Schulungs- und Fortbildungsanforderungen

Das Personal muss geschult werden, bevor es entsprechende Tätigkeiten antritt. Diese Schulung muss mindestens die Themen Basiswissen zu Public Key Infrastrukturen, Anforderungen an PKIs z.B. CAB-Forum, Certificate Policy und/oder Certification Practice Statement umfassen. Zusätzliche Themen sind gängige Manipulationsmöglichkeiten von Dokumenten und des Verifikationsprozesses und Bedrohungen durch Phishing und Social Engineering.

5.3.4 Nachschulungsintervalle und -anforderungen

Das Personal muss regelmäßig nachgeschult werden insbesondere die Personen in vertrauenswürdigen Rollen müssen auf dem entsprechenden Wissensstand gehalten werden, der für diese aktuell festgelegt ist. Bei Änderungen sollte eine Nachschulung innerhalb von 3 Monaten durchgeführt werden.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Es muss sichergestellt werden, dass durch einen Wechsel eines Arbeitsplatzes in unterschiedlichen Bereichen siehe 5.2.4) kein Rollenausschluss umgangen werden kann. Dies muss in den Sicherheitskonzepten betrachtet werden.

5.3.6 Sanktionen bei unbefugten Handlungen

Unbefugte Handlungen müssen protokolliert und sanktioniert werden und je nach Schwere muss die Handlung zum Ausschluss der Person aus dem CA-Betrieb führen.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Für externes Personal müssen die gleichen Anforderungen gelten und umgesetzt sein, wie die für Mitarbeiter beschriebenen. Dies gilt auch für die Regelungen für die Speicherfrist von Dokumenten und die Anforderungen an das Event-Logging.

5.3.8 Dokumentation für das Personal

Den Rolleninhabern müssen ausreichende Dokumentationen zur Erledigung ihrer Tätigkeiten zur Verfügung gestellt werden.

5.4 Protokollereignisse

5.4.1 Art der aufgezeichneten Ereignisse

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

CA-Schlüsselpaare und CA-Systeme

Für das Lebenszyklus -Management für CA-Schlüsselpaare bzw. von CA-Systemen müssen mindestens die folgenden Ereignisse protokolliert werden:

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

EE- und CA-Zertifikate

Für das Lifecycle-Management von sowohl EE- als auch CA-Zertifikaten müssen mindestens die folgenden Ereignisse protokolliert werden:

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

Sonstige sicherheitsrelevante Ereignisse

Zusätzlich müssen für den Betrieb der Infrastruktur alle sicherheitsrelevanten Ereignisse protokolliert werden. Dies beinhaltet mindestens die folgenden Ereignisse:

- Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI,
- Durchgeführte Aktionen an und durch die PKI- und sonstige sicherheitsrelevante Systeme,
- Änderungen an Sicherheitsprofil,
- Systemabstürze, Hardware-Ausfälle und andere Anomalien,
- Firewall- und Router-Aktivitäten,
- Zutritt und Verlassen von Einrichtungen des Trust Centers

Diese Dokumentationspflicht MUSS auch für die Bearbeitung von Zertifikatsanträgen durch Dritte durch den Dritten umgesetzt werden.

Alle Protokolldaten müssen den Berechtigten internen und externen Auditoren auf Anfrage zugänglich gemacht werden, um die Konformität zu den genannten Anforderungen überprüfen zu können.

5.4.2 Bearbeitungs- und Archivierungsintervall für Audit-Protokolle (Logs)

Die Protokolldaten müssen regelmäßig, mindestens alle sechs Monate, ausgewertet und archiviert werden.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Die Protokolldaten müssen mindestens sieben (7) Jahre aufbewahrt werden. Die Protokolldaten müssen einen internen oder externen Auditor auf Anfrage zur Verfügung gestellt werden.

5.4.4 Schutz der Audit-Protokolle

Die Protokolldaten müssen gesichert und integritätsgeschützt aufbewahrt werden. Die CA muss sicherstellen, dass die Protokolldaten nicht gelöscht werden.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Auditprotokolle müssen regelmäßig gesichert und an einem anderen Standort gelagert werden.

5.4.6 Audit-Protokolle-Erfassungssystem (intern vs. extern)

Wird eine automatische Protokollierung verwendet, so MUSS die CA Sorge tragen, dass die Integrität zu jeder Zeit sichergestellt wird. Bei Systemstörungen sollte bis zur Behebung der Betrieb ausgesetzt werden.

5.4.7 Benachrichtigung des Ereignisauslösenden Subjekts

Löst eine Person ein Auditereignis aus, so KANN die Person je nach Art über die Auslösung informiert werden.

5.4.8 Schwachstellenprüfung

Die CA MUSS ihre Systeme regelmäßig mindestens quartalsmäßig auf Schwachstellen untersuchen.

Das Sicherheitskonzept MUSS eine jährliche Risikoanalyse beinhalten, die die vorhersehbaren internen und externen Bedrohungen identifiziert, die zu einem unautorisierten Zugriff, Veröffentlichung, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können. Die Risikoanalyse muss die Wahrscheinlichkeit und den potentiellen Schaden dieser Bedrohungen betrachten. Weiterhin muss die Sensibilität der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses berücksichtigt werden.

Die Risikoanalyse muss überprüfen, ob Vorgaben, Verfahren, Informationsverarbeitende Systeme, Technik und andere Zusammenstellungen, welche die CA nutzt, ausreichend sind, um den Bedrohungen wirksam zu begegnen.

5.5 Datenarchivierung

5.5.1 Art der archivierten Datensätze

Die CA muss mindestens die folgenden Daten archivieren:

- CPS, CP, AGB und vertragliche Unterlagen
- Zertifizierungsunterlagen und Auditberichte
- Systemkonfigurationen
- Antragsunterlagen inkl. Prüfungen
- Ausgestellte Zertifikate

- Sperranträge
- Sicherheitskonzeption
- Sicherheitsvorfälle
- Protokolldaten

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Alle in Kapitel 5.5.1 genannten Aufzeichnungen müssen mindestens sieben (7) Jahre aufbewahrt werden. Gesetzliche Anforderungen müssen eingehalten werden.

5.5.3 Schutz von Archiven

Die CA MUSS sicherstellen, dass nur autorisierte und vertrauenswürdige Personen Zutritt zu Archiven erhalten.

5.5.4 Sicherungsverfahren für Archive

Archivdaten müssen gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt werden. Die Haltbarkeit der Medien und der genutzten Datenformate MUSS dabei sichergestellt werden.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Alle Ereignisse, die durch die Datensätze in 5.5.1 dokumentiert werden, müssen das Datum und die Uhrzeit beinhalten.

5.5.6 Archiverfassungssystem (intern oder extern)

Telekom Security verwendet interne Archivierungssysteme oder Archivierungsdienstleister, die entsprechende Zertifizierungen vorweisen können.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Nur autorisiertes und vertrauenswürdiges Personal erhält Zutritt zu Archiven und Zugang/Zugriff zu Archivdaten. Archivdaten werden integritätsgesichert und im Rahmen eines Zugriffs überprüft. Dies wird in die Protokollierung aufgenommen.

5.6 Schlüsselwechsel

Die CAs muss darlegen, wie ein Schlüsselwechsel der CA erfolgt und der neue Schlüssel zu dem Benutzer gelangt.

5.7 Kompromittierung und Wiederherstellung der Dienstleistung

Die eingeschlossenen CAs müssen über einen Geschäftserhaltungsplan (business continuing plan) verfügen, der jährlich gereviewt und durch Notfallübungen getestet wird.

5.7.1 Umgang mit Störungen und Kompromittierungen

Der Geschäftserhaltungsplan (business continuing plan) muss folgende Aspekte beinhalten:

1. die Bedingungen für die Einleitung der beschriebenen Maßnahmen,
2. die Notfallprozesse,
3. die Rücknahme-Prozesse (fallback)
4. Wiederaufnahmepläne
5. Reviewangaben für die Planung

6. Sensibilisierung und Wissensanforderungen
7. Die persönliche Verantwortung der Beteiligten
8. Vorgaben für die Wiederherstellungszeiten
9. Regelmäßiges Testen möglicher Fälle
10. Einen Zeitplan zur Wiederherstellung bzw. Wiederaufnahme des Geschäftsbetriebes nach einem Fehler oder Ausfall.
11. Eine Anforderung kritisches kryptografisches Material (e.g. HSM) an einem alternativen Ort zu lagern.
12. Die Festlegung von akzeptablen Zeiten für Systemausfall und Wiederherstellung.
13. Die Festlegung von Backupzyklen für essentielle Geschäftsinformationen und Software.
14. Die Entfernung von Wiederherstellungsstandorten und dem Hauptstandort der CA.
15. Planungsunterlagen für die Sicherung der Geschäftsräume während eines Desasters und der Wiederherstellung an diesem Standort oder an einem anderen Standort.

Die CA muss diese Prozesse jährlich testen, überprüfen und ggf. überarbeiten.

Die CA muss nicht notwendiger Weise die Maßnahmen zur Geschäftserhaltung offenlegen, dies muss nur gegenüber den befugten Auditoren auf Anfrage erfolgen.

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

Bei einer Beschädigung der EDV-Komponenten, Software und/oder Daten MUSS der Vorfall unmittelbar untersucht und gemeldet werden.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

Bei Kenntnisnahme einer Kompromittierung des privaten Schlüssels einer CA MUSS der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet werden.

Endteilnehmer MÜSSEN von der CA über die mögliche Kompromittierung über die einschlägigen Webseiten informiert werden). Falls erforderlich müssen betroffene Zertifikate unverzüglich gesperrt werden und die entsprechende Zertifizierungsstelle Sperrlisten (ARL, CRL) generieren und veröffentlichen.

5.7.4 Geschäftskontinuität nach einem Notfall

Die CA muss für den Rechenzentrumsbetrieb einen Notfallplan entwickeln, implementieren und testen, um die Auswirkungen von Katastrophen jeder Art (Naturkatastrophen oder Katastrophen menschlichen Ursprungs) zu mildern und die Verfügbarkeit kritischer Geschäftsprozesse schnellstmöglich wiederherzustellen. Dies MUSS alle Prozesse, Komponenten, Systeme und Dienste der CA abdecken. Dieser Plan MUSS regelmäßig mindestens jährlich überprüft, getestet und entsprechend aktualisiert werden, um im Falle einer Katastrophe gezielt und strukturiert reagieren zu können.

Der Notfallplan MUSS mindestens die folgenden Informationen enthalten:

- Die notwendigen Kriterien für die Aktivierung des Planes
- Mögliche Notfallmaßnahmen (je nach Situation)
- Fallback Verfahren
- Wiederanlauf Verfahren
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung
- Bewusstsein-schaffende Maßnahmen
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals

- Die Verantwortung der Individuen (Rollenbeschreibung und -zuweisung)
- Wiederanlaufzeit (RTO)
- Regelmäßige Durchführung der Notfallpläne zu Testzwecken
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der Geschäftstätigkeit nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse
- Eine Verpflichtung kritische kryptographische Geräte und Informationen an einem anderen Standort zu sichern bzw. vorzuhalten.
- Festlegung der maximal tolerierbaren Ausfallzeit (MTD) und entsprechende Zeiten zur Wiederherstellung
- Häufigkeit, in der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur Hauptgeschäftsstelle bzw. zum Rechenzentrum des Trust Centers
- Verfahren zur bestmöglichen Sicherung der Betriebsstätten und –Einrichtungen nach einer Katastrophe (Notbetrieb) bis zur Wiederherstellung eines den Anforderungen entsprechend gesicherten Normalbetriebs

Auf Anfrage muss der interne und externe Auditor Einsicht in den Notfallplan nehmen können.

5.8 Einstellung des CA oder RA Betriebes

Die eingeschlossenen CAs müssen entsprechende Maßnahmen bei Beendigung des Betriebs, d.h. Einstellung der Dienstleistung in einem Betriebseinstellungskonzept beschreiben. Dies umfasst insbesondere die Mitteilung der Betriebseinstellung und die Verwahrung der entsprechenden Unterlagen der CA.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

Zertifizierungsstellen, die in der Hierarchie der eingeschlossenen Root-CA-Zertifikate stehen, müssen Regelungen wie die im Folgenden beschriebenen in adäquater Weise umsetzen und in ihrer CPS beschreiben.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

6.1.1.1 Generierung von CA-Schlüsselpaaren

Die Generierung von Root-CA- Schlüsselpaaren soll nach einem Generationsskript durchgeführt werden und von einem qualifizierten Auditor begleitet werden. Es ist einer Schlüsselzeremonie zu folgen.

CA-Schlüssel sind in einem „FIPS 140-2 Level 3“ oder „Common Criteria EAL 4“ konformen Hardware Security Module zu erzeugen Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip erzwungen. Die Erstellung von CA-Schlüsseln wird gemäß [EN 319 411] dokumentiert.

6.1.1.2 Generierung von RA-Schlüsselpaaren

Keine Vorgabe.

6.1.1.3 Generierung von Subscriber-Schlüsselpaaren (EE-Zertifikate)

Der Zertifikatnehmer ist bei der Erzeugung von EE-Schlüsseln verpflichtet, diese entsprechend der Vorgaben aus [EN 319 411-1] kryptografisch sicher zu erzeugen.

6.1.2 Bereitstellung des privaten Schlüssels an Zertifikatsnehmer

Die erzeugten Schlüssel sind über folgende Wege an den Kunden sicher per CD, integritätsgeschützten Datencontainer, signierte und verschlüsselte Email zu übergeben.

Private Schlüssel dürfen nur vom Zertifikatsnehmer archiviert werden.

Wenn die CA Kenntnis davon erlangt, dass der private Schlüssel des Zertifikatsnehmers an eine nicht autorisierte Person oder eine nicht verbundene Organisation übermittelt wurde, dann widerruft die CA alle Zertifikate, die den öffentlichen Schlüssel enthalten, der dem übermittelten privaten Schlüssel entspricht.

6.1.3 Bereitstellung des öffentlichen Schlüssels an die Zertifizierungsstelle

Die Lieferung des öffentlichen Schlüssels an die Zertifizierungsstelle ist dies im CPS der jeweiligen Zertifizierungsstelle zu beschreiben. Der öffentliche Schlüssel soll in der Regel in Form eines signierten Zertifikatsrequests auf einem sicheren Weg geliefert werden.

6.1.4 Bereitstellung des öffentlichen CA-Schlüssels

Die Lieferung kann als Anhang zum Zertifikat erfolgen. Eine Bereitstellung kann darüber durch Veröffentlichung in einer Web-Seite oder in einem LDAP Verzeichnis erfolgen.

Die konkrete Lieferung/Bereitstellung des öffentlichen Schlüssels der ausstellenden CAs ist im CPS der jeweiligen Zertifizierungsstelle zu beschreiben.

6.1.5 Algorithmen und Schlüssellängen

6.1.5.1 Root-CA Zertifikate

Die Schlüssellänge der Root-CA-Zertifikate muss bei Nutzung eines RSA Schlüssels mindestens 2048-Bit, bei Nutzung eines ECC Schlüssels mindestens 256-Bit (zulässig ECC Kurve: NIST P-256, P-384 oder P-521) betragen.

Als Hash-Algorithmus muss entweder SHA-256, SHA-384 oder SHA-512 Anwendung finden.

Bei Anwendung von DSA müssen für den minimalen DSA Modulus und Divisor Größe L=2048 und N=224 oder L=2048 und N=256 Bits gelten.

6.1.5.2 Subordinate-CA Zertifikate

Die Schlüssellänge für Sub-CA-Zertifikate MUSS für RSA Schlüssel mindestens 2048-Bit, für ECC Schlüssel mindestens 256 Bit betragen. Der Hash-Algorithmus muss min. SHA-256 Bit betragen.

Bei Anwendung von DSA, müssen min. L=2048 und N=224 Anwendung finden (siehe FIPS 186-4)

6.1.5.3 Subscriber-Zertifikate (EE)

Die Schlüssellänge für EE-Zertifikate muss für RSA Schlüssel mindestens 2048-Bit, für ECC Schlüssel mindestens 256 Bit betragen. Der Hash-Algorithmus muss min. SHA-256 Bit betragen.

Bei Anwendung von DSA, müssen min. L=2048 und N=224 Anwendung finden (siehe FIPS 186-4)

6.1.6 Generierung öffentlicher Schlüsselparameter und Qualitätskontrolle

Die Festlegung der Parameter der öffentlichen Schlüssel von Root CA-, Sub-CA- und EE-Zertifikaten und ggf. anzuwendende Qualitätskontrollen sind in den CPS Dokumenten der Zertifizierungsstellen festgelegt.

Die Vorgaben von [CAB-BR] im entsprechenden Kapitel sind einzuhalten.

6.1.7 Schlüsselverwendung

Private Root-CA-Schlüssel dürfen ausschließlich zum Signieren von Sub-CA-Zertifikaten, OCSP Zertifikaten und Sperrlisten verwendet werden.

Die privaten Sub-CA-Schlüssel dürfen zum Signieren von Sub-CA-Zertifikaten, OCSP Zertifikaten, EE-Zertifikaten und Sperrlisten benutzt werden.

Die EE-Schlüssel dürfen nur für die im Zertifikat benannten Nutzungsarten verwendet werden.

Es sind ausschließlich die Schlüsselverwendungen (keyUsage) aus Kapitel 7 zu verwenden.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

Die privaten Schlüssel der Root-CAs müssen auf einem sicherheitsüberprüften Hardware Security Modul (FIPS 140-2 / Level 3 evaluiert) abgelegt sein.

Technische oder andere Kontrollen, die sich gemäß [CAB-BR] und [ETSI] auf die kryptographischen Module beziehen, sind einzuhalten.

6.2.2 Mehrpersonenkontrolle (n aus m) bei privaten Schlüsseln

Die Kontrolle von privaten Root Schlüsseln ist im CPS der jeweiligen Zertifizierungsstelle im Detail zu definieren. Die Ausführung von Aktionen und er Zugriff ist so zu beschränken, dass mindestens 2 Personen mit unterschiedlichen Berechtigungen erforderlich sind.

6.2.3 Hinterlegung von privaten Schlüsseln

Eine Hinterlegung von privaten Schlüsseln bei Treuhändern außerhalb von Telekom Security wird nicht durchgeführt.

6.2.4 Sicherung (Key-Backup) von privaten Schlüsseln

Die Sicherung von privaten Schlüsseln und zugehörige Sicherheitskontrollen sind im CPS der jeweiligen Zertifizierungsstelle zu beschreiben.

Die privaten Schlüssel dürfen nur von Personen in vertrauenswürdigen Rollen gesichert, gespeichert und wiederhergestellt werden. Die Sicherung darf nur auf kryptografischen Schlüsselspeichergeräten erfolgen.

6.2.5 Archivierung von privaten Schlüsseln

Nach dem Ende der Gültigkeit von Root-CA-Schlüsseln sind die Vorgaben des Löschkonzeptes umzusetzen.

Sub-CA-Schlüssel dürfen nur vom Zertifikatsnehmer archiviert werden.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Die Übertragung von privaten Schlüsseln ist in geeigneten Security Token vorzunehmen. Private Schlüssel, dürfen zu keinem Zeitpunkt unverschlüsselt vorliegen. Das 4 Augenprinzip (gemäß Kapitel 6.2.2) ist zu dokumentieren.

6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

Es darf nur den Anforderungen entsprechende Hardware, gemäß NIST –Liste und [ETSI] genutzt werden.

Die Speicherung von privaten Schlüsseln auf kryptografischen Modulen ist, falls zutreffend, im CPS der jeweiligen Zertifizierungsstelle zu beschreiben.

6.2.8 Methode zur Aktivierung privater Schlüssel

Aktivierung privater Root-CA-Schlüssel auf kryptografischen Modulen

Die Aktivierung privater Schlüssel auf kryptografischen Modulen ist im CPS der jeweiligen Zertifizierungsstelle zu beschreiben.

Die Root-CA-Schlüssel müssen protokolliert durch Mehrpersonen (2 Personen unterschiedlicher Rolle) aktiviert werden. Die Voraussetzungen sind freigegebene kryptogr. Hardware (HSM), 4-Augenprinzip und der Einsatz von Shared Secrets.

Aktivierung privater Sub-CA-Schlüssel auf kryptografischen Modulen

Die Aktivierung privater Schlüssel auf kryptografischen Modulen ist im CPS der jeweiligen Zertifizierungsstelle zu beschreiben.

Aktivierung von Endteilnehmer-Zertifikaten auf kryptographischen Modulen

Die Schlüssel sind wirtschaftlich angemessen durch mindestens eine der folgenden Maßnahmen zu schützen:

- Passwort-Schutz
- Schutz durch geeignete Hardware
- Verschlüsselung
- geeignete Ablage

6.2.9 Methode zur Deaktivierung privater Schlüssel

Die Deaktivierung privater Root-CA-Schlüssel ist unverzüglich nach Ende der Aktionen durch Mehrpersonen (2 Personen unterschiedlicher Rolle) vorzunehmen. Die privaten Root-CA-Schlüssel werden durch Beendigung der Verbindung zwischen HSM und Anwendung deaktiviert. Die Deaktivierung ist zu protokollieren.

6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von Root-CA-Schlüsseln durch Mehrpersonen (2 Personen unterschiedlicher Rolle) vorzunehmen und zu dokumentieren. Dabei muss sichergestellt werden, dass nach Vernichtung keine Fragmente oder Sicherungen des Schlüssels übrigbleiben, die zu einer Rekonstruktion des Schlüssels führen könnte.

6.2.11 Methode zur Beurteilung kryptographischer Module

Kryptografische Module sind anhand Common Criteria Level EAL 4 oder FIPS 140-2 Level 3 zu beurteilen.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung von öffentlichen Schlüsseln

Die Archivierung von Root-CA-Schlüsseln ist immer durch Mehrpersonen (2 Personen unterschiedlicher Rolle) durchzuführen und zu dokumentieren.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die maximale Gültigkeit für Root-CA-Schlüssel und Root-CA-Zertifikate beträgt 25 Jahre.

Die maximale Gültigkeit für Sub-CA-Schlüssel und Sub-CA-Zertifikate beträgt 25 Jahre.

Die maximale Gültigkeit von SSL/TLS Zertifikaten beträgt 825 Tage.

Die maximale Gültigkeit von Nutzerzertifikaten beträgt 60 Monate.

Die Gültigkeit von Zertifikaten darf nicht länger sein als die des ausstellenden CA-Zertifikats.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Die Erzeugung von Aktivierungsdaten ist durch Mehrpersonen (2 Personen unterschiedlicher Rolle) durchzuführen und zu dokumentieren.

Wird das EE-Schlüsselpaar vom Zertifikatnehmer erzeugt, muss das Aktivierungsgeheimnis bei diesem Verfahren ebenfalls produziert werden und steht dem Zertifikatnehmer somit zur Verfügung.

6.4.2 Schutz von Aktivierungsdaten

Die Aktivierungsdaten (Geheimnisanteile) sind in geeigneter Weise vor unberechtigtem Zugriff und Einsicht zu schützen:

Ablage entsprechend in dafür vorgesehenen Tresoren, Smartcards oder durch Aufteilen von Passworten auf mehre berechtigte Personen.

6.4.3 Weitere Aspekte von Aktivierungsdaten

Übertragung von Aktivierungsdaten

Die Übertragung von Aktivierungsdaten ist nur durch die persönliche Übergabe zulässig.

Vernichtung von Aktivierungsdaten

Die Vernichtung hat zu erfolgen, wenn die Aktivierungsdaten nicht mehr benötigt werden. Die Vernichtung ist durch geeignete Maßnahmen wie sichere Löschfunktion, Unkenntlichmachung durch Schreddern oder in speziell gekennzeichneten Behältern für sichere Aktenentsorgung, durchzuführen.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Es ist sicherzustellen, dass die Verwaltung der CA-Systeme vor unbefugtem Zugriff Dritter gesichert ist.

Die Verwendung von Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, 2-Faktor-Authentisierung, personalisierte Chipkarten, 4-Augen-Prinzip), um die CA-Funktionalitäten, Verzeichnisdienste und OCSP-Responder vor internen und externen Eindringligen zu schützen, ist zwingend vorgeschrieben.

6.5.2 Bewertung der Computersicherheit

Eine Bewertung der Computersicherheit hat jedem die Computersicherheit betreffenden Vorfall, mindestens aber einmal im Jahr zu erfolgen.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Kontrollen der Systementwicklung

Es sind alle Aspekte der sicheren Systementwicklung zu berücksichtigen (wie sichere Entwicklungsumgebung, Configuration Management).

6.6.2 Kontrollen des Sicherheitsmanagements

Die Sicherheitsverwaltungskontrollen sind im CPS zu beschreiben.

6.6.3 Sicherheitskontrollen des Lebenszyklus

Eingesetzte Geräte müssen gemäß Herstellerangaben betrieben werden. Vor Inbetriebnahme müssen sie eingehend geprüft und dürfen nur zum Einsatz kommen, wenn zweifelsfrei feststeht, dass sie nicht manipuliert wurden.

Durch Versiegelung der Hardware (bei Root-CAs) und Softwarechecks müssen Manipulationen und Manipulationsversuche erkennbar sein.

6.7 Netzwerk-Sicherheitskontrollen

Es sind alle erforderlichen Netzwerk-Sicherheitsmaßnahmen zu ergreifen

Folgende Netzwerk-Sicherheitsmaßnahmen sind zu implementieren:

Die Netzwerke der untergeordneten Zertifizierungsdienste sind durch aktuelle, dem Stand der Technik entsprechende Firewalls, vom Internet zu trennen. Der Datenverkehr ist auf das für die Funktionen notwendige Maß zu beschränken.

Sicherheitskritische Komponenten und Systeme, die vom Internet aus erreichbar sind (z.B. Verzeichnisdienst, OCSP-Responder) sind durch Firewalls vom Internet und den internen Netzen zu trennen. Alle anderen sicherheitskritischen Komponenten und Systeme (z.B. CA, DB, Signer) müssen in einem separaten Netz betrieben werden.

6.8 Zeitstempel

Datums- und Zeitinformationen in Zertifikaten, Sperrlisten, Online-Statusprüfungen und anderen wichtige Informationen sollen aus einer zuverlässigen Zeitquelle abgeleitet werden (siehe Kapitel 5.5.5).

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

Die Zertifikate sind nach dem X.509 Standard aufgebaut. Die Namensattribute sowohl für Zertifikatsnehmer, als auch –herausgeber werden im X.501 Standard notiert.

Die Seriennummer muss mit einem kryptographisch sicheren Zufallszahlengenerator erstellt werden. Sie muss größer als Null sein und mindestens 64 bit Entropie besitzen. Sie muss pro Aussteller einmalig sein.

Die Zertifikatsprofile müssen in dem CPS der jeweiligen Zertifizierungsstelle im Detail definiert werden.

7.1.1 Versionsnummer(n)

Zertifikate müssen entsprechend der internationalen Norm X.509 in der Version 3 (X.509v3) ausgestellt werden.

7.1.2 Zertifikatsinhalte und -erweiterungen nach RFC 5280

Die Telekom Security PKI nutzt zur Erfüllung der X509v3 Vorgaben Zertifikatserweiterungen. Abhängig von der Art des Zertifikats werden verpflichtende und optionale Erweiterungen definiert.

Zu jeder Erweiterung werden Vorgaben hinsichtlich der zu verwendenden Parameter und Anforderungen zur Kritikalität des Parameters gegeben.

7.1.2.1 Root-CA-Zertifikate

Root-CA-Zertifikate dürfen keine Erweiterung „certificatePolicies“ enthalten.

Root-CA-Zertifikate müssen folgende Erweiterungen („Pflichtfeld“) enthalten:

Tabelle 7 - Zertifikatserweiterungen von Root-CA-Zertifikaten (1)

Erweiterung (Pflichtfelder)	**OID**	**Parameter**	**Kritikalität der Erweiterung**
KeyUsage	2.5.29.15	keyCertSign, cRLSign, digitalSignature (optional)	kritisch
BasicConstraints	2.5.29.19	CA=TRUE, (keine pathLenConstraint	kritisch
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key	unkritisch

Root-CA-Zertifikate können folgende optionale Erweiterungen enthalten:

Tabelle 8 - Zertifikatserweiterungen von Root-CA-Zertifikaten (2)

Erweiterung (optional)	OID	Parameter	Kritikalität der Erweiterung
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels	unkritisch

7.1.2.2 Sub-CA-Zertifikate

Sub-CA-Zertifikate müssen folgende Erweiterungen („Pflichtfeld“) enthalten:

Tabelle 9 - Zertifikatserweiterungen von Sub-CA-Zertifikaten (1)

Erweiterung	OID	Parameter	Kritikalität
KeyUsage	2.5.29.15	keyCertSign, cRLSign, digitalSignature (optional)	kritisch
BasicConstraints	2.5.29.19	CA=TRUE, pathLenConstraint	kritisch
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs	unkritisch
cRLDistributionPoints	2.5.29.31	Adresse(n) der CRLAusgabestelle	unkritisch
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…} accessMethod=caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}	unkritisch

Sub-CA-Zertifikate können folgende optionale Erweiterungen enthalten:

Tabelle 10 - Zertifikatserweiterungen von Sub-CA-Zertifikaten (2)

Erweiterung	OID	Parameter	Kritikalität
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels	unkritisch
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key	unkritisch
nameConstraints			Gemäß [CAB-BR]
ExtKeyUsage	2.5.29.37	Entsprechend [RFC 5280]	unkritisch

Andere Erweiterungen sind zugelassen, müssen aber als unkritisch gesetzt sein.

7.1.2.3 EE-Zertifikate

EE-Zertifikate (End Entity / Endteilnehmer) müssen folgende Erweiterungen enthalten:

Tabelle 11 - Zertifikatserweiterungen von EE-Zertifikaten (1)

Erweiterung	OID	Parameter	Kritikalität
certificatePolicies	2.5.29.32	OIDs der unterstützten	unkritisch

Erweiterung	OID	Parameter	Kritikalität
		CPs cpsURI	
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…} accessMethod=calssu er {1.3.6.1.5.5.7.48.2}, accessLocation {…}	unkritisch
ExtKeyUsage	2.5.29.37	Entsprechend [RFC 5280]	unkritisch
SubjectAltName	2.5.29.17	Alternativer Inhabername	unkritisch

EE-Zertifikate können folgende optionale Erweiterungen enthalten:

Tabelle 12 - Zertifikatserweiterungen von EE-Zertifikaten (2)

Erweiterung	OID	Parameter	Kritikalität
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels	unkritisch
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key	unkritisch
CRLDistributionPoints	2.5.29.31	Adresse(n) der CRLAusgabestelle	unkritisch
KeyUsage	2.5.29.15	keyCertSign und cRLSign dürfen NICHT gesetzt sein Möglich sind: digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly und Kombinationen	kritisch
BasicConstraints	2.5.29.19	Der Wert CA=TRUE darf NICHT gesetzt sein	Kritisch
QCStatements (nur QCP-w)	1.3.6.1.5.5.7.1.3	esi4-qcStatement-1 {0 4 0 1862 1 1}; esi4-qcStatement-5 {0 4 0 1862 1 5}; esi4-qcStatement-5; qc-type-web {0 4 0 1862 1 6 3};	unkritisch

7.1.2.4 Alle Zertifikate

Alle weiteren Felder müssen konform zu [RFC 5280] sein.

7.1.2.5 Anwendung von [RFC 5280]

Alle weiteren Felder müssen konform zu [RFC 5280] sein.

7.1.3 Objekt-Kennungen von Algorithmen

Zum Signieren von Zertifikaten darf nur eine eingeschränkte Anzahl an Algorithmen genutzt werden.

Folgende Signaturalgorithmen dürfen für neue Zertifikate verwendet werden:

- SHA256 RSA (OID 1.2.840.113549.1.1.11)
- SHA384 RSA (OID 1.2.840.113549.1.1.12)
- SHA512 RSA (OID 1.2.840.113549.1.1.13)
- SHA256 ECDSA (OID 1.2.840.10045.4.3.2)
- SHA384 ECDSA (OID 1.2.840.10045.4.3.3)
- SHA512 ECDSA (OID 1.2.840.10045.4.3.4)

CAs dürfen den SHA-1 Algorithmus nicht mehr zur Ausstellung von Sub-CA oder EE-Zertifikaten einsetzen. Sub-CA, und EE-Zertifikate dürfen nur mit dem SHA-256 Hash-Algorithmus oder höher ausgestellt werden. EE-Zertifikate dürfen keine Zertifikatskette haben die auf eine Sub-CA mit SHA-1 Algorithmus zurückgeht.

CAs können Root CA Zertifikate oder Sub-CA Zertifikate die als **Cross-Zertifikate** fungieren mittels SHA-1 Algorithmus ausstellen. Ebenso können CAs weiterhin ihre bereits existierenden SHA-1 Root Zertifikate verwenden.

7.1.4 Namensformen

Für die Namensformen von Root-CA, Sub-CA und EE-Zertifikaten müssen die Vorgaben der [CAB-BR] im entsprechenden Kapitel eingehalten werden.

7.1.4.1 Issuer Informationen

Der Inhalt des „Issuer Distinguished Name“ Feldes muss dem Subject DN der Issuing CA entsprechen. Die Angabe muss konsistent zu den Vorgaben aus RFC 5280, Kapitel 4.1.2.4 sein.

7.1.4.2 Subject Information für Endteilnehmer Zertifikate

7.1.4.2.1 Subject Alternative Name Erweiterung

Bzgl. der Subject Alternative Name Extension dürfen CAs keine Zertifikate ausgeben, die in der Subject Alternative Name Erweiterung oder im Subject CommonName Feld eine reservierte IP-Adresse oder einen internen Namen enthalten. Einträge im dNSName müssen die vorgeschlagene Namenssyntax gemäß [RFC 5280] erfüllen und dürfen keine Unterstriche “_“ enthalten.

7.1.4.2.2 Subject Distinguished Name Fields

Die Endteilnehmer-Zertifikate der untergeordneten Zertifizierungsstellen (Sub-CA) müssen einen, für diesen Service, eindeutigen Ausstellernamen (Issuer DN) und einen eindeutigen Auftragstellernamen (Subject DN), gemäß den Ausführungen aus Kapitel 3.1 enthalten.

Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.1 (DV) verwendet, DÜRFEN folgende Felder des Subject DN NICHT ausgefüllt sein:

- organizationName
- streetAddress
- localityName
- stateOrProvinceName
- postalCode

Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.2 (OV) verwendet, MÜSSEN zwingend folgende Felder des Subject DN ausgefüllt sein:

- organizationName

- localityName
- stateOrProvinceName (falls ein sinnvoller Wert existiert, z.B. Bundesland)
- countryName

Werden in einem Zertifikat die Policy-OIDs 2.23.140.1.1 (EV) und 0.4.0.194112.1.4 (qcp-web) verwendet, MÜSSEN zwingend folgende Felder des Subject DN ausgefüllt sein:

- organizationName
- AltName
- businessCategory
- jurisdictionLocalityName (Ausnahme lt. CAB-BR zulässig)
- jurisdictionStateOrProvinceName (Ausnahme lt. CAB-BR zulässig)
- jurisdictionCountryName (Ausnahme lt. CAB-BR zulässig)
- serialNumber
- streetAddress
- localityName
- stateOrProvinceName (falls ein sinnvoller Wert existiert, z.B. Bundesland)
- countryName
- postalCode

7.1.4.3 Subject Informationen für Root-CA- und Sub-CA-Zertifikate

7.1.4.3.1 Subject Distinguished Name Fields

Bei Root-CA- und Sub-CA-Zertifikaten müssen folgende Felder ausgefüllt sein:

- commonName
- organizationName
- countryName

Subject Attribute dürfen nicht ausschließlich Metadaten wie „.“, „-“ oder „ “ enthalten, fehlen, unvollständig oder nicht anwendbar sein. Die CA muss ggf. andere vorhandene Attribute und deren Informationen verifizieren.

7.1.5 Namensbeschränkungen

Root-CA-Zertifikate DÜRFEN nicht namensberschränkt werden.

Namensbeschränkungen für Sub-CA-Zertifikate sind optional. Sie sind zur technischen Beschränkung einer Sub-CA einzusetzen.

Damit ein Sub-CA-Zertifikat technisch beschränkt ist, MUSS das Zertifikat eine Extended Key Usage (EKU)-Erweiterung enthalten, die alle berechtigten Schlüsselverwendungen angibt. Nur für diese Verwendungen dürfen von der Sub-CA Zertifikate ausgestellt werden dürfen.

Wird der die EKU id-kp-serverAuth gesetzt, muss das Sub- CA-Zertifikat die Erweiterung Name Constraints X.509v3 mit Einschränkungen für dNSName, iPAddress und/oder DirectoryName enthalten.

Der anyExtendedKeyUsage Wert darf innerhalb dieser Erweiterung NICHT gesetzt werden.

Beim Setzen von Beschränkungen müssen die detaillierten Vorgaben der [CAB-BR] im entsprechenden Kapitel eingehalten werden.

7.1.6 Objekt-Identifikatoren für Zertifizierungsrichtlinien

7.1.6.1 Reservierte Objekt-Identifikatoren für Zertifizierungsrichtlinien

Die reservierten Objekt-Identifikatoren lt. [CAB-BR] im entsprechenden Kapitel sind zu beachten und dürfen nur für die vorgesehenen Zwecke gesetzt werden.

7.1.6.2 Root-CA Zertifikate

Root-CA-Zertifikate dürfen keine Zertifizierungsrichtlinien enthalten

7.1.6.3 Sub-CA Zertifikate

Externe Sub-CA Zertifikate (non affiliate) enthalten eine Policy-OID, die dediziert die Zusicherung repräsentiert, dass die Sub-CA während ihres Lebenszyklus die Anforderungen der [CAB-BR] im entsprechenden Kapitel, erfüllt.

In externen Sub-CA Zertifikaten (non affiliate) ist die anyPolicy-OID (2.5.29.32.0) nicht erlaubt. Für interne Sub-CA Zertifikate (affiliate) darf diese OID verwendet werden.

In allen Fällen ist sicherzustellen, dass mindestens eine der verwendeten Policy-OIDs sowohl in entsprechenden öffentlichen Geräte-Zertifikaten, als auch in dem/den entsprechenden Sub-CA Zertifikaten vorhanden ist.

Die Regelungen dieses Kapitels gelten für alle Hierarchie-Ebenen hierarchisch unterhalb der Root-CAs, d.h. auch für die Verkettung von Sub-CA Zertifikaten.

7.1.6.4 Endteilnehmer Zertifikate

Endteilnehmer-Zertifikate, welche von einer Sub-CA im Scope dieses Dokuments ausgestellt werden, müssen eine Certificate Policy Erweiterung und Policy-OID enthalten, welche dediziert die Zusicherung repräsentiert, dass das Zertifikat während seines Lebenszyklus die Anforderungen der [CAB-BR] erfüllt. Dies MUSS in der Zertifikats Policy oder im CPS dokumentiert werden.

Diese Policy-OID muss im CPS der jeweiligen Sub-CA definiert und beschrieben sein.

7.1.7 Verwendung der Erweiterung von Policy Constraints

Keine Vorgabe.

7.1.8 Syntax und Semantik von Policy Qualifiers

Siehe Abschnitt 1.2.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Certificate Policies

In Sub-CA- und EE-Zertifikaten ist die Erweiterung CertificatePolicies (Zertifikatsrichtlinie) NICHT kritisch. Es liegt im Ermessen der Zertifikatnehmer und Zertifikatsnutzer, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

Die ausgestellten Sperrlisten müssen folgenden Anforderungen entsprechen:

- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

- [X.509] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)

7.2.1 Versionsnummer(n)

Zertifikatssperrlisten müssen im Format X.509 Version 2, welche die Anforderungen gemäß RFC 5280 erfüllt, ausgestellt werden.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

7.2.2.1 Erweiterung „Stellenschlüsselkennung “ (AuthorityKeyIdentifier)

Die Sperrlisten müssen die Erweiterung „Stellenschlüsselkennung“ (AuthorityKeyIdentifier) enthalten. Der Risikowert dieser Erweiterung ist als „nicht kritisch“ zu setzen.

7.2.2.2 Erweiterung „Sperrlistennummer“

Die Sperrlisten müssen die Erweiterung „Sperrlistennummer“ (cRLNumber) als fortlaufende Seriennummer der Sperrliste enthalten. Der Risikowert dieser Erweiterung ist als „nicht kritisch“ zu setzen.

7.3 OCSP-Profil

7.3.1 Versionsnummer(n)

Es MUSS OCSP V1 gemäß [RFC 6960] eingesetzt werden.

7.3.2 OCSP-Erweiterungen

Keine Vorgabe.

8 AUDITS UND ANDERE BEWERTUNGSKRITERIEN

Grundsätzlich gilt innerhalb der Hierarchie, dass die eingeschlossenen CAs gemäß einer Policy der ETSI EN 319 411-1 zertifiziert sein müssen oder vergleichbar.

Werden Teile der PKI durch Dritte betrieben, so müssen diese sich verpflichten, dass sowohl Audits durch die Deutsche Telekom Security GmbH oder einem Beauftragten als auch Audits externer Prüfstellen im Rahmen der Zertifizierung möglich und unterstützt werden.

8.1 Häufigkeit und Art der Prüfungen

Die eingeschlossenen CAs müssen regelmäßig durch interne Audits überprüft werden. Die Prüfung muss die Anforderungen an Betrieb und Personal und die Konformität zu diesem CP und den Anforderungen der Norm, die unter 8.4 angewendet wird, umfassen.

Es müssen regelmäßig Prüfungen bei Dritten durchgeführt werden, wenn Aufgaben an Dritte ausgelagert wurden.

Entsprechend der Anforderungen findet mindestens einmal jährlich eine Überprüfung der Zertifizierung durch eine akkreditierte Prüfstelle statt. Diese muss durch die eingeschlossenen CAs so beauftragt werden, dass ausreichend Zeit für die Überprüfung gegeben ist und kein Zeitraum ohne Zertifizierung entsteht.

Weiterhin müssen anlassbezogene Prüfungen durchgeführt werden, wenn dies durch z.B. Sicherheitsvorfälle notwendig wird.

Für Webserver-Zertifikate müssen quartalsmäßige interne Überprüfungen stattfinden. Hierbei wird mindestens eine 3% große Stichprobe aller im Beobachtungszeitraum erzeugten Zertifikate herangezogen und die Erfüllung der Anforderungen überprüft.

8.2 Identität/Qualifikation des Prüfers

Für interne Audits müssen fachkundige Prüfer (interner Auditor) eingesetzt werden, die über eine Ausbildung in der Durchführung von Audits und über langjährige Fachkunde in PKI-Technologie verfügen.

Die Prüfung der Konformität nach den oben genannten Standards muss durch eine akkreditierte Prüfstelle erfolgen. Die Zertifizierung muss durch eine akkreditierte Zertifizierungsstelle erfolgen.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Der Prüfer muss Mitarbeiter oder ein Beauftragter einer akkreditierten Prüfstelle sein. Die Prüfung muss entsprechend den Regelungen der ISO/IEC 17021 erfolgen.

Für interne Audits sollten fachkundige Prüfer (interner Auditor) eingesetzt werden, die ansonsten keine Funktion innerhalb der zu prüfenden CA übernehmen.

8.4 Abgedeckte Bereiche der Prüfung

Der Umfang der Prüfung wird durch den gewählten Standard bestimmt. Die internen Audits müssen die Einhaltung der Anforderungen des CA/Browserforums, des Root-Programms der Mozilla Foundation, des Sicherheitsmanagements und des gewählten Standards umfassen.

Die CA muss eine Auditierung nach (1) WebTrust for CAs v2.0 oder neuer und WebTrust for SSL Baseline with Network Security v2.2 oder neuer oder (2) ETSI EN 319 411-1 inkl. normativer Referenzen zur ETSI EN 319 401 oder (3) ETSI EN 319 411-2 inkl. normativer Referenzen zur ETSI EN 319 401 oder (4) im Falle einer Government CA auf Basis eines internen Auditierungsschemas, welches alle Anforderungen der oben genannten Standards oder vergleichbar erfüllt, durchführen.

Die Auditierung oder das Assessment müssen in regelmäßigen Abständen durchgeführt werden.

Die Durchführung muss durch einen qualifizierten Auditor erfolgen.

8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Die eingeschlossenen CAs müssen über Standardvorgehen für die Beseitigung von Mängeln und Defiziten verfügen. Es muss eine individuelle Risikoanalyse erstellt und dokumentiert werden. Es müssen Maßnahmen zur Beseitigung festgelegt und dokumentiert werden, so dass je nach möglichem Risiko eine Minimierung erreicht wird. Die Maßnahmen werden durch das Sicherheitsmanagement gemonitort und die Umsetzung überwacht.

8.6 Mitteilung der Ergebnisse

Die Konformität des Prüfgegenstandes mit den Anforderungen des Standards muss durch eine akkreditierte Zertifizierungsstelle in Form eines Zertifikats bestätigt werden. Eine Veröffentlichung des zugrundeliegenden Prüfberichtes muss nicht erfolgen, wenn das Ergebnis im Zertifikat referenziert wird.

Die relevanten Zertifikatsberichte müssen auf der Website des Trust Centers unter

https://www.telesec.de/de/trust-center

veröffentlicht werden Bei gesetzlichen Anforderungen müssen die Ergebnisse auch an die festgelegten Stellen kommuniziert werden. Die Zertifikate müssen spätestens 3 Monate nach Auditabschluß veröffentlicht werden.

8.7 Selbst-Auditierung

Es ist ein interner Audit-Prozess zur Sicherstellung der Einhaltung der CP/CPS Vorgaben umzusetzen.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BE-STIMMUNGEN

9.1 Entgelte

Die Gebühren sind in den jeweiligen Allgemeinen Geschäftsbedingungen (AGB) der Zertifizierungsstellen festzulegen.

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

Keine Vorgabe.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Keine Vorgabe.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

Keine Vorgabe.

9.1.4 Entgelte für andere Leistungen

Keine Vorgabe.

9.1.5 Erstattung von Entgelten

Keine Vorgabe.

9.2 Finanzielle Verantwortlichkeiten

Die finanziellen Verantwortlichkeiten sind in den jeweiligen Allgemeinen Geschäftsbedingungen (AGB) der Zertifizierungsstellen oder einzelvertraglich festzulegen.

9.2.1 Versicherungsschutz

Keine Vorgabe.

9.2.2 Sonstige finanzielle Mittel

Keine Vorgabe.

9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Keine Vorgabe.

9.3 Vertraulichkeit von Geschäftsinformationen

Die Behandlung von vertraulichen Geschäftsinformationen ist in den Richtlinien der Zertifizierungsstellen festzulegen. Es sind die einschlägigen gesetzlichen Bestimmungen sowie ggf. weiteren Regelungen zum Datenschutz zu beachten.

9.3.1 Umfang von vertraulichen Informationen

Keine Vorgabe.

9.3.2 Umfang von nicht vertraulichen Informationen

Keine Vorgabe.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Keine Vorgabe.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

Die Behandlung von personenbezogenen Daten ist in den Richtlinien der Zertifizierungsstellen in einem Datenschutzkonzept festzulegen.

9.4.1 Datenschutzkonzept

Keine Vorgabe.

9.4.2 Vertraulich zu behandelnde Daten

Keine Vorgabe.

9.4.3 Nicht vertraulich zu behandelnde Daten

Keine Vorgabe.

9.4.4 Verantwortung für den Schutz vertraulicher Daten

Keine Vorgabe.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Keine Vorgabe.

9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Keine Vorgabe.

9.4.7 Andere Umstände zur Offenlegung von Daten

Keine Vorgabe.

9.5 Urheberrecht

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von Telekom Security unzulässig. Die geistigen Eigentumsrechte an den Zertifikaten und der ARL verbleiben bei Telekom Security. Die Nutzungsrechte an den ausgegebenen Zertifikaten werden durch Einzelverträge mit den entsprechenden Zertifizierungsstellen ausgestaltet.

9.6 Zusicherungen und Gewährleistung

9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle (CA)

Durch Ausstellen eines Zertifikats übernimmt die CA die hier aufgeführten Zertifikatgewährleistungen gegenüber den folgenden Zertifikatberechtigten:

1. dem Abonnenten, der Partei unter der Abonnentenvereinbarung oder der Vereinbarung über die Nutzungsbedingungen für das Zertifikat ist,
2. allen Lieferanten für Anwendungssoftware, mit denen die Wurzel-CA einen Vertrag über die Einbeziehung ihres Wurzelzertifikats in die Software geschlossen hat, die von jenem Lieferanten für Anwendungssoftware vertrieben wird, und
3. allen vertrauenden Parteien, die sich angemessenerweise auf ein gültiges Zertifikat verlassen. Die CA sagt gegenüber den Zertifikatberechtigten zu und gewährleistet, dass die CA während des Zeitraums der Gültigkeit des Zertifikats diese Anforderungen und ihre Certificate Policy und/oder ihr Certification Practice Statement bei der Ausgabe und Verwaltung des Zertifikats befolgt.

Die Zertifikatgewährleistungen beinhalten insbesondere Folgendes, ohne jedoch darauf beschränkt zu sein:

1. Recht zur Nutzung des Domain-Namens oder der IP-Adresse: Zum Zeitpunkt der Ausgabe hat die CA (i) ein Verfahren implementiert, um zu verifizieren, dass der Antragsteller entweder das Recht hatte, den/die Domain-Namen und die IP-Adresse(n), die im Feld „subject“ und in der Erweiterung „subjectAltName“ des Zertifikats aufgeführt sind, zu nutzen, oder die dazugehörige Kontrolle besaß (oder, nur im Fall von Domain-Namen, mit einem solchen Recht oder einer solchen Kontrolle von einer Person mit dem Recht zur Nutzung oder der Kontrolle ausgestattet wurde), (ii) das Verfahren bei der Ausgabe des Zertifikats befolgt und (iii) das Verfahren in der Certificate Policy und/oder dem Certification Practice Statement der CA exakt beschrieben.
2. Autorisierung für das Zertifikat: Zum Zeitpunkt der Ausgabe hat die CA (i) ein Verfahren implementiert, um zu verifizieren, dass das Subjekt die Ausgabe des Zertifikats genehmigt hat, und dass der Bevollmächtigte des Antragstellers die Genehmigung besitzt, das Zertifikat im Namen des Subjekts zu beantragen, (ii) das Verfahren bei der Ausgabe des Zertifikats befolgt und (iii) das Verfahren in der Certificate Policy und/oder dem Certification Practice Statement der CA exakt beschrieben.
3. Genauigkeit der Informationen: Zum Zeitpunkt der Ausgabe hat die CA (i) ein Verfahren implementiert, um die Genauigkeit aller in dem Zertifikat enthaltenen Informationen zu verifizieren (mit Ausnahme des Attributs „subject:organizationalUnitName“), (ii) das Verfahren bei der Ausgabe des Zertifikats befolgt und (iii) das Verfahren in der Certificate Policy und/oder dem Certification Practice Statement der CA exakt beschrieben.
4. Keine irreführenden Informationen: Zum Zeitpunkt der Ausgabe hat die CA (i) ein Verfahren implementiert, um die Wahrscheinlichkeit zu reduzieren, dass die Informationen im Attribut „subject:organizationalUnitName “irreführend sind, (ii) das Verfahren bei der Ausgabe des Zertifikats befolgt und (iii) das Verfahren in der Certificate Policy und/oder dem Certification Practice Statement der CA exakt beschrieben.
5. Identität des Antragstellers: Wenn das Zertifikat Informationen zur Subjektidentität enthält, hat die CA zum Zeitpunkt der Ausgabe (i) ein Verfahren implementiert, um die Identität des Antragstellers gemäß den Abschnitten 3.2 und 11.2 zu verifizieren, (ii) das Verfahren bei der Ausgabe des Zertifikats befolgt und (iii) das Verfahren in der Certificate Policy und/oder dem Certification Practice Statement der CA exakt beschrieben.
6. Abonnentenvereinbarung: Wenn es sich bei der CA und dem Abonnenten nicht um verbundene Unternehmen handelt, sind der Abonnent und die CA Parteien einer rechtsgültigen und durchsetzbaren Abonnentenvereinbarung, die diese Anforderungen

erfüllt, oder wenn die CA und der Abonnent verbundene Unternehmen sind, hat der Bevollmächtigte des Antragstellers die Nutzungsbedingungen bestätigt und akzeptiert.
7. 24x7 Service: Die CA unterhält ein 24 x 7 öffentlich zugängliches Repository mit aktuellen Informationen über den Status (gültig oder widerrufen) aller nicht abgelaufenen Zertifikate. - und –
8. Entzug: Die CA wird das Zertifikat aus einem der in diesen Anforderungen genannten Gründe entziehen. Die Wurzel-CA WIRD für die Erfüllung und Gewährleistungen der untergeordneten CA, die Befolgung dieser Anforderungen durch die untergeordnete CA sowie für alle Verbindlichkeiten und Entschädigungspflichten der untergeordneten CA unter diesen Anforderungen haftbar, als wäre die Wurzel-CA die untergeordnete CA, die die Zertifikate ausgibt.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Keine Vorgabe.

9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Die CA WIRD, im Rahmen der Abonnentenvereinbarung oder der Vereinbarung über die Nutzungsbedingungen verlangen, dass der Abonnent die Zusagen und Gewährleistungen in diesem Abschnitt zugunsten der CA und der Zertifikatberechtigten übernimmt. Vor Ausgabe eines Zertifikats WIRD die CA, zugunsten der CA oder der Zertifikatberechtigten, Folgendes beschaffen, entweder:

1. die Zustimmung des Antragstellers zur Abonnentenvereinbarung mit der CA oder
2. die Zustimmung des Antragstellers zur Vereinbarung über die Nutzungsbedingungen.

Die CA WIRD ein Verfahren implementieren, um sicherzustellen, dass jede Abonnentenvereinbarung oder Vereinbarung über die Nutzungsbedingungen gegenüber dem Antragsteller rechtsgültig durchsetzbar ist. In jedem Fall MUSS die Vereinbarung für das Zertifikat gelten, das gemäß dem Zertifizierungsantrag ausgegeben wird. Die CA KANN eine elektronische oder „Click-through"-Vereinbarung verwenden, sofern die CA festgestellt hat, dass solche Vereinbarungen rechtlich durchsetzbar sind. Eine separate Vereinbarung KANN für jeden Zertifizierungsantrag verwendet werden, oder eine einzige Vereinbarung KANN verwendet werden, um mehrere zukünftige Zertifizierungsanträge und die resultierenden Zertifikate zu erfassen, solange jedes Zertifikat, das die CA an den Antragsteller ausgibt, eindeutig unter jene Abonnentenvereinbarung oder Vereinbarung über die Nutzungsbedingungen fällt.

Die Abonnentenvereinbarung oder Vereinbarung über die Nutzungsbedingungen MUSS Bestimmungen enthalten, die dem Antragsteller selbst die folgenden Pflichten und Gewährleistungen auferlegen (oder vom Antragsteller im Namen seines Auftraggebers oder Agenten unter einer Unterauftragnehmervereinbarung oder Vereinbarung über Hosting-Dienste übernommen werden):

1. Genauigkeit der Informationen: Eine Verpflichtung und Gewährleistung, jederzeit exakte und vollständige Informationen gegenüber der CA vorzulegen, sowohl im Zertifizierungsantrag als auch gemäß anderen Aufforderungen durch die CA in Verbindung mit der Ausgabe des Zertifikats/der Zertifikate, die von der CA bereitgestellt werden sollen.
2. Schutz des privaten Schlüssels: Eine Verpflichtung und Gewährleistung seitens des Antragstellers, alle angemessenen Maßnahmen zu ergreifen, um die ausschließliche Kontrolle des privaten Schlüssels, der dem öffentlichen Schlüssel entspricht, der in das/die beantragte(n) Zertifikat(e) einbezogen werden soll, (und aller dazugehörigen

Aktivierungsdaten oder -geräte, z. B. Kennwörter oder Tokens), seine Geheimhaltung und seinen ordnungsgemäßen Schutz jederzeit zu wahren.

3. Zertifikatakzeptanz: Eine Verpflichtung und Gewährleistung, dass der Abonnent den Inhalt des Zertifikats auf Genauigkeit prüft und verifiziert.
4. Verwendung des Zertifikats: Eine Verpflichtung und Gewährleistung, das Zertifikat nur auf Servern zu installieren, die unter dem/den im Zertifikat aufgeführten „subjectAltName(s)“ zugänglich sind, und das Zertifikat ausschließlich gemäß allen geltenden Gesetzen und nur im Einklang mit der Abonnentenvereinbarung oder Vereinbarung über die Nutzungsbedingungen zu verwenden.
5. Berichterstattung und Entzug: Eine Verpflichtung und Gewährleistung, die Verwendung eines Zertifikats und des dazugehörigen privaten Schlüssels unverzüglich aufzugeben und die CA umgehend aufzufordern, das Zertifikat zu entziehen, sofern einer der folgenden Umstände eintritt: (a) Informationen in dem Zertifikat sind oder werden unzutreffend oder ungenau, oder (b) es liegt ein tatsächlicher oder mutmaßlicher Missbrauch oder eine Gefährdung des privaten Schlüssels des Abonnenten vor, der mit dem in das Zertifikat einbezogenen öffentlichen Schlüssel verbunden ist.
6. Beendigung der Verwendung des Zertifikats: Eine Verpflichtung und Gewährleistung, jede Verwendung des privaten Schlüssels, der mit dem in das Zertifikat einbezogenen öffentlichen Schlüssel verbunden ist, nach Entzug jenes Zertifikats aufgrund von Schlüsselgefährdung unverzüglich aufzugeben.
7. Reaktionsbereitschaft: Eine Verpflichtung, auf die Anweisungen der CA bezüglich einer Schlüsselgefährdung oder eines Zertifikatmissbrauchs innerhalb der genannten Frist zu reagieren.
8. Bestätigung und Akzeptanz: Eine Bestätigung und Akzeptanz, dass die CA berechtigt ist, das Zertifikat unverzüglich zu entziehen, wenn der Antragsteller die Bestimmungen der Abonnentenvereinbarung oder der Vereinbarung über die Nutzungsbedingungen verletzt hat, oder wenn die CA feststellt, dass das Zertifikat verwendet wird, um strafbare Handlungen, wie etwa Phishing, Angriffe, Betrug oder Verbreitung von Malware, zu ermöglichen.

9.6.4 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

Keine Vorgabe.

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Keine Vorgabe.

9.7 Haftungsausschluss

Keine Vorgabe.

9.8 Haftungsbeschränkungen

Die Zertifizierungsstellen können ihre Haftung gegenüber Dritten beschränken Diese Haftungsbeschränkungen sind im CP/CPS der Zertifizierungsstelle zu beschreiben.

9.9 Schadensersatz

Keine Vorgabe.

9.9.1 Schadenersatz durch die CAs

Keine Vorgabe.

9.9.2 Schadenersatz durch die Endteilnehmer

Keine Vorgabe.

9.9.3 Schadenersatz durch beteiligte Parteien

Keine Vorgabe.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Dieses Dokument tritt mit der Veröffentlichung auf den Telekom Security Webseiten in Kraft. Änderungen treten ebenfalls mit der Veröffentlichung auf den öffentlichen Webseiten (siehe Kapitel 2.3) in Kraft.

9.10.2 Beendigung

Dieses Dokument bleibt in der jeweils gültigen Version in Kraft, bis sie durch eine neue Version ersetzt wird.

9.10.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung des Telekom Security PKI Dienstes bleiben alle Benutzer an die in der CP/CPS enthaltenen Regelungen gebunden, bis das letzte ausgegebene Zertifikat seine Gültigkeit verliert oder gesperrt wird.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Vorgabe.

9.12 Änderungen

Keine Vorgabe.

9.12.1 Verfahren für Änderungen

Keine Vorgabe.

9.12.2 Benachrichtigungen über Änderungen

Keine Vorgabe.

9.12.3 Gründe zur Vergabe einer neuen OID

Keine Vorgabe.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Keine Vorgabe.

9.14 Geltendes Recht

Keine Vorgabe.

9.15 Einhaltung geltenden Rechts

Keine Vorgabe.

9.16 Verschiedene Bestimmungen

9.16.1 Vollständiger Vertrag

Keine Vorgabe.

9.16.2 Abtretung

Keine Vorgabe.

9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieses Dokuments unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser Erklärung im Übrigen nicht. Statt der unwirksamen und undurchführbaren Bestimmung gilt eine solche Bestimmung als vereinbart, die dem wirtschaftlichen Zweck dieses Dokuments in rechtswirksamer Weise am nächsten kommt. Das Gleiche gilt für die Ergänzung etwaiger Vertragslücken.

9.16.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Keine Vorgabe.

9.16.5 Höhere Gewalt

Keine Vorgabe.

9.17 Sonstige Bestimmungen

Keine Vorgabe.