Telekom Security PKI – Certificate Practice Statement

Erklärung zum Zertifizierungsbetrieb für 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 - Dokumenteneigenschaften

Eigenschaft	Wert
Herausgeber	Deutsche Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Deutschland
Dateiname	Telekom-Security-PKI-CPS-DE-v12.00-20200605.docx
Gültig ab	01.07.2020
Titel	Telekom Security PKI – Certificate Practice Statement Erklärung zum Zertifizierungsbetrieb für Telekom Security Trust Center Public Key Infrastruktur
Version	12.00
Letztes Review	05.06.2020
Status	Freigabe
Ansprechpartner	Telekom Security Leiter Trust Center Betrieb
Kurzbeschreibung	Erklärung zum Zertifizierungsbetrieb für die Root CAs

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 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	Einarbeitung 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

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

1 EINLEITUNG

1.1 Überblick

Die Trust Center Public Key Infrastruktur (PKI) wird durch die Konzerneinheit Deutsche Telekom Security GmbH in der Deutschen Telekom AG im DT Security 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 Erklärung zum Zertifizierungsbetrieb (engl. Certification Practise Statement, kurz CPS) für alle innerhalb der DT 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 DT Security PKI alle Anforderungen und Regelungen der jeweils aktuellen veröffentlichten Version der [CAB-BR] (http://www.cabforum.org/documents.html) erfüllen und einhalten. 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	Datum	Objektbezeichnung (Object Identifier)
Telekom Security PKI – Certificate Practice Statement	12.00	01.07.2020	1.3.6.1.4.1.7879.13.39

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, die unter den folgenden öffentlichen Stammzertifizierungsstellen (Root-CAs) betrieben werden:

Deutsche Telekom Root CA 2

Key: RSA 2048, SHA-1

Serial#: 26

Thumbprint: 85:a4:08:c0:9c:19:3e:5d:51:58:7d:cd:d6:13:30:fd:8c:de:37:bf

Valid until: 10. Juli 2019

T-TeleSec GlobalRoot Class 2

Key: RSA 2048, SHA-256

Serial#: 01

Thumbprint: 59:0d:2d:7d:88:4f:40:2e:61:7e:a5:62:32:17:65:cf:17:d8:94:e9

Valid until: 2. Oktober 2033

T-TeleSec GlobalRoot Class 3

Key: RSA 2048, SHA-1

Serial#: 01

Thumbprint: 55:a6:72:3e:cb:f2:ec:cd:c3:23:74:70:19:9d:2a:be:11:e3:81:d1

Valid until: 2. Oktober 2033

TeleSec GlobalRoot Class 1 G3

Key: ECDSA_P384, sha384ECDSA

Serial#: 1a:f8:94:c5:45:27:c2:c5:68:25:b8:a9:31:5c:bf:da

Thumbprint: 52 7f 0d 83 1b 02 bd 85 a6 8b f6 db 23 f6 e7 0d e2 f8 a0 20

Valid until: 10. April 2044

TeleSec GlobalRoot Class 2 G3

Key: ECDSA_P384, sha384ECDSA

Serial#: 08:22:70:67:e1:16:f6:90:56:ef:0b:fe:fb:bd:d9:91

Thumbprint: 63 2e 29 d7 8a 73 ab 29 5f 50 84 35 a5 f0 6a 7e f6 55 d9 81

Valid until: 10. April 2044

TeleSec GlobalRoot Class 3 G3

Key: ECDSA_P384, sha384ECDSA

Serial#: 2b:d4:0e:3e:f9:1f:9a:c5:f9:19:af:04:24:6c:7e:fb

Thumbprint: 46 3c 28 b0 b9 41 91 a6 23 38 aa dc db 79 b4 46 ca 97 a9 e9

Valid until: 10. April 2044

Die Root-CA Zertifikate sind vom Trust Center selbst-signiert und werden durch DT Security veröffentlicht. Die Veröffentlichung erlaubt eine lückenlose Gültigkeitsüberprüfung aller in dieser Hierarchie ausgestellten Zertifikate. Es werden ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen (Sub-CAs) ausgestellt. Zertifikate für Endteilnehmer (Subscriber Zertifikate) werden nicht ausgegeben. Regelungen bzgl. Endteilnehmer-Zertifikaten werden in separaten CPS weiterer DT Security Zertifikatslösungen beschrieben.

1.3.2 Registrierungsstellen (RA)

Registrierungen und alle damit zusammenhängenden Aktivitäten für die in diesem CPS aufgeführten Root-CAs werden durch eine zentrale interne Registrierungsstelle der DT Security bearbeitet. Es werden weder weitere externe noch interne Registrierungsstellen (RA) hinzugezogen.

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)

Zertifikatsnutzer sind juristischen Personen bzw. Organisationseinheiten, die auf die Integrität und Qualität eines ausgestellten Endteilnehmer Zertifikates vertrauen.

1.3.5 Andere Teilnehmer

Nicht anwendbar.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Siehe CP, Kapitel 1.4.1

1.4.2 Unzulässige Verwendung von Zertifikaten

Siehe CP, Kapitel 1.4.2

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

1.5.3 Pflege der Richtlinie und Konformität des CPS

Dieses Dokument (CPS) 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 Dokument (CP)

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

Die vorliegende CPS 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 CPS 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.
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).

Begriff	Erläuterung
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 DT 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.
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.

Begriff	Erläuterung
ETSI-Zertifizierung	Überprüfung und Bestätigung für Zertifizierungsstellen durch einen unabhängigen Gutachter, dass 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.
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 DT 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.

Begriff	Erläuterung
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.
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

Begriff	Erläuterung
	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.
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.
Registrierungsstelle eines Unternehmens (Enterprise RA)	Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der nicht der Zertifizierungsstelle (CA) angegliedert ist (non Affiliate), der die Ausstellung von Zertifikaten für diese Organisation genehmigt. Diese Rollen (Trusted Roles) können z.B. vom Master- und Sub-Registrator des Mandanten bzw. Bevollmächtigten wahrgenommen werden.

Begriff	Erläuterung
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.
Schlüsselkompromittierung	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 ausfindig 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.
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 Zertifikatsnhemers 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

Begriff	Erläuterung
	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.
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.

Begriff	Erläuterung
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.
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.
Zertifikatsproblembericht	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.

Begriff	Erläuterung
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
CARL	Certification Authority Revocation List (siehe ARL)
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

Überschrift	Definition
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
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

Kürzel	Referenz
[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

Nicht anwendbar.

2 VERÖFFENTLICHUNG UND VERANTWORTLICHKEIT FÜR INFORMATIONEN (REPOSITORIES)

Veröffentlichung und Verantwortlichkeit für Informationen (Repositories)

2.1 Informationsdienste (Repositories)

Es werden die folgenden Informationsdienste innerhalb der PKI unterschieden:

- OCSP
- ARL oder auch CARL
- CP und CPS
- Sonstige

2.2 Veröffentlichung von Zertifikaten und zugehörigen Informationen

DT Security stellt die ARL und OCSP-Auskünfte den PKI-Beteiligten 7 X 24h online-zur Verfügung.

OCSP

Über das Online Certificate Status Protocol (OCSP) kann der Status eines Zertifikats abgefragt werden. Dazu wird der Zertifikatsstatus über eine definierte Schnittstelle öffentlich zugänglich gemacht.

CRL

Das Trust Center stellt den Zertifikatsnutzern der PKI im Internet eine öffentlich erreichbare CRL zur Verfügung.

CP und CPS

Die Internetpräsenz des Trust Centers ist unter http://www.telesec.de/pki/index.html zu erreichen. Die CP und die CPS sind unter https://www.telesec.de/de/trust-center veröffentlicht.

Sonstige Informationen

Zusätzlich stellt das Trust Center den Zertifikatsnutzern der PKI folgende Informationen auf der Internetpräsenz zur Verfügung:

- das Root-CA Zertifikat und dessen Fingerprint SHA1/SHA-256
- Information über den Wechsel eines Root-CA oder eines Sub-CA-Zertifikats
- Informationen über eine Kompromittierung, den Verdacht auf Kompromittierung oder die Sperrung eines Root-CA- oder Sub-CA-Zertifikats

2.3 Zeitpunkt oder Intervall der Veröffentlichung

Sperrinformationen für Root-CA- und CA-Zertifikate werden im Fall einer Sperrung aktualisiert (CRL, OCSP-Responder) CP und CPS und ggf. weitere Informationen werden auf den Internetseiten https://www.telesec.de zur Verfügung gestellt.

OCSP

Vor der Nutzung der Zertifikate stehen die Informationen für OCSP Anfragen zur Verfügung.

Aktualisierung der ARL / CARL

Siehe 4.9.7

CP und CPS

Dieses Dokument und das zugehörige CP werden mindestens einmal im Jahr einem Review unterzogen.

Bei relevanten Änderungen der im CP/CPS beschriebenen Anforderungen, Erklärungen, Maßnahmen oder Prozeduren ist das jeweilige Dokument zeitnah zu aktualisieren.

2.4 Zugang zu den Informationsdiensten

Die benannten öffentlichen Informationsspeicher sind mit lesendem Zugriff berechtigt und unterliegen keiner gesonderten Zugangskontrolle.

Der schreibende Zugriff auf alle in Kapitel 2.2 genannten Informationen erfolgt ausschließlich durch berechtigte Mitarbeiter bzw. autorisierte Systeme des Trust Centers.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

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

3.1.1 Namensformen

Die Namensregeln für den „SubjectDistinguishedName“ (Subject DN) und „IssuerDistinguishedName“ (Issuer DN) sind nach dem X.501-Standard definiert und enthalten Felder der folgenden Attribute:

- Country (C)
- Organization (O)
- Organizational Unit (OU)
- State or Province (S)
- Locality (L)
- Common Name (CN)
- E-mail Address (E)
- Subject Alternative Name (SAN)

3.1.2 Aussagekraft von Namen

Der Name im „SubjectDistinguishedName“ (CN) sowie „SubjectAlternativeName“ (SAN) identifiziert den Zertifikatsnehmer eindeutig. Es werden auch zulässige Abkürzungen des z.B. im Handelsregister eingetragenen Namens verwendet.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Es werden keine anonymen oder pseudonymen Zertifikatsdaten verwendet.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Nicht anwendbar bzw. keine Regelungen.

3.1.5 Eindeutigkeit von Namen

Die Vorgaben aus dem entsprechenden Kapitel im CP werden erfüllt.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Die Vorgaben aus dem entsprechenden Kapitel im CP werden erfüllt.

3.2 Identitätsprüfungen bei Erstbeauftragung

Nicht anwendbar.

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Nicht anwendbar.

3.2.2 Prüfung der Organisations- und Domain-Identität

Die Vorgaben aus dem entsprechenden Kapitel im CP werden erfüllt.

3.2.2.1 Identität

Siehe CP, Kapitel 3.2.2

3.2.2.2 Firmierung/Handelsname

Siehe CP, Kapitel 3.2.2

3.2.2.3 Überprüfung der Länderkennung

Siehe CP, Kapitel 3.2.2

3.2.2.4 Überprüfung der Berechtigung oder der Kontrolle über die Domain

Nicht anwendbar.

3.2.2.4.1 Überprüfung, ob der Auftraggeber der Domain Kontakt ist

Nicht anwendbar.

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

Nicht anwendbar.

3.2.2.4.3 Telefonischer Kontakt zum Domain Kontakt

Nicht anwendbar.

3.2.2.4.4 Konstruierte E-Mail zum Domain Kontakt

Nicht anwendbar.

3.2.2.4.5 Domainvollmacht

Nicht anwendbar.

3.2.2.4.6 Vereinbarte Änderung auf der Webseite

Nicht anwendbar.

3.2.2.4.7 Änderung im DNS

Nicht anwendbar.

3.2.2.4.8 IP Addresse

Nicht anwendbar.

3.2.2.4.9 Testzertifikat

Nicht anwendbar.

3.2.2.4.10 TLS unter Verwendung einer Zufallszahl

Nicht anwendbar.

3.2.2.4.11 Beliebige andere Methode

Nicht anwendbar.

3.2.2.4.12 Validierung eines Antragstellers als Domain Kontakt

Nicht anwendbar.

3.2.2.4.13 E-Mail an einen DNS CAA Kontakt

Nicht anwendbar.

3.2.2.4.14 E-Mail an einen DNS TXT Kontakt

Nicht anwendbar.

3.2.2.4.15 Telefonischer Kontakt mit dem Domain Kontakt

Nicht anwendbar.

3.2.2.4.16 Telefonischer Kontakt mit dem DNS TXT Record Telefonkontakt

Nicht anwendbar.

3.2.2.4.17 Telefonischer Kontakt mit dem DNS CAA Record Telefonkontakt

Nicht anwendbar.

3.2.2.5 Authentifizierung für eine IP Addresse

Nicht anwendbar.

3.2.2.5.1 Abgestimmte Änderung an einer Webseite

Nicht anwendbar.

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

Nicht anwendbar.

3.2.2.5.3 Adressauflösung (Reverse Address Lookup)

Nicht anwendbar.

3.2.2.5.4 Andere Methoden

Nicht anwendbar.

3.2.2.5.5 Telefonischer Kontakt mit IP Adressen-Kontakt

Nicht anwendbar.

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

Nicht anwendbar.

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

Nicht anwendbar.

3.2.2.6 Überprüfen einer Wildcard Domain

Nicht anwendbar

3.2.2.7 Zuverlässigkeit der Datenquelle

Siehe CP, Kapitel 3.2.2

3.2.2.8 CAA Records

Nicht anwendbar.

3.2.3 Authentifizierung einer natürlichen Person

Die Vorgaben aus dem entsprechenden Kapitel im CP werden erfüllt.

3.2.4 Nicht verifizierte Teilnehmerinformationen

Alle von DT Security ausgestellten Root- und Sub-CA Zertifikate beinhalten keine ungeprüften Subjekt-Informationen.

3.2.5 Überprüfung der Berechtigung

Die Vorgaben aus dem entsprechenden Kapitel im CP werden erfüllt.

3.2.6 Kriterien für Interoperabilität

Die Vorgaben aus dem entsprechenden Kapitel im CP werden erfüllt.

3.3 Identitätsprüfung und Authentifizierung bei einer Schlüsselerneuerung

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Nicht anwendbar.

3.3.2 Identitätsprüfung bei Schlüsselerneuerung nach Zertifikatssperrung

Nicht anwendbar.

3.4 Identifizierung und Authentifizierung bei Sperranträgen

Das Trust Center bietet den Zertifikatsnehmern einen zentralen Sperrservice, um im Falle des Verlustes oder bei Missbrauchsverdacht das eigene Zertifikat sperren zu können. Die Authentisierung einer Sperrung geschieht durch die Angabe der Grunddaten (Name, Firma, Rückrufnummer, E-Mailadresse). Der Sperrwunsch wird durch die Angabe des Sperrpasswortes autorisiert.

Zur Sperrung autorisierte Personen und Institutionen können die Sperrung eines Zertifikates entweder per E-Mail oder telefonisch beauftragen. Im Falle der Sperrung wird das Zertifikat in eine Sperrliste aufgenommen, sowie bei OCSP Anfragen als gesperrt gemeldet.

4 BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsbeauftragung

Die Ausstellung von Root-CA-, SubCA- und Dienstezertifikaten (z.B. OCSP) unterliegen aufgrund der Kritikalität besonderen Prozessen und Prüfungen. Diese werden im Folgenden beschrieben:

4.1.1 Wer kann ein Zertifikat beauftragen?

Eine Beantragung kann ausschließlich von einem Bevollmächtigten der jeweiligen Antragsstellerorganisation erfolgen. Die Zertifikate werden ausschließlich an juristische Personen ausgestellt.

4.1.2 Beauftragungsprozess und Zuständigkeiten

Das Antragsverfahren erfolgt je nach Zertifikat in folgenden Schritten:

Root-CA

- Auftrag des Managements
- Beteiligung der Prüf- und Zertifizierungsstelle ETSI
- Prüfung des Auftrages durch den Operator
- Freigabe zur Zertifizierung durch den Operator
- Kontrolle der Hardware
- Generierung des Schlüsselpaares
- Erzeugung des Self-Signed-Zertifikates
- Abnahme durch Prüf- und Zertifizierungsstelle ETSI
- Ablage und spätere Archivierung der Unterlagen

Sub-CA / Cross

- Vertragsschluß bei Dritten oder Managementauftrag
- Erstellung des Zertifikatsauftrages
- Erstellung der Schlüssel und Beifügung der Anfrage inkl. öffentlichem Schlüssel
- Prüfung des Auftrags durch den Operator
- Kontrolle der Schlüssellieferung
- Freigabe zur Zertifizierung durch den Operator
- Zertifikatserstellung und Übergabe
- Ablage und spätere Archivierung der Unterlagen

Dienstezertifikate

- Erstellung des Zertifikatsauftrages
- Erstellung der Schlüssel und Beifügung der Anfrage inkl. öffentlichem Schlüssel
- Prüfung des Auftrags durch den Operator
- Kontrolle der Schlüssellieferung
- Freigabe zur Zertifizierung durch den Operator
- Zertifikatserstellung und Übergabe
- Ablage und spätere Archivierung der Unterlagen

4.2 Bearbeitung des Zertifikatsauftrags

4.2.1 Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung wird im Rahmen des Registrierungsprozesses durchgeführt und beinhaltet mindestens die folgenden Schritte:

- Abgeschlossener Vertrag liegt bei Beauftragung durch einen Dritten vor.
- Ausgefülltes, aktuelles Auftragsformular in elektronischer Form oder als Papierformular. Das Antragsformular muss von einem Bevollmächtigten des Auftragsgebers elektronisch oder handschriftlich unterschrieben sein.
- Prüfung des Zertifikatsauftrags auf Berechtigung des Unterschreibenden. Weiterhin Prüfung der Vollständigkeit und Prüfung der Unterschrift.
- Bei einer SubCA muss das dienstespezifische CPS vorgelegt werden.
- ggf. Vorlage weiterer Dokumente z.B. Unterlagen der Prüf- und Zertifizierungsstelle über eine erfolgreiche Zertifizierung gemäß der geforderten Standards oder eine Teilbestätigung und die spätere Nachlieferung des Zertifikates.
- Prüfung und Freigabe dienstespezifisches CPS
- Nachweis des Besitzes des privaten Schlüssels gemäß Kapitel 3.2.1 und Prüfung des Request.

Alle Prozessschritte werden dokumentiert und durch den Bearbeiter signiert.

4.2.2 Annahme oder Abweisung von Zertifikatsanträgen

Nur bei erfolgreicher Überprüfung wird ein Zertifikatsauftrag autorisiert und die Produktion vorbereitet.

Im Falle einer Abweisung des Auftrags wird der Zertifikatsnehmer in geeigneter Weise unter Angabe von Gründen benachrichtigt und es werden Maßnahmen mit dem Auftraggeber vereinbart, um die Mängel zu beseitigen und den Prozess weiterzuführen.

4.2.3 Bearbeitungsdauer

Die Bearbeitung des Zertifikatauftrags beginnt innerhalb eines angemessenen Zeitraums nach Erhalt der Beauftragung. Sofern keine Bearbeitungsdauer einzelvertraglich festgelegt ist, gibt es keine Bestimmungen für die Bearbeitungsdauer eines Auftrags.

4.3 Ausstellung von Zertifikaten

4.3.1 CA-Tätigkeiten während der Ausstellung von Zertifikaten

Eine Freigabe ist die Voraussetzung für die Produktion eines Zertifikates durch die Root-CA. Eine CAA-Prüfung findet für Zertifikate der Root-CA nicht statt. Der zuständige Operator dokumentiert die Prozessschritte und lädt den Request auf einen Datenträger. Die Produktion erfolgt ausschließlich im 4-Augenprinzip und so können zwei Rolleninhaber dann das gewünschte Zertifikat produzieren.

Bei der Produktion von neuen Root-Zertifikaten werden die Prüfstelle bzw. die Zertifizierungsstelle als Zeugen beteiligt. Eine Teilnahme eines Kundenvertreters als Gast kann ebenfalls erfolgen.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung von Zertifikaten

Der Zertifikatsauftraggeber wird nach der Produktion informiert und erhält das Zertifikat zur Überprüfung.

4.4 Zertifikatsannahme

Vor der Veröffentlichung wird das produzierte Zertifikat an den Zertifikatsnehmer gesandt, um auf korrekte Inhalte und korrekte Kodierung geprüft zu werden.

4.4.1 Akzeptanz durch den Zertifikatsnehmer

Vom Antragsteller ist eine Annahmebestätigung innerhalb von 7 Tagen an das Trust Center erforderlich.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die Root-CA und Sub-CA-Zertifikate werden nach Annahme auf den Webseiten des Trust Centers http://www.telesec.de veröffentlicht.

4.4.3 Benachrichtigung weiterer Instanzen durch die CA

Es erfolgt keine explizite Benachrichtigung weiterer Instanzen. Nach der Produktion eines neuen Sub-CA-Zertifikates wird das Zertifikat in die Zertifikatsdatenbank CCADB https://www.ccadb.org eingestellt.

4.5 Verwendung von Schlüsselpaar und Zertifikat

Die Root-CA stellt ausschließlich Zertifikate für sich selbst, für nachgelagerte CAs (Subordinated CA) und Dienstezertifikate aus.

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die im Rahmen dieses CPS ausgestellten Zertifikate werden ausschließlich für Zertifizierungsstellen ausgestellt und dürfen nur dort genutzt werden.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Relying Parties

Die vertrauenden Dritten dürfen Zertifikate der Root-CA nur verwenden, wenn

- kompatible Software zu den verwendeten Standards und Gültigkeitsmodellen verwendet wird, und
- vor der Nutzung eines Zertifikats dessen Gültigkeit nach dem angewendeten Gültigkeitsmodell überprüft wird, und
- das Zertifikat ausschließlich für autorisierte und legale Zwecke eingesetzt wird.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Weder bei der Erzeugung von Root-CA-Zertifikaten oder Sub-CA-Zertifikaten oder Dienstezertifikate ist eine Zertifikatserneuerung vorgesehen. Aus diesem Grund enthält dieser Abschnitt keine Bestimmungen.

4.6.1 Bedingungen für eine Zertifikatserneuerung

Nicht anwendbar.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Nicht anwendbar.

4.6.3 Ablauf der Zertifikatserneuerung

Nicht anwendbar.

4.6.4 Benachrichtigung des Zertifikatsnehmers

Nicht anwendbar.

4.6.5 Annahme einer Zertifikatserneuerung

Nicht anwendbar.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Nicht anwendbar.

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung durch die CA

Nicht anwendbar.

4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

Weder bei der Erzeugung von Root-CA-Zertifikaten oder Sub-CA-Zertifikaten oder Dienstezertifikaten ist eine Schlüsselerneuerung vorgesehen. Aus diesem Grund enthält dieser Abschnitt keine Bestimmungen.

4.7.1 Bedingungen für eine Schlüsselerneuerung

Nicht anwendbar.

4.7.2 Wer darf eine Zertifizierung eines neuen öffentlichen Schlüssels beauftragen?

Nicht anwendbar.

4.7.3 Ablauf der Schlüsselerneuerung

Nicht anwendbar.

4.7.4 Benachrichtigung eines Zertifikatsauftraggers über das neue Zertifikat

Nicht anwendbar.

4.7.5 Annahme eines neuen Zertifikats

Nicht anwendbar.

4.7.6 Veröffentlichung des neuen Zertifikats durch die CA

Nicht anwendbar.

4.7.7 Benachrichtigung weiterer Instanzen über eine Schlüsselerneuerung

Nicht anwendbar.

4.8 Änderung von Zertifikatsdaten

Eine Änderung von Zertifikatsdaten ist nicht Teil des Zertifikatslebenszyklus der Zertifikate die diesem CPS unterliegen. Sollte eine Anpassung notwendig werden, so wird dies dokumentiert und ein neuer Zertifikatsrequest bzw. -auftrag generiert. Aus diesem Grund enthält dieser Abschnitt keine Bestimmungen.

4.8.1 Bedingungen für eine Zertifikatsdatenänderung

Nicht anwendbar.

4.8.2 Wer darf eine Änderung der Zertifikatsdaten beauftragen?

Nicht anwendbar.

4.8.3 Ablauf der Änderung von Zertifikatsdaten

Nicht anwendbar.

4.8.4 Benachrichtigung eines Zertifikatsauftraggebers über Ausgabe eines neuen Zertifikats

Nicht anwendbar.

4.8.5 Annahme des geänderten Zertifikats

Nicht anwendbar.

4.8.6 Veröffentlichung einer Schlüsselerneuerung

Nicht anwendbar.

4.8.7 Benachrichtigung weiterer Instanzen über das geänderte Zertifikat

Nicht anwendbar.

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.

4.9.1 Sperrgründe

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

Nicht anwendbar.

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 sich zentrale Informationen im Zertifikat geändert haben.
6. 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.
7. Die Herausgeber-CA entscheidet, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist.
8. 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.
9. 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.
10. Die Herausgeber-CA hat den Verdacht, dass der eigene private Schlüssel kompromittiert wurde.
11. Die CP oder CPS der herausgebenden CA sieht eine Sperrung vor.
12. Die Herausgeber-CA sollte ein Zertifikat nach einer Evaluierungszeit oder einem gesetzten Zeitpunkt sperren, wenn ein oder mehrere der folgenden Gründe vorliegt:
13. Gesetzliche Vorschriften oder richterliche Urteile oder eine Weisung einer aufsichtsführenden Behörde liegt vor.

4.9.2 Wer kann eine Sperrung beauftragen?

Wenn die CA selbst oder der Zertifikatsnehmer Informationen erlangen, die einen der im vorherigen Kapitel genannten Sperrgründe darstellt, muss eine Sperrung veranlasst werden. Diese muss durch die CA selbst ggf. nach Rücksprache mit dem Zertifikatsnehmer durchgeführt oder durch den Zertifikatsnehmer veranlasst werden.

Eine Sperrung kann außerhalb der zwingenden Sperrgründe nur durch den Zertifikatsnehmer selbst oder einen Bevollmächtigten erfolgen. Da der Zertifikatsnehmer hier i.d.R. eine juristische Person ist, muss die Vollmacht nachgewiesen werden.

4.9.3 Ablauf einer Sperrung

Die Sperrung eines Sub-CA-Zertifikates kann durch autorisierte Personen entweder per signierter E-Mail 7x24h oder schriftlich beauftragt werden. Aufgrund der Kritikalität sollte vorher eine telefonische Kontaktaufnahme erfolgen, bei welcher auch Verdachtsmomente adressiert

werden können. Kontaktinformationen befinden sich online unter www.telesec.de bzw. in Kapitel 1.5.2.

Sind die Voraussetzungen zur Sperrung (Berechtigung und Grund) erfüllt, wird die Sperrung vorgenommen, und das gesperrte Zertifikat in die Sperrinformationen übernommen. Die Sperrinformationen werden in standard-konformer Form (ARL) bereitgestellt.

Die autorisierte Person oder Institution werden über die Durchführung der Sperrung informiert.

4.9.4 Fristen für einen Sperrauftrag

Die CA und der Zertifikatsnehmer müssen bei Vorliegen entsprechender Gründe unverzüglich die Sperrung initiieren.

4.9.5 Fristen für 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 1.5.2 geforderten Fristen für eine Sperrung nicht überschreiten. Bei der Festlegung des Sperrdatums sind folgende Punkte zu berücksichtigen:

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

Im Zuge der Sperrung muss durch die beteiligte CA innerhalb einer Woche ein Incidentreport erstellt und an die Root-CA übermittelt werden. Diese prüft den Report entsprechend.

4.9.6 Methoden zur Prüfung von Sperrinformationen durch Relying Parties

Sperrinformationen für die ausgestellten Zertifikate der Root-CA werden in standardisierter Form (ARL) im DER–Format bereitgestellt und können daher mit standardkonformen Anwendungen geprüft werden. Weiterhin kann der Sperrstatus über eine OCSP-Anfrage festgestellt werden.

4.9.7 Frequenz der Veröffentlichung von Sperrinformationen

Die Sperrinformationen der Root-CA werden in standardisierter Form (ARL) alle 6 Monate aktualisiert und zur Verfügung gestellt. Wird innerhalb dieser 6 Monate ein für die Liste relevantes Zertifikat gesperrt, erfolgt ereignisbezogen zu diesem Zeitpunkt die Ausstellung einer neuen ARL.

Im Fall der Sperrung eines Sub-CA-Zertifikats erfolgt die Sperrung innerhalb von 24 Stunden nach der Sperrung. Der Wert für das nächste Update (next Update) Feld darf nicht länger als 12 Monate von dem aktuellen Update Datum entfernt gesetzt werden.

Da Cross-Zertifikate verwendet werden, wird mindestens alle 31 Tage eine ARL erzeugt.

Ein Eintrag wird NICHT aus der CRL entfernt, 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 Sperrlisten stehen innerhalb einer wirtschaftlich angemessenen Zeit nach der Generierung im Verzeichnisdienst zur Verfügung. Die Latenzzeit für die ARL beträgt maximal 5 Tage.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

DT Security betreibt einen OCSP-Responder um die Gültigkeit ausgestellter Root-CA und Sub-CA-Zertifikate zu validieren.

Sowohl die Sperrlisten als auch der OSCP-Dienst werden 7x24h bereitgestellt. Es stehen Online-Informationen zum Zertifikatsstatus via OCSP unter http://ocsp.telesec.de/ocspr bereit.

Die OCSP-Antworten entsprechen den Vorgaben des RFC 6960.

4.9.10 Anforderungen an Online Überprüfungsverfahren

Vertrauende Dritte müssen den Status eines Zertifikats überprüfen können, um Informationen darüber zu erhalten, ob ein Zertifikat, dem sie vertrauen möchten, gültig ist. Für den Abruf aktueller Statusinformationen steht der OCSP-Service (OCSP-Responder) zur Verfügung (siehe Kapitel 4.9.9). Dieser wird konform zur RFC 6960 und/oder RFC 5019 bereitgestellt.

Die Root-CA aktualisiert die OCSP-Datenbank mindestens alle zwölf Monate (12) oder innerhalb von vierundzwanzig (24) Stunden nach einer Sperrung.

Die von Sub-CAs für Subscriber-Zertifikate bereitgestellten OCSP-Informationen werden min. alle vier (4) Tage aktualisiert. OCSP-Antworten haben maximal eine Gültigkeit von 10 Tagen.

Der OCSP-Responder gibt Rückmeldungen zum Status, liefert aber keinen „good“-Status für den Fall, dass eine Zertifikatsseriennummer im Status „unused“ ist. Stattdessen antwortet der OCSP auf solche Anfragen mit „unknown“.

Die OCSPs werden diesbezüglich gemonitort.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Derzeit werden keine anderen Formen der Bekanntmachung eingesetzt.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat möglichst unverzüglich zu sperren. Es existieren keine weiteren Regelungen.

4.9.13 Suspendierung von Zertifikaten

Eine Suspendierung (Sperrgrund „on-hold“) für eine Zertifizierungsstelle wird nicht angeboten.

4.9.14 Wer kann eine Suspendierung beantragen

Suspendierung wird hier nicht angeboten.

4.9.15 Ablauf einer Suspendierung

Suspendierung wird hier nicht angeboten.

4.9.16 Begrenzung der Suspendierungsperiode

Suspendierung wird hier nicht angeboten.

4.10 Statusauskunftsdienste für Zertifikate

Ein Online-Statusauskunftsdienst steht zur Verfügung (siehe Kapitel 4.9.9).

4.10.1 Betriebliche Vorgaben

Keine besonderen Merkmale über die genannten hinaus (siehe Kapitel 4.9)

4.10.2 Verfügbarkeit

Der Statusauskunftsdienst hat eine Verfügbarkeit von 7*24 Stunden.

Es besteht eine Möglichkeit zur Sperrung eines Zertifikats von 7*24 Stunden.

4.10.3 Optionale Merkmale

Keine optionalen Merkmale vorhanden.

4.11 Kündigung durch den Zertifikatsnehmer

Im Falle der Kündigung des Vertragsverhältnisses durch den Zertifikatsnehmer erfolgt die Sperrung des Zertifikats.

4.12 Schlüsselhinterlegung und Wiederherstellung

Für eine im Trust Center betriebene Zertifizierungsstelle werden die Schlüsselpaare auf einem sicherheitsüberprüften Hardware Security Module HSM verschlüsselt hinterlegt und in sicherer Umgebung abgelegt. Eine Schlüsselhinterlegung bei Dritten ist nicht realisiert.

4.12.1 Richtlinien für Schlüsselhinterlegung und -wiederherstellung.

Nicht anwendbar.

4.12.2 Sitzungsschlüsselkapselung und Richtlinien für die Wiederherstellung.

Nicht anwendbar.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE MAßNAHMEN

Die Root-CAs, die in diesem CPS betrachtet werden, sind innerhalb des Trust Centers in einem speziell geschützten Bereich untergebracht und werden von vertrauenswürdigem und fachkundigem Personal betrieben. Alle Prozesse für die Beauftragung und Erzeugung von Zertifikaten sind genau definiert. Alle Sicherheitsmaßnahmen sind in einem Sicherheitskonzept (nicht öffentlich verfügbar) dokumentiert.

5.1 Trust Center Sicherheitsmaßnahmen (Physikalische Kontrollen)

In diesem Kapitel werden die infrastrukturellen Maßnahmen beschrieben.

5.1.1 Standort und bauliche Maßnahmen

Die Root-CAs werden an einem Standort des Trust Centers betrieben, für den mittlere Sicherheitsanforderungen gefordert sind. An diesem Standort ist der Großteil des Trust Center Betriebs- bzw. Administrationspersonals stationiert, so dass kurze Dienstwege zur Wartung und Überwachung der Infrastruktur gegeben sind. In dem Gebäude befinden sich Räume, in denen lediglich Container und Kanäle zu finden sind, deren Schutzbedarf durch zusätzliche technische oder organisatorische Maßnahmen vollständig abgedeckt werden kann.

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

5.1.2 Physikalischer Zutritt

Zutritt Gebäude:

Das Gebäude ist mit einem Pförtner innerhalb der Kernarbeitszeit von 06-18 Uhr besetzt. Außerhalb dieses Zeitfensters werden die jeweiligen Ausgänge alarmgesichert und das Gebäude Video-überwacht. Alle Zugänge sind nur über Chipkartenauthentisierung zu öffnen.

Die Chipkarten, Schlüssel und die Zutrittsanlagensteuerung zum Administrationsbereich werden intern durch DT Security verwaltet. Externe Gäste werden durch die Mitarbeiter am Empfang abgeholt.

Zutritt Administrationsbereich:

Die Räume, in denen die Technikkomponenten untergebracht sind, befinden sich im 1. Obergeschoss in einem abgeschlossenen Sicherheitsbereich des administrativen Betriebspersonals, im Folgenden kurz als Administrationsbereich bezeichnet. Sowohl die Büroräume des zuständigen administrativen Betriebspersonals als auch der Technikbereich innerhalb des Administrationsbereichs sind mit einem zusätzlichen restriktiven Zutritt versehen. Diese Zutrittskontrollanlage ist zusätzlich zu der Kontrollanlage des Gebäudes installiert. Um den Administrationsbereich zu betreten müssen somit zwei Zutrittskontrollsysteme durchlaufen werden:

- Mittels des Zutrittskontrollsystems werden die Zutrittsregelungen umgesetzt und protokolliert.
- Die Zutrittsberechtigungen werden regelmäßig überprüft. Alle Berechtigungsvergaben und Zutritte werden protokolliert.
- Jede der Türen ist mit Blockschloss und Chipkartenleser versehen.
- Die Zutrittsberechtigungen sowie die zu deren Umsetzung notwendigen Chipkarten und Schlüssel werden auf Grund der Vorgaben durch den Leiter des Betriebs vergeben und sind in Listen festgehalten.
- Die Nutzung der Schlüssel ist für Notfälle vorbehalten, daher besitzt lediglich eine kleine Benutzergruppe diese Schlüssel. Die Verwendung eines Schlüssels wird über die Zutrittskontrollanlage protokolliert.
- Die Zutrittskontrollanlage wird von einem Administrator administriert. Einsicht in die Protokolle der Zutrittskontrollanlage ist nur im 4-Augen-Prinzip möglich.

Der Server steht in einem abgesicherten Serverschrank. Die Bedienung des Servers erfolgt im 4-Augen-Prinzip. Der Zugriff auf die eingesetzten Hardware Security Module (HSMs) wird zusätzlich abgesichert. Die HSMs stehen hierzu in einem Tresor im Administrationsbereich, auf welchen nur zugelassene Administratoren zugreifen dürfen.

Alarmsicherung:

- Die Wände und Fensterfront des Administrationsbereiches sind mit einer Überwachung und Einbruchsicherung versehen.
- Im Flur ist ein Bewegungsmelder angebracht.
- Die beiden Türen innerhalb des Fluchtweges sind ebenso alarmgesichert.
- Der Sicherheitsbereich verfügt über eine eigene Einbruchmeldeanlage. Die Signalisierung der Alarme erfolgt auf die Alarmanlage des Standorts. Eine Scharfschaltung erfolgt außerhalb der Arbeitszeiten.

5.1.3 Stromversorgung und Klimatisierung

Die Stromversorgung des Standorts verfügt über ein separates Netz (grüne Steckdosen) für eine unterbrechungsfreie Stromversorgung.

Der Administrationsbereich ist mit einer Klimatisierung ausgestattet. Die Außenwände sind hierzu in massiver Bauweise umgesetzt. In einer Außenwand sind die Be- und Entlüftung der Klimaanlage integriert. Die Lüftungsgitter sind dabei von innen verschraubt und können von außen nicht demontiert werden. Der Bereich zur Wartung der Klimaanalage ist durch eine separate Türe gesichert. Die Tür wird nur unter Aufsicht zu Wartungsarbeiten geöffnet.

5.1.4 Wasserschäden

Der Administrationsbereich ist im Hinblick auf Vermeidung von Wasserschäden im 1. Obergeschoss untergebracht.

5.1.5 Brandschutz

Die geltenden Brandschutzbestimmungen (u.a. Auflagen der örtlichen Feuerwehr, Vorschriften über Feuerresistenz, VDE-gerechte Elektroinstallation) werden eingehalten. Alle Brandschutztüren zum und innerhalb des Administrationsbereichs besitzen automatische Schließeinrichtungen. In Absprache mit der Feuerwehr wird nur in äußersten Notfällen mit Wasser gelöscht.

Das Gebäude ist in mehrere Brandabschnitte unterteilt. Innerhalb des Gebäudes sind der Administrationsbereich, sowie wichtige Nebenräume durch die Wandkonstruktion und die Qualität der eingesetzten Türen als eigenständige Brandabschnitte konzipiert.

Das ganze Gebäude ist mit Rauchmeldern ausgestattet. Die Brandmeldezentrale mit Aufschaltung zur Feuerwehr Siegen befindet sich direkt am Haupteingang in der Pförtnerloge.

5.1.6 Aufbewahrung von Datenträgern

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

5.1.7 Entsorgung

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

5.1.8 Externe Sicherung

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

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Alle Personen, die für die Root-CAs tätig sind, werden als vertrauenswürdige Rollen geführt. Dies sind die Bereiche Operatoren, die Systemadministratoren, die internen Auditoren und die Betriebsverantwortlichen. Für alle Personen gelten die hohen Anforderungen an diese Rollenübertragung.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Die Aufrechterhaltung des Betriebs der Zertifizierungsstelle und des Verzeichnisdienstes (Administration, Sicherung, Wiederherstellung) wird von fachkundigen und vertrauenswürdigen Mitarbeitern wahrgenommen.

Arbeiten an hochsensitiven Komponenten (z.B. Schlüsselerstellungssystem, HSM) sind durch besondere interne Kontrollverfahren geregelt und werden von mindestens zwei Mitarbeitern im 4-Augen-Prinzip in vertrauenswürdiger Rolle in sicherer Umgebung durchgeführt.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

DT Security Mitarbeiter, die als vertrauenswürdige Personen eingestuft sind und vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer internen Sicherheitsüberprüfung (siehe Kapitel 5.3.2).

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

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

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Die folgenden Rollen erfordern eine Aufgabentrennung und werden daher von verschiedenen Mitarbeitern wahrgenommen:

- Sicherung und Rücksicherung von Datenbanken und HSMs,
- Key Lifecycle Management von Sub-CA- und Root-CA-Zertifikaten.

5.3 Personelle Maßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

DT Security verlangt von seinen Mitarbeitern, die als vertrauenswürdige Personen tätig werden möchten, Nachweise vorzulegen über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen, siehe auch Kapitel 5.3.2.

5.3.2 Sicherheitsüberprüfung

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

- Überprüfung und Bestätigung der bisherigen Beschäftigungsverhältnisse,
- Überprüfung von Arbeitszeugnissen,
- Bestätigung des höchsten oder maßgebenden Schul-/Berufsabschlusses,
- Führungszeugnis gemäß BZRG §30.

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

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

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

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

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

In regelmäßigen Abständen, spätestens jedoch nach drei Jahren, ist ein neues Führungszeugnis der DT Security vorzulegen oder es wird eine erneute Prüfung durchgeführt.

5.3.3 Schulungs- und Fortbildungsanforderungen

Das Personal der DT Security besucht Fortbildungsmaßnahmen die zur kompetenten und zufriedenstellenden Erfüllung ihrer beruflichen Pflichten erforderlich sind. DT Security führt Unterlagen über diese Schulungsmaßnahmen.

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

- fortgeschrittene PKI-Kenntnisse inkl. Key Management,
- Verfahrensweisen nach ITIL,
- Datenschutz,
- Sicherheits- und Betriebsrichtlinien und –verfahren von DT Security,
- Verwendung und Betrieb eingesetzter Hardware und Software,
- Meldung von und Umgang mit Störungen und Kompromittierungen und
- Verfahren für die Schadensbehebung im Notfall (Desaster Recovery) und Geschäftskontinuität (Business Continuity).
- Anforderungen des CA-Browserforums
- Anforderungen der Browserhersteller z.B. Mozilla Root Program

5.3.4 Nachschulungsintervalle und -anforderungen

Das Personal der DT Security erhält im erforderlichen Umfang und den erforderlichen Abständen Auffrischungsschulungen und Fortbildungslehrgänge, insbesondere werden die Weiterentwicklung der Root-Programme der Browserhersteller und des CA/Browserforum geschult.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Es wird beim Wechsel von Mitarbeitern darauf geachtet, dass keine Risiken durch den Wechsel entstehen.

5.3.6 Sanktionen bei unbefugten Handlungen

DT Security behält sich vor, unbefugte Handlungen oder andere Verstöße gegen dieses CPS und der daraus abgeleiteten Verfahrens- und Arbeitsanweisungen zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen können Maßnahmen bis einschließlich der Kündigung beinhalten und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.

5.3.7 Anforderungen an unabhängige Auftragnehmer

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

Obiger Personenkreis, der die in Kapitel 5.3.2 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von DT Security nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.3.8 Dokumentation für das Personal

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

5.4 Protokollereignisse

5.4.1 Art der aufgezeichneten Ereignisse

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

CA-Schlüsselpaare und CA-Systeme

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

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

CA-Zertifikate

Für das Lifecycle-Management von CA-Zertifikaten protokolliert das Trust Center mindestens die folgenden Ereignisse:

- 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 werden vom Trust Center für den Betrieb der Infrastruktur alle sicherheitsrelevanten Ereignisse protokolliert. Das beinhaltet mindestens die folgenden Ereignisse:

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

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

Die erstellten Audit-Protokolle/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft DT Security die Audit-

Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen.

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

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Audit-Protokolle/Logging-Dateien werden nach Bearbeitung sieben (7) Jahre archiviert.

5.4.4 Schutz der Audit-Protokolle

Audit-Protokolle/Logging-Dateien werden gegen unbefugten Zugriff geschützt.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Eine Sicherung von Audit-Protokollen/Logging-Dateien wird bedarfsweise durchgeführt.

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

Audit-Daten/Logging-Dateien werden durch die Anwendung erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von DT Security -Mitarbeitern aufgezeichnet.

5.4.7 Benachrichtigung des Ereignisauslösenden Subjekts

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

5.4.8 Schwachstellenprüfung

Die Trust Center Administratoren werden regelmäßig über bekanntgewordene Schwachstellen von Software-Produkten informiert. Nach Auswertung der Information erfolgt eine Schwachstellenbewertung, aus der Gegenmaßnahmen abgeleitet und umgehend durchgeführt werden.

5.5 Datenarchivierung

5.5.1 Art der archivierten Datensätze

DT Security archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener Form,
- alle Audit-/Event-Logging-Dateien, die erfasst werden.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommener Sperrungen, sind für mindestens sieben (7) Jahre nach Ablauf der Zertifikatsgültigkeit vorzuhalten,
- Audit- und Event Logging Daten werden sieben (7) Jahre gespeichert.

5.5.3 Schutz von Archiven

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

5.5.4 Sicherungsverfahren für Archive

Eine inkrementelle Sicherung der elektronischen Archive wird täglich durchgeführt.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Datensätze wie beispielsweise Zertifikate, Zertifikatssperrlisten, OSCP-Antworten, Logging-Dateien enthalten Informationen über Datum und Uhrzeit. Als Zeitquelle dient das Empfangssignal des DCF 77, aus dem die UTC abgeleitet wird.

5.5.6 Archiverfassungssystem (intern oder extern)

DT Security verwendet ausschließlich interne Archivierungssysteme.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

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

5.6 Schlüsselwechsel

Innerhalb des Gültigkeitszeitraums kann ein Schlüsselwechsel bzw. Zertifikatswechsel erforderlich werden bei:

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

Die Generierung neuer Schlüssel und Zertifikate wird dokumentiert und gemäß den Regelungen des Schlüsselgenerierungsverfahrens (Key Generation Ceremony) überwacht. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3).

Zertifikate können nur innerhalb des Gültigkeitszeitraums der hierarchisch übergeordneten Stammzertifizierungsstelle (Root-CA) erneuert werden. Abgelaufene oder gesperrte Zertifikate stehen weiterhin zu Validierung auf einer Webseite zur Verfügung.

Bei Schlüsselwechseln von Root-CA oder Sub-CA ist die Generierung neuer Schlüssel und Zertifikate zu dokumentieren, und gemäß den Auflagen des jeweiligen Sicherheitskonzepts zu überwachen. Neue Zertifikate und ihre Fingerprints sind zu veröffentlichen (siehe hierzu Kapitel 2.2).

5.7 Kompromittierung und Wiederherstellung der Dienstleistung

Bei Kompromittierung privater Schlüssel von Root-CA oder Sub-CA ist dies unverzüglich mitzuteilen (siehe hierzu Kapitel 2.2). Sub-CA Zertifikate sind daraufhin unverzüglich zu sperren, und die entsprechende ARL ist unverzüglich zu veröffentlichen. Die Generierung neuer Schlüssel und Zertifikate ist zu dokumentieren, und gemäß den Auflagen des jeweiligen

Sicherheitskonzepts zu überwachen. Neue Zertifikate und ihre Fingerprints sind zu veröffentlichen (siehe hierzu Kapitel 2.2).

5.7.1 Umgang mit Störungen und Kompromittierungen

Störungen werden über die in Kapitel 1.5.2 definierten Kontakte eingereicht und im Rahmen des Service Managements bearbeitet.

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

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

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

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

Endteilnehmer werden über die mögliche Kompromittierung über die einschlägigen Webseiten informiert (siehe hierzu Kapitel 2.3). Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechende Zertifizierungsstellen-Sperrliste (ARL) zu generieren und zu veröffentlichen.

5.7.4 Geschäftskontinuität nach einem Notfall

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

Der Notfallplan enthält mindestens die folgenden Informationen:

- Die notwendigen Kriterien für die Aktivierung des Planes
- Mögliche Notfallmaßnahmen (je nach Situation)
- 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

Im Rahmen eines Compliance-Audits (siehe Kapitel8) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

5.8 Einstellung des CA oder RA Betriebes

Eine Betriebsbeendigung kann nur durch die DT Security Geschäftsleitung ausgesprochen werden.

Falls eine oder alle DT Security Root-CAs (siehe Kapitel 1.3.1) den Betrieb einstellen müssen, wird ein Beendigungsplan erstellt. Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen, betroffene nachgeordnete Stellen vorab über diese Betriebsbeendigungen zu informieren.

Ein Beendigungsplan kann die folgenden Regelungen enthalten:

- Fortführung des Sperrservice
- Sperrung von ausgegebenen CA Zertifikaten
- eventuell erforderliche Übergangsregelungen auf eine Nachfolge CA
- je nach Ausgestaltung bestehender Einzelverträge entstehende Kostenerstattung
- Aufbewahrung der Unterlagen und Archive der CA

Wenn der Betrieb (insbesondere der Sperrdienst) nicht durch eine andere Zertifizierungsstelle übernommen wird, werden alle ausgestellten Zertifikate gesperrt.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

Das Trust Center ist in einem speziell geschützten Gebäude untergebracht und wird von fachkundigem Personal betrieben. Alle Prozesse für die Beauftragung und Erzeugung von Zertifikaten der dort betriebenen Zertifizierungsstellen sind genau definiert. Alle technischen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept (nicht öffentlich verfügbar) dokumentiert.

Die folgenden Aussagen beschreiben technische Maßnahmen und gelten für die vom Trust Center betriebene Root-CA-Zertifikate.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

6.1.1.1 Generierung von CA-Schlüsselpaaren

Alle Schlüsselpaare für Root-CA-Zertifikate werden in abgeschirmter Umgebung und in einer sicherheitsüberprüften Hardware Security Module (FIPS 140-2/ Level 3 evaluiert) erzeugt und gespeichert. Es wird eine entsprechende Schlüsselzeremonie durchgeführt.

Bei der Schlüsselerzeugung wird die Durchsetzung des 4-Augen-Prinzips erzwungen. Die Erstellung von CA-Schlüsseln gemäß [EN 319 411] dokumentiert.

6.1.1.2 Generierung von RA-Schlüsselpaaren

Nicht anwendbar.

6.1.1.3 Generierung von Subscriber-Schlüsselpaaren (EE-Zertifikate)

Nicht anwendbar.

6.1.2 Bereitstellung des privaten Schlüssels an Zertifikatsnehmer

Nicht anwendbar.

Es ist keine Auslieferung privater Schlüssel an Zertifikatsnehmer vorgesehen.

6.1.3 Bereitstellung des öffentlichen Schlüssels an die Zertifizierungsstelle

Öffentliche Schlüssel einer zu zertifizierenden Sub-CA werden in Form eines signierten PKCS#10 Requests an das Trust Center (Zertifizierungsstelle) zur Zertifikatserzeugung gesichert übermittelt.

6.1.4 Bereitstellung des öffentlichen CA-Schlüssels

Die öffentlichen Schlüssel der DT Security Root-CAs können sowohl vom LDAP-Server ldap.telesec.de, als auch von den Webseiten des Trust Centers (dort finden sich auch die entsprechenden Fingerprints veröffentlicht) bezogen werden (siehe hierzu auch Kapitel 2).

6.1.5 Algorithmen und Schlüssellängen

6.1.5.1 Root-CA Zertifikate

Die Schlüssellänge der DT Security Root-CA-Zertifikate beträgt bei Nutzung eines RSA-Schlüssels mindestens 2048-Bit, bei Nutzung eines ECC-Schlüssels 384 Bit.

Als Hash-Algorithmus finden SHA-1[1], SHA-256 Bit und SHA384ECDSA Anwendung, siehe auch Kapitel 7.1.3.

6.1.5.2 Subordinate-CA Zertifikate

Die Schlüssellänge der Sub-CA-Zertifikate beträgt für RSA-Schlüssel mindestens 2048-Bit, für ECC-Schlüssel mindestens 256 Bit.

Als Hash-Algorithmus wird min. SHA-256 Bit eingesetzt.

6.1.5.3 Subscriber-Zertifikate (EE)

Nicht anwendbar.

6.1.6 Parameter der Generierung öffentlicher Schlüsselparameter und Qualitätskontrolle

Öffentliche Schlüssel werden gemäß den Vorgaben von [CAB-BR] generiert.

Die in Requests für Sub-CAs enthaltenen Schlüssel werden den Vorgaben von [CAB-BR] im entsprechenden Kapitel geprüft.

6.1.7 Schlüsselverwendung

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

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

DT Security hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA-Schlüsseln gewährleisten zu können.

Im Fall von Root-CA und Sub-CA Zertifikaten werden die privaten Schlüssel auf einem sicherheitsüberprüften Hardware Security Module erzeugt und abgelegt. Ein Backup der Schlüssel ist unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken möglich. Details regelt das Sicherheitskonzept.

6.2.1 Standards und Kontrollen für kryptografische Module

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

[1] Für SHA-1 besteht dabei die Einschränkung das dieser Algorithmus nur für noch laufende Root-CAs Anwendung finden darf, jedoch nicht mehr für die Ausstellung von neuen Root-CAs. Siehe CP, Kapitel 7.1.3

Während des gesamten Lebenszyklus werden die Module durch technische und organisatorische Maßnahmen vor unbefugter Manipulation geschützt.

6.2.2 Mehrpersonenkontrolle (n aus m) bei privaten Schlüsseln

DT Security hat technische, organisatorische und prozessuale Mechanismen implementiert, die die Teilnahme mehrerer vertrauenswürdiger und geschulter Personen des Trust Centers erfordern, um vertrauliche kryptografische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels wird durch einen geteilten Authentisierungsprozess geschützt. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

6.2.3 Hinterlegung von privaten Schlüsseln

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

6.2.4 Sicherung (Key Backup) von privaten Schlüsseln

DT Security erstellt für Wiederherstellungs- und Notfallzwecke Sicherungskopien (Back-Up) des Schlüsselmaterials der Root-CA-Zertifikate. Diese Schlüssel werden in verschlüsselter Form innerhalb von kryptografischen Hardware-Modulen (HSM) und zugehörigen Schlüsselspeichergeräten gespeichert.

Die Wiederherstellung von privaten Schlüsseln wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentification mit Key) geschützt. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit die Arbeiten ermöglichen.

6.2.5 Archivierung von privaten Schlüsseln

Wenn Root-CA-Schlüssel das Ende ihrer Gültigkeitsdauer erreicht haben, werden sie vernichtet. Eine Archivierung von Schlüsseln findet nicht statt.

Die Vorgaben des Löschkonzeptes werden umgesetzt.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

DT Security generiert Root-CA-Schlüssel auf kryptografischen Hardware-Modulen (HSM). Von diesen Schlüsseln werden Kopien für Wiederherstellungs- und Notfallzwecke (siehe Kapitel 6.2.4 und 6.2.5) erstellt. In diesem Falle erfolgt die Übertragung in verschlüsselter Form zwischen beiden Modulen.

Alle Arbeitsschritte können nur von berechtigten Personen im 4-Augenprinzip durchgeführt werden und sind zu dokumentieren.

6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

DT Security speichert Root-CA-Schlüssel in sicherer Form auf zugelassen und FIPS 140-2 Level 3 evaluierten kryptografischen Hardware-Modulen (HSM).

6.2.8 Methode zur Aktivierung privater Schlüssel

Aktivierung privater Schlüssel auf kryptografischen Modulen

Die Root-CA-Schlüssel werden im Vier-Augen-Prinzip aktiviert und protokolliert.

Die Aktivierungsdaten werden gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung geschützt.

Aktivierung privater Sub-CA-Schlüssel auf kryptografischen Modulen

Private Schlüssel von Sub-CA-Zertifikaten liegen nur dem jeweiligen Service vor.

Aktivierung von Endteilnehmer-Zertifikaten auf kryptographischen Modulen

Private Schlüssel von Endteilnehmern liegen nicht vor.

6.2.9 Methode zur Deaktivierung privater Schlüssel

Die privaten CA-Schlüssel werden durch Beendigung der Verbindung zwischen HSM und Anwendung deaktiviert. Die Deaktivierung wird nach Beendigung von Aktionen (Generierung von Schlüsseln, Signieren von Sperrlisten) protokolliert.

6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von Root-CA-Schlüsseln erfolgt durch Löschung im HSM, sowie sämtlicher Backup-Token. Die Löschung wird durch Mehrpersonen (2 Personen unterschiedlicher Rolle) durchgeführt und dokumentiert. Eine weitere Verwendung des privaten Schlüssels ist somit nicht mehr möglich.

6.2.11 Methode zur Beurteilung kryptographischer Module

Die Beurteilung erfolgt auf den vorgegebenen Methoden. FIPS 140-2/Level 3 evaluiert evaluierte Komponenten werden auf Gültigkeit gemäß NIST überwacht.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung von öffentlichen Schlüsseln

Öffentliche Schlüssel werden in Form der erstellten Zertifikate archiviert.

Im Rahmen der regelmäßigen Backup Maßnahmen von DT Security werden die Zertifikate gesichert und archiviert. Andere Vorgehensweisen werden einzelvertraglich festgelegt.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Root-CA-Schlüssel und Root-CA-Zertifikate haben eine Gültigkeit von maximal 25 Jahren.

OCSP-Zertifikate haben eine maximale Gültigkeit von 1 Jahr.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Bei der Generierung und Installation wurden die Vorgaben der CP eingehalten.

Die Aktivierungsdaten der Root-CA-Schlüssel werden durch das HSM abgefragt. Bei Passwort-Vergabe ist das 4-Augen-Prinzip durch Aufteilung des Passworts auf 2 Hälften erzwungen. Je eine Hälfte wird durch eine Person der Rolle TC-PV und RFK gesetzt. Zusätzlich ist die Aktivierung durch gemeinsamen Einsatz von 2 unterschiedlichen PED-Keys notwendig die sich getrennt im Zugriff von Personen der Rolle TC-PV und RFK befinden.

6.4.2 Schutz von Aktivierungsdaten

Die beteiligten Personen (Trusted Roles) hinterlegen ihre Aktivierungsdaten blickgeschützt in dafür vorgesehene Tresore.

6.4.3 Weitere Aspekte von Aktivierungsdaten

Übertragung von Aktivierungsdaten

Die Übertragung von Aktivierungsdaten erfolgt persönlich.

Vernichtung von Aktivierungsdaten

Sobald die Aktivierungsdaten nicht mehr benötigt werden, werden diese sicher gelöscht, geschreddern oder in speziell gekennzeichneten Behältern für sichere Aktenentsorgung, vernichtet.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

DT Security stellt sicher, dass die benötigten Systeme, je nach Schutzbedarf entsprechend Sicherheitskonzept gesichert werden.

Die Root-CA wird offline, d.h. ohne Netzanbindung betrieben.

6.5.2 Bewertung der Computersicherheit

Im Rahmen des Sicherheitskonzeptes wurden unterschiedliche Bedrohungsanalysen durchgeführt, die die Wirksamkeit aller getroffenen Maßnahmen untersuchen.

Die Bewertung wird nach jedem Vorfall, spätestens aber einmal jährlich überprüft.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Kontrollen der Systementwicklung

Keine Bestimmungen.

6.6.2 Kontrollen des Sicherheitsmanagements

DT Security hat Mechanismen und/oder Richtlinien implementiert, um die Konfiguration seiner CA-Systeme kontrollieren und überwachen zu können. Die Integrität wird vor der Installation manuell verifiziert.

6.6.3 Sicherheitskontrollen des Lebenszyklus

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

Durch Versiegelung der Hardware und Softwarechecks werden Manipulationen und Manipulationsversuche bei jeder Aktion oder Revision erkennbar.

6.7 Netzwerk-Sicherheitskontrollen

Folgende Netzwerk-Sicherheitsmaßnahmen sind implementiert:

- Verzeichnisdienste und OCSP-Responder
  - Die vom Internet aus erreichbaren Verzeichnisdienste und OCSP-Responder sind durch Firewalls von den internen Netzen getrennt.
  - In regelmäßigen Abständen werden Schwachstellenüberprüfungen durchgeführt. Weitere Details sind in Kapitel 5.4.8 beschrieben.
- Sicherheitskritische Komponenten
  - Die sicherheitskritischen Komponenten und Systeme (z.B. CA, DB, Signer, HSM) sind nur direkt im Rack verkabelt und netztechnisch komplett isoliert.

6.8 Zeitstempel

Die Zeitquelle wird am Offline System manuell synchronisiert.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

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

Zertifikatsprofile für CA- und Teilnehmerzertifikate werden in der CPS der jeweiligen Zertifizierungsstelle im Detail definiert.

Die Seriennummern werden mit einem kryptographisch sicheren Zufallszahlengenerator erstellt. Sie sind größer als Null und besitzen mindestens 64 bit Entropie.

7.1.1 Versionsnummer(n)

Root-CA-Zertifikate werden entsprechend der internationalen Norm X.509 in der Version 3 ausgestellt.

7.1.2 Zertifikatsinhalte und -erweiterungen nach RFC 5280

7.1.2.1 Root-CA-Zertifikate

Die Zertifikatserweiterungen der Root-CA- und Sub-CA-Zertifikate entsprechen den Vorgaben der CP.

7.1.2.2 Sub-CA-Zertifikate

Die Zertifikatserweiterungen der Root-CA- und Sub-CA-Zertifikate entsprechen den Vorgaben der CP.

7.1.2.3 EE-Zertifikate

Nicht Bestandteil dieses CPS.

7.1.2.4 Alle Zertifikate

Alle weiteren Felder werden konform zu [RFC 5280] umgesetzt.

7.1.2.5 Anwendung von [RFC 5280]

Alle weiteren Felder werden konform zu [RFC 5280] umgesetzt.

7.1.3 Objekt-Kennungen von Algorithmen

Folgende Signaturalgorithmen werden in Root-CA-Zertifikaten verwendet:

- SHA256 RSA (OID 1.2.840.113549.1.1.11)
- SHA384 ECDSA (OID 1.2.840.10045.4.3.3)

Der SHA-1 Algorithmus findet für neue Root-CA-Zertifikate keine Anwendung mehr. Laufende Root-CA-Zertifikate dürfen diesen nach [CA-BR, v.1.6.7] anhand ihrer Laufzeit weiterhin nutzen.

7.1.4 Namensformen

Für die Namensformen von Root-CA werden die CP eingehalten.

7.1.4.1 Herausgeber Informationen

Nicht anwendbar.

7.1.4.2 Subject Information für Subscriber-Zertifikate

7.1.4.2.1 Subject Alternative Name Erweiterung

Nicht anwendbar.

7.1.4.2.2 Subject Distinguished Name Fields

Nicht anwendbar.

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

7.1.4.3.1 Subject Distinguished Name Fields

Für die Namensformen der Root-CA werden die CP-Vorgaben eingehalten.

7.1.5 Namensbeschränkungen

Für die Namensbeschränkungen der Root-CA werden die CP-Vorgaben eingehalten.

7.1.6 Objekt-Identifikatoren für Zertifizierungsrichtlinien

7.1.6.1 Reservierte Objekt-Identifikatoren für Zertifizierungsrichtlinien

Siehe CP, Kapitel 7.1.6.1

7.1.6.2 Root-CA Zertifikate

Die eingeschlossenen Root-CA-Zertifikate enthalten keine Zertifizierungsrichtlinien.

7.1.6.3 Sub-CA Zertifikate

Die Zertifizierungsrichtlinien von unterliegenden Sub-CA-Zertifikaten sind in den CPS der jeweiligen Services benannt.

7.1.6.4 Endteilnehmer-Zertifikate

Nicht anwendbar.

7.1.7 Verwendung der Erweiterung Policy Constraints

Kein Einsatz der Erweiterung Policy Constraints bei den Root-CA-Zertifikaten.

7.1.8 Syntax und Semantik von Policy Qualifiers

Kein Einsatz von Policy Qualifiers bei den Root-CA-Zertifikaten.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung: Certificate Policies

Kein Einsatz der Erweiterung Certificate Policies bei den Root-CA-Zertifikaten.

7.2 Sperrlistenprofile

Die von DT Security ausgestellten Sperrlisten entsprechen folgenden Anforderungen:

- [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)

DT Security unterstützt Zertifikatssperrlisten im Format X.509 Version 2, gemäß RFC 5280.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

7.2.2.1 Erweiterung „Stellenschlüsselkennung “ (AuthorityKeyIdentifier)

Die Sperrlisten enthalten die Erweiterung „Stellenschlüsselkennung“. Der Risikowert dieser Erweiterung ist als „nicht kritisch“ gesetzt.

7.2.2.2 Erweiterung „Sperrlistennummer“

Die Sperrlisten enthalten die Erweiterung „Sperrlistennummer“ als fortlaufende Seriennummer der Sperrliste. Der Risikowert dieser Erweiterung ist als „nicht kritisch“ gesetzt.

7.3 OCSP-Profil

7.3.1 Versionsnummer(n)

Es wird OCSP V1 gemäß [RFC 6960] eingesetzt.

7.3.2 OCSP-Erweiterungen

Es werden keine OCSP-Erweiterungen genutzt.

8 AUDITS UND ANDERE BEWERTUNGSKRITERIEN

Die Root-CAs sind gemäß der relevanten Policies der ETSI TS 102 042 (ab Juni 2018 ETSI EN 319 411-1) zertifiziert. Hierzu findet eine jährliche Überprüfung statt. Die Zertifizierung der Root-CAs findet im Rahmen der Zertifizierung der Sub-CAs statt. Die Zuordnung wird auf der Webseite http://www.telesec.de/de/trust-center unter den veröffentlichten Zertifikaten angegeben.

Da keine Aufgaben der Root-CA durch Dritte ausgeführt werden, werden keine Regelungen und Prüfungen bei Dritten notwendig.

8.1 Häufigkeit und Art der Prüfungen

Entsprechend der Anforderungen findet mindestens einmal jährlich eine Überprüfung im Rahmen der Zertifizierung und ein internes Audit statt.

8.2 Identität/Qualifikation des Prüfers

Für die Feststellung der ETSI Konformität wird für die Prüfung eine akkreditierte Prüfstelle und für die Zertifizierung eine akkreditierte Zertifizierungsstelle beauftragt. Die Durchführung der internen Audits erfolgt durch die vertrauenswürdige Rolle „Interner Auditor“, die entsprechend qualifiziert ist (CISA oder/und Lead Auditor ISO 27001).

8.3 Beziehung des Prüfers zur prüfenden Stelle

Die Prüfung der ETSI-Konformität erfolgt entsprechend ISO/IEC 17021 und erfüllt die dort genannten Anforderungen an die Beziehung des Prüfers zur prüfenden Stelle. Für den internen Auditor gilt ein Rollenausschluß zu allen anderen Rollen der zu prüfenden Stelle.

8.4 Abgedeckte Bereiche der Prüfung

Die Prüfung umfasst den kompletten Scope der ETSI-Norm ETSI EN 319 411-1. Dies umfasst gemäß ETSI EN 319 411-1 Kapitel 4.4 den kompletten CA-Betrieb inkl. der Komponenten Registration Service, Certificate Generation Service, Dissemination Service, Revokation Management Service, Revokation Status Service und Subject Device Provision Service.

8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Werden bei einer Prüfung durch die akkreditierte Prüfstelle Mängel oder Fehler festgestellt, so werden diese bewertet und je nach Bewertung müssen Sofortmaßnahmen eingeleitet werden oder innerhalb von bestimmten Fristen eingeleitet werden. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen. Der Leiter Trust Center, vertreten durch den IT-Sicherheitsbeauftragten, ist verantwortlich für die Fortschreibung und Umsetzung des Maßnahmenplans.

8.6 Mitteilung der Ergebnisse

Die Zertifizierungsurkunden werden durch die akkreditierte Zertifizierungsstelle dem Management der DT Security CAs übergeben und werden dann auf der Webseite des Trust Centers unter: https://www.telesec.de/de/trust-center veröffentlicht.

Die Prüfberichte der Prüfstelle, die der Zertifizierung zugrunde liegen, werden nicht veröffentlicht. Die Anforderungen und das Ergebnis der Prüfung werden in der Zertifizierungsurkunde als Anlage beigefügt und veröffentlicht.

8.7 Selbst-Auditierung

Trust Center führt interne Selbst-Auditierungen durch und überprüft in regelmäßigen Abständen die Konformität des CP/CPS gegenüber den formalen Vorgaben, z.B. aus [CA-BR].

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BE-STIMMUNGEN

9.1 Entgelte

Die Gebühren werden in den jeweiligen Allgemeinen Geschäftsbedingungen (AGB) der Zertifizierungsstellen festgelegt.

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

DT Security ist berechtigt, für das Ausstellen, Erneuern und Verwalten von Zertifikaten Entgelte zu berechnen. Die Preise sind in den für die jeweilige Leistung geltenden Allgemeinen Geschäftsbedingungen (AGB) der Zertifizierungsstelle oder einzelvertraglich geregelt.

9.1.2 Entgelte für den Zugriff auf Zertifikate

DT Security berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst keine Entgelte.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

DT Security berechnet für den Zugriff auf Sperr- oder Statusinformationen für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile keine Entgelte.

9.1.4 Entgelte für andere Leistungen

DT Security berechnet keine Entgelte für den Abruf dieses Dokuments und der damit verbundenen einfachen Betrachtung.

Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1, 9.5), welche das Urheberrecht des Dokuments hält.

Die Nutzung dieses Dokuments ist ebenfalls entgeltfrei, wenn Sie als mitgeltende Vertragsunterlage für die Vertragsbeziehung zwischen Kunden und DT Security dient.

9.1.5 Erstattung von Entgelten

Die Erstattung von Entgelten durch DT Security erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts. Detaillierte Regelungen finden Sie in den Allgemeinen Geschäftsbedingungen (AGB).

9.2 Finanzielle Verantwortlichkeiten

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

9.2.1 Versicherungsschutz

DT Security verfügt über einen Betriebs- und Vermögenshaftpflichtversicherungsschutz. Es ist sichergestellt, dass die Anforderungen, die sich hinsichtlich des Versicherungsschutzes ergeben, erfüllt werden.

9.2.2 Sonstige finanzielle Mittel

Nicht anwendbar.

9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

Daten von juristischen Personen und Organisationen als Zertifikatsnehmer werden in einem Umfang erhoben und verifiziert, wie es zur Ausstellung der Sub-CA Zertifikate und zur Sicherstellung des Vertrauens in diese Zertifikate notwendig ist.

Personenbezogene Informationen werden gemäß Bundesdatenschutzgesetz geschützt. Personenbezogene Daten werden nur dann Dritten zugänglich gemacht, wenn dies durch gesetzliche Anforderungen notwendig ist.

9.3.1 Umfang von vertraulichen Informationen

Unter vertraulichen Informationen werden alle Informationen von PKI-Beteiligten (siehe Kapitel 1.3.2 und 1.3.3) eingestuft, die nicht unter Kapitel 9.3.2 fallen.

9.3.2 Umfang von nicht vertraulichen Informationen

Unter nicht vertraulichen Informationen werden alle impliziten und expliziten Informationen eingestuft, die in ausgegebenen Zertifikaten, Sperrlisten und Statusinformationen enthalten sind oder davon abgeleitet werden können.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortlichkeit für den Schutz der vertraulichen Informationen sowie über die Einhaltung der datenschutzrechtlichen Bestimmungen liegt bei DT Security als PKI-Diensteanbieter.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

Personenbezogene Daten von Zertifikatsnehmern werden in einem Umfang erhoben und verifiziert, wie es zur Ausstellung der Teilnehmerzertifikate und zur Sicherstellung des Vertrauens in diese Zertifikate notwendig ist.

Im Rahmen der Datenüberprüfung wird nur die Identität des Zertifikatsnehmers, aber nicht seine Vertrauenswürdigkeit, Bonität oder Kreditwürdigkeit festgestellt.

Die personenbezogenen Daten werden gemäß Bundesdatenschutzgesetz und §14 des deutschen Signaturgesetzes geschützt. Personenbezogene Daten werden nur dann Dritten zugänglich gemacht, wenn dies durch gesetzliche Anforderungen notwendig ist

9.4.1 Datenschutzkonzept

DT Security hält sich an die Vorgaben aus dem Datenschutzkonzept für die DT Security PKI. Das Datenschutzkonzept kann in Auszügen auf Anforderung bereitgestellt werden.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.1.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.2.

9.4.4 Verantwortung für den Schutz vertraulicher Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.3.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsauftraggeber stimmt der Nutzung von personenbezogenen Daten durch eine CA oder RA zu, soweit dies zur Leistungserbringung erforderlich ist. Ferner dürfen alle Daten veröffentlicht werden, die nach Kapitel 9.4.3 als nicht vertraulich behandelt werden.

9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die Verpflichtung zur Geheimhaltung der vertraulichen Informationen oder personenbezogener Daten entfällt, soweit die Offenlegung kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens bestehen, die zur Offenlegung vertraulicher oder privater Informationen führen könnten, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei hierüber unter Beachtung der gesetzlichen Bestimmungen informieren.

9.4.7 Andere Umstände zur Offenlegung von Daten

Nicht anwendbar.

9.5 Urheberrecht

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von DT Security unzulässig. Die geistigen Eigentumsrechte an den Zertifikaten und der ARL verbleiben bei DT 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)

DT Security verpflichtet sich, dass:

- keine unrichtigen Angaben in Zertifikate aufzunehmen, die den Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- alle Zertifikate den Anforderungen dieses Dokuments genügen und
- die Sperrfunktionalitäten und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) allen wesentlichen Anforderungen der geltenden CP/CPS erfüllen.

Weiterhin sichert das Trust Center zu, dass zum Zeitpunkt der Ausstellung eines SSL/TLS Zertifikates:

1. eine definierte Prozedur existiert um sicherzustellen, dass der Antragsteller das Recht hat, die im Zertifikat benannten Domains und/oder IP-Adressen zu verwenden. Alternativ ist er über eine entsprechende Vollmacht autorisiert, welche von einer Person oder einer Organisation ausgestellt wurde, welche das Recht zur Verwendung hat.
2. die unter 1) genannte Prozedur befolgt wird und
3. das unter 1) benannte Verfahren in diesem CP/CPS detailliert spezifiziert wird.
4. eine definierte Prozedur befolgt wird, um sicherzustellen, dass der im Zertifikat benannte Zertifikatsnehmer (Subjekt) die Ausstellung des Zertifikates genehmigt hat, sowie, dass der Repräsentant des Antragstellers berechtigt ist, den Antrag zu stellen.
5. die unter 4) genannte Prozedur befolgt wird und
6. das unter 4) benannte Verfahren in diesem CP/CPS detailliert spezifiziert wird.
7. eine definierte Prozedur befolgt wird, um zu prüfen, dass mit Ausnahme des OU-Feldes im subject DN alle im Zertifikat enthaltenen Informationen korrekt sind
8. die unter 7) genannte Prozedur befolgt wird und
9. das unter 7) benannte Verfahren in diesem CP/CPS detailliert spezifiziert wird.
10. eine definierte Prozedur befolgt wird, um die Wahrscheinlichkeit zu minimieren, dass das OU-Feldes des subject DN irreführende Informationen enthält
11. die unter 10) genannte Prozedur befolgt wird und
12. das unter 10) benannte Verfahren in diesem CP/CPS detailliert spezifiziert wird.

Außerdem sichert das Trust Center zu, dass im Falle, dass das auszustellende SSL/TLS Zertifikat Informationen zur Identität des Zertifikatsnehmers enthält

13. eine definierte Prozedur zur Überprüfung der angegebenen Identität befolgt wird, welche die Anforderungen der zum Zeitpunkt der Zertifikatsaustellung gültigen Version der [BR] Kapitel 9.2.4 und 11.2 erfüllt.
14. die unter 13) genannte Prozedur befolgt wird und
15. das unter 13) benannte Verfahren in diesem CP/CPS detailliert spezifiziert wird.

Das Trust Center sichert weiterhin zu, dass:

16. falls der Zertifikatsnehmer ein Konzernunternehmen (affilate) ist, der Repräsentant des Antragstellers vor der Ausstellung eines Zertifikates die "Allgemeinem Nutzungsbedingung" akzeptieren muss.
17. falls der Zertifikatsnehmer kein Konzernunternehmen (affiliate) ist, der Antragsteller mit der DT Security die "Allgemeinen Geschäftsbedingungen" in einer rechtlich durchsetzbaren Form vereinbart.
18. es ein öffentlich zugängliches Verzeichnis betreibt, welches Status Informationen zu allen nicht abgelaufenen Zertifikaten (gültig oder gesperrt) enthält. Dieses Verzeichnis ist 24 x 7 x 365 verfügbar.
19. die ausgestellten Zertifikate aus allen in den [CAB-BR] aufgeführten Gründen sperren wird.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Alle Registrierungsstellen verpflichten sich, dass:

- keine wesentlich unrichtigen Angaben in Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen
- keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, gemacht wurden

und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der beschriebenen Pflichten entstehen
- alle Zertifikate den wesentlichen Anforderungen dieses Dokuments genügen.

9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Keine Bestimmungen.

9.6.4 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der Vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Nicht anwendbar.

9.7 Haftungsausschluss

Der Haftungsausschluss ist in den geltenden Allgemeinen Geschäftsbedingungen (AGB) geregelt.

9.8 Haftungsbeschränkungen

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf eine vorsätzliche Pflichtverletzung zurückzuführen sind, haftet die Zertifizierungsstelle unbegrenzt. Im Übrigen wird die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen in den Allgemeinen Geschäftsbedingungen (AGB) oder einzelvertraglich geregelt.

9.9 Schadensersatz

Schadensersatz ist in den geltenden Allgemeinen Geschäftsbedingungen (AGB) geregelt.

9.9.1 Schadenersatz durch die CAs

Schadensersatz ist in den geltenden Allgemeinen Geschäftsbedingungen (AGB) geregelt.

9.9.2 Schadenersatz durch die Endteilnehmer

Schadensersatz ist in den geltenden Allgemeinen Geschäftsbedingungen (AGB) geregelt.

9.9.3 Schadenersatz durch beteiligte Parteien

Schadensersatz ist in den geltenden Allgemeinen Geschäftsbedingungen (AGB) geregelt.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Dieses Dokument tritt mit der Veröffentlichung auf den DT 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 DT 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

Falls nicht anders vertraglich vereinbart, werden für individuelle Mitteilungen an die Zertifizierungsstelle die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben.

9.12Änderungen des CPS

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich DT Security das Recht vor, Änderungen und Anpassungen dieses Dokuments durchzuführen.

9.12.1 Verfahren für Änderungen

Änderungen des CP/CPS können nur vom DT Security Change Advisory Board durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und Veröffentlichungsdatum.

Änderungen treten unverzüglich mit der Veröffentlichung in Kraft (siehe auch Kapitel 2.3).

Aktualisierte Versionen setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet das DT Security Change Advisory Board über die weitere Vorgehensweise.

9.12.2 Benachrichtigungen über Änderungen

Nachgelagerte Zertifizierungsstellen werden über Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch einzulegen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion nach Ablauf dieser Frist in Kraft. Darüberhinausgehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Falls das DT Security Change Advisory Board der Ansicht ist, dass gravierende z.B. sicherheitsrelevante Änderungen unverzüglich erforderlich sind, dann tritt die neue CP/CPS unverzüglich mit der Freigabe (siehe Kapitel 9.12.1) in Kraft.

9.12.3 Gründe zur Vergabe einer neuen OID

Es liegen keine gesonderten Regelungen vor.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

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

9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland.

9.15 Einhaltung geltenden Rechts

Das vorliegende Dokument unterliegt den geltenden deutschen Gesetzen, Vorschriften, Richtlinien, Verordnungen, Erlassen und Anordnungen, insbesondere den darin beschriebenen Import und Export Bestimmungen von Security-Komponenten (Software, Hardware oder technischer Informationen). Geltende zwingende Gesetze, Vorschriften, Richtlinien, Verordnungen, Erlasse und Anordnungen setzen die entsprechenden Bestimmungen des vorliegenden Dokuments außer Kraft.

9.16 Verschiedene Bestimmungen

9.16.1 Vollständiger Vertrag

Nicht anwendbar.

9.16.2 Abtretung

Nicht anwendbar.

9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieses CPS 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)

Nicht anwendbar.

9.16.5 Höhere Gewalt

Nicht anwendbar.

9.17 Sonstige Bestimmungen

Nicht anwendbar.