Deutsche Telekom Corporate PKI (DTAG cPKI)

Certificate Policy (CP) & Certificate Practice Statement (CPS)
Zertifizierungsrichtlinie und Erklärung zum Zertifikatsbetrieb

T-Systems International GmbH | Telekom Security

Version:	04.00		
Revision:	29	**Status:**	Freigabe
Gültig ab:	01.02.2019	**Klassifizierung:**	öffentlich
Autor:	T-Systems International GmbH, Telekom Security		

T-SYSTEMS INTERNATIONAL GMBH
Hausanschrift: Hahnstraße 43d, 60528 Frankfurt am Main
Postanschrift: Postfach 71 02 45, 60492 Frankfurt am Main
Telefon: +49 69 20060-0 | E-Mail: info@t-systems.com | Internet: www.t-systems.de
Aufsichtsrat: Dr. Christian P. Illek (Vorsitzender)
Geschäftsführung: Adel Al-Saleh (Vorsitzender), Christoph Ahrendt, François Fleutiaux, Georg Pepping
Handelsregister: Amtsgericht Frankfurt am Main HRB 55933, Sitz der Gesellschaft Frankfurt am Main | USt-IdNr. DE118645675
WEEE-Reg.-Nr. DE50335567

Impressum

Herausgeber

T-Systems International GmbH
Telekom Security, Delivery Telekom Security, Trust Center & ID-Solutions
Trust Center Operations
Untere Industriestraße 20
57250 Netphen
Deutschland

Dateiname	Dokumentennummer	Dokumentenbezeichnung
CP-CPS_CPKI NG_ DTAG_SecureEmail_DE_20190201_v.04.00.docm	4.00	Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der DTAG cPKI

Version	Stand	Status
04.00	28.01.2019	Freigabe

Ansprechpartner	Telefon / Fax	E-Mail
T-Systems International GmbH Telekom Security Trust Center & ID-Solutions	+49 (0) 1805-268204 1	telesec_support@t-systems.com

Kurzinfo

Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Deutsche Telekom AG (DTAG) Corporate PKI Next Generation (cPKI). Es beschreibt das für den Betrieb der cPKI erforderliche Sicherheitsniveau und beinhaltet Sicherheitsvorgaben sowie Erklärungen hinsichtlich technischer, organisatorischer und rechtlicher Aspekte.

T-SYSTEMS INTERNATIONAL GMBH
Hausanschrift: Hahnstraße 43d, 60528 Frankfurt am Main
Postanschrift: Postfach 71 02 45, 60492 Frankfurt am Main
Telefon: +49 69 20060-0 | E-Mail: info@t-systems.com | Internet: www.t-systems.de
Aufsichtsrat: Dr. Christian P. Illek (Vorsitzender)
Geschäftsführung: Adel Al-Saleh (Vorsitzender), Christoph Ahrendt, François Fleutiaux, Georg Pepping
Handelsregister: Amtsgericht Frankfurt am Main HRB 55933, Sitz der Gesellschaft Frankfurt am Main | USt-IdNr. DE118645675
WEEE-Reg.-Nr. DE50335567

Änderungshistorie / Release Notes

Version	Stand	Autor/Bearbeiter	Änderungen/Kommentar
0.1	14.02.2008	Ch. Rösner	First draft
0.1a	11.03.2008	S. Kölsch	Changes for RFC 3647-conformity
0.1b	18.03.2008	S. Kölsch	Changes for European Bridge CA
0.2	25.03.2008	S. Kölsch	English headlines, new Corporate Design
0.3	28.05.2008	S. Kölsch	added Remarks for European Bridge CA-conformity after meeting with ChR, TP.
0.4	07.10.2008	S. Kölsch	General Changes
0.5	10.10.2008	S. Kölsch	Revised version, first official draft
0.6	23.12.2009	J. Portaro	Completion for coordination and formal release
0.7	02.04.2010	K. Kirchhöfer T. Pfeifer J. Portaro M. Dornhöfer	Additions
0.8	22.06.2010	M. Dornhöfer	Änderung der Überschriften auf Englisch, cPKI Ausbaustufe1 (CMO)
0.9	23.06.2010	M. Dornhöfer	cPKI Ausbaustufe 2 (FMO)
0.91	15.07.2010	J. Portaro	Trennung CPS Dokumente für CMO und FMO
0.99	24.11.2010	J. Portaro K.-H. Rödel	Prüfung und Bearbeitung offener Punkte
1.0	15.06.2011	Ch. Rösner, S. Kölsch, J. Portaro, M. Dornhöfer	Finale Prüfung und Erstellung Version 1.0
1.1	12.05.2014	J. Portaro	Prüfung und Änderung aufgrund Einführung der cPKI als Nachfolgedienst der vormaligen iPKI/cPKI. Herstellung Web-Trust Konformität. Markierung noch zu klärender Punkte.
1.2	25.03.2015	K.-H. Rödel Oliver Stegemann	Inhaltlich geprüft Freigegeben
1.3	02.10.2015	K.-H. Rödel	Anpassungen für Pseudonym Zertifikate.
1.4	04.03.2016	K.-H. Rödel	Prüfung und Änderung aufgrund Einführung von Funktions-, Gruppen und Pseudonym Zertifikate. Herstellung Web-Trust Konformität
1.5	09.11.2016	K.-H. Rödel	Änderung der CAs auf SHA-256 inkl. der neuen Fingerprints. Anpassung auf ETSI Konformität Überarbeitung der Kapitel 1, 2.2, 6, 7, 8 und A.2
2.0	21.11.2016	K.-H. Rödel Oliver Stegemann	Inhaltlich geprüft Umbrüche gesetzt, Rechtschreibung, fehlende Verweise aktualisiert, Kapitel 7.1.2 um Code Signing und Computer Zertifikate ergänzt Schrift Formatierung auf Tele-Grotesk
2.01	22.11.2016	K.-H. Rödel Tim Bauerdick Oliver Stegemann	Inhaltlich geprüft

Version	Stand	Autor/Bearbeiter	Änderungen/Kommentar
			Rechtschreibung, Anpassung Kapitel 1 (Aufteilung interne und öffentliche CAs), 1.4.1 (Austausch Grafik) und Ergänzungen in 7.1.2
2.02	22.11.2016	K.-H. Rödel Oliver Stegemann	Inhaltlich geprüft Freigabe
2.03	01.11.2017	K.-H. Rödel Oliver Stegemann	Jährliches Review, Inhaltlich geprüft Freigabe
2.1	18.04.2018	K.-H. Rödel Oliver Stegemann	Anpassungen Kapitel 1 ff und Kapitel 2 ff aufgrund der Inbetriebnahme neuer CAs Inhaltlich geprüft Freigabe
3.18	02.08.2018	Karl-Heinz Rödel	Vollständige Überarbeitung auf Basis ETSI Änderung CAs Umzug Trust Center Version für Review
3.19	02.08.2018	Oliver Stegemann	Qualitätssicherung/Review
3.20	03.08.2018	Karl-Heinz Rödel	Finalisierung, Freigabe und Veröffentlichung dieser Version
3.21	30.08.2018	Karl-Heinz Rödel	Anpassung Kapitel 3.23: 4.1.2.1; 5.2.3.2; 5.3.1.2; 5.3.2.2: 5.3.3.2: 5.3.4.2; 5.3.6.2; 5.3.8.2 Änderung von Registrierung auf Authentifizierung, bzw. Identifizierung.
3.22	25.09.2018	Karl-Heinz Rödel	Anpassung Kap. 3.2.3 und 3.2.5 BR-Fristen Kap. 1.3.1.2.1 Nutzungszeitraum Issuing CA 1 unter Globalroot Class 2 Kap. 1.5.4 doppelte Abschnitte gelöscht Anpassung Link zur cPKI Web-Seite auf https://corporate-pki.telekom.de im gesamten Dokument aktualisiert Kap. 4.10.1 OCSP RFC 2560 auf RFC6960 aktualisiert Kapitel 7 ff fehlender Text in den Fußnoten eingefügt
3.23	26.09.2018	Karl-Heinz Rödel	Ergänzung Kap. 6.7 um das Management von Benutzerzugriffsrechten und Änderung zur Anbindung Trust Center
3.24	10.10.2018	Karl-Heinz Rödel	Änderungen Aufgrund Anforderungen Mozilla 2.61 = CA-Communication Sept.2018 Update CP/CPS und CAB Ballot SC6 Version 3: Revocation Timeline Extension: Kapitel 1.3.1, 1.5.2, 2.1, 2.2, 2.4 und 3.1.1.1.6 ergänzt, In den Kapiteln 3.2.2.2.1, 3.2.5.2, 3.3, 4.2.2.1.1 und 6.3.2 wurde anstelle von „27 Monaten“ durch 825 Tage ersetzt, Kapitel 3.2.2.2 aktualisiert, Kapitel 3.2.5.2, 3.2.5.3, 4.1.2.2 aktualisiert, Kapitel 3.4 Internetadresse aktualisiert, Kapitel 4.3 aktualisiert, Kapitel 4.9.7, 4.9.1.1, 4.9.3.2, 4.10.1 aktualisiert, Änderungen in Kapitel 5 und 6, Kapitel 7.2 und 8 aktualisiert, Kapitel 9.17.1 hinzu gefügt, Kapitel 9.17.1 hinzu gefügt
3.25	05.11.2018	Karl-Heinz Rödel	Anpassungen Aufgrund Rückfragen TÜV: Aufnahme Kap. 9.17.1 Barrierefreiheit

Version	Stand	Autor/Bearbeiter	Änderungen/Kommentar
			Weitere Ausführungen zur Stellung des Zertifikatsantrags durch den Antragsteller und Zustimmung zu den Nutzungsbedingungen in Kap, 4.1.1 und 4.1.2.1
3.26	14.11.2018	Karl-Heinz Rödel	Anpassung Zertifikate für juristische Personen Kapitel 3.2.3, 3.2.3.5, 4.1.2.2.1, 4.1.2.4, 4.2.1.2, 4.2.3.2.1, 4.3.1.2.1 Aufnahme der Sicherstellung der Konsistenz der Daten der verschiedenen Auskunftsdienste (OCSP und CRL) 4.9.7
3.27	09.01.2019	Karl-Heinz Rödel	Anpassung Kapitel 3.1 Namensregeln und folgende. Aufgrund Aufnahme von GivenName und Surname für natürliche Personen in den SDN
3.28	28.01.2019	Oliver Stegemann	Review
4.00	07.02.2019	Kay Kirchhöfer	Freigabe

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 EINLEITUNG

Das Trust Center wird durch die Konzerneinheit T-Systems International GmbH (im Folgenden „T-Systems“ genannt) betrieben.

Im Jahr 1998 nahm das Trust Center (unter der Bezeichnung „Trust Center der Deutschen Telekom“) den Betrieb als erster Zertifizierungsdiensteanbieter auf, das über eine Akkreditierung nach dem deutschen Signaturgesetz (SigG) verfügte.

Zusätzlich zu den genau festgelegten und zertifizierten Arbeitsabläufen zeichnet sich das Trust Center der T-Systems durch einen sehr hohen Sicherheitsstandard aus. Die Vertrauenswürdigkeit des eingesetzten Trust-Center-Personals ist durch öffentliche Stellen überprüft worden. Alle Dienste sind Gegenstand regelmäßiger Qualitätskontrollen. Die eingesetzte Technologie ist Stand der Technik und wird laufend durch ausgebildete Administratoren überwacht.

Das Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Wurzel-Instanzen (Roots), sowohl für die Ausgabe qualifizierter als auch fortgeschrittener Zertifikate. Die Zertifizierungsstellen der Zertifikats-Dienstleistungen unterscheiden sich hinsichtlich der Anwendungskontexte für Zertifikate, der konkreten Ausprägung der technischen Schnittstellen, Registrierungsverfahren, der Zertifikatsprofile, der Prozesse bei Sperrungen, sowie der Veröffentlichung von Informationen.

Sowohl die bauliche als auch die organisatorische Infrastruktur erfüllt die strengen Anforderungen des deutschen Signaturgesetzes. Zu den vom T-Systems Trust Center angebotenen Leistungen gehört unter anderem der TeleSec Public Key Service (PKS), der die Ausstellung qualifizierter Zertifikate gemäß der europäischen eIDAS-Verordnung umfasst. Zusätzlich finden sich im Portfolio weitere Dienstleistungen zu unterschiedlichsten PKI-Lösungen, die nach den Vorgaben des Signaturgesetzes „fortgeschrittener Signaturen“ entsprechen; ferner Einmalpasswortverfahren und qualifizierte Zeitstempel.

Im Jahre 2013 wurde ein Informations-Sicherheits-Managementsystem (ISMS) für das T-Systems Trust Center etabliert, das gemäß ISO27001 auf Basis IT-Grundschutz zertifiziert ist. Das ISMS stellt Verfahren und Regeln zur Verfügung, um die Informationssicherheit zielgerichtet zu steuern, zu kontrollieren, zu überprüfen, dauerhaft verbessern zu können und aufrecht zu erhalten.

1.1 Überblick

1.1.1 Deutsche Telekom Corporate-PKI (cPKI)

Die Deutsche Telekom AG Corporate Public Key Infrastructure (im folgenden auch cPKI genannt) ist eine zentral im Trust Center der T-Systems betriebene PKI zur Generierung und Verwaltung von unterschiedlichen X.509v3-Zertifikatstypen, die insbesondere Einsatz finden bei E-Mail-Security, starker Authentifizierung (Client-Server), Remote-VPN, Servern und aktiven Netzkomponenten (z.B. Router, Gateways).

Mit der cPKI betreibt T-Systems International GmbH (im folgenden T-Systems genannt) als Verbundes Unternehmen (Affilate) für die Deutsche Telekom AG (im folgenden DTAG genannt) vertreten durch die Deutsche Telekom IT GmbH (im folgenden Auftraggeber genannt) eine vollständige PKI-Lösung, dessen Infrastruktur im hochsicheren T-Systems Trust Center installiert ist und von qualifiziertem Personal betrieben wird. Diese PKI erstellt und verwaltet Zertifikate als elektronische Identitätsnachweise für Mitarbeiter des Konzerns DTAG. Jeder Mitarbeiter erhält durch Verwendung der durch die PKI bereitgestellten Funktionen, die Möglichkeit sich an elektronischen Services zu verlässlich zu authentifizieren und mittels Signatur und Verschlüsselung (z.B. Medium E-Mail) auf sichere Art und Weise mit anderen Kommunikationspartnern Informationen auszutauschen.

Der Schwerpunkt der Aufgaben der cPKI sind die CA-Prozesse zur Ausstellung, Bereitstellung und Verwaltung von Zertifikaten nach X.509 Standard. Diese Prozesse gewährleisten eine integrierte Zertifikatsverwaltung in der Systeminfrastruktur der Deutschen Telekom und das Management des Schlüsselmaterials (Verschlüsselungsschlüssel) für die Interaktion mit IT-Systemen und Benutzern.

Alle Mitarbeiter der DTAG mit einem Active Directory (AD) Account in Deutschland erhalten einen, per zertifikatsbasierter SSL/TLS-Client-Authentifizierung gesicherten, dedizierten Zugang auf die cPKI, um die PKI-Funktionen nutzen können. Alle sicherheitsrelevanten Aktionen erfolgen über eine verschlüsselte Verbindung (HTTPS).

Unter der cPKI selbst sind unterschiedliche Sub-CAs subsummiert, die auch hierarchisch unterschiedlichen Stammzertifizierungsstellen unterstehen.

In Abbildung 1 ist die aktuell gültige Übersicht des PKI-Service „cPKI“ mit den Root- und Sub-CAs, aus denen Zertifikate ab Zertifikatsausstellungsdatum 18.04.2018 ausgestellt werden, grafisch dargestellt.

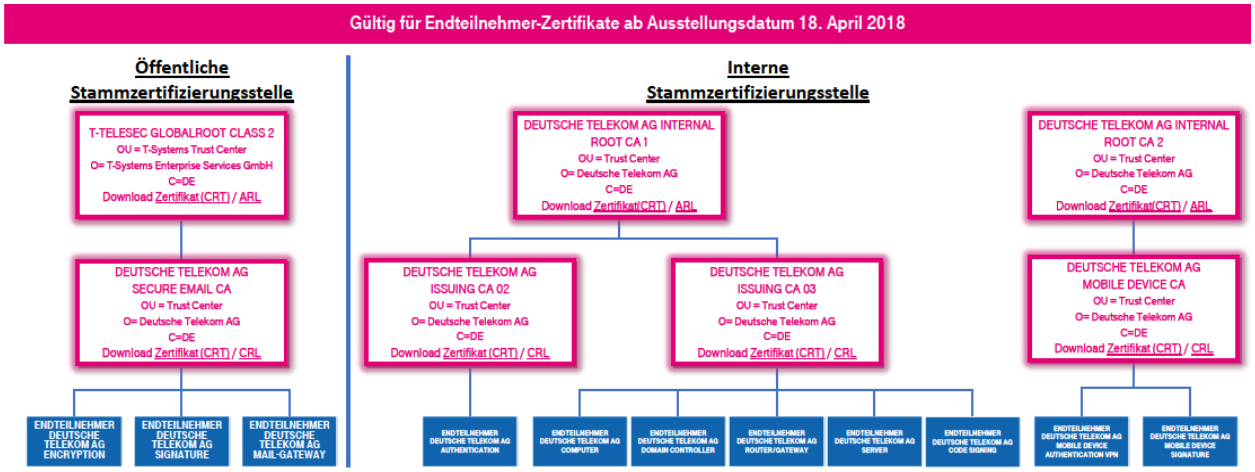

Abbildung 1: Übersicht des PKI-Service „cPKI“ mit den Root- und Sub-CAs ab Zertifikatsausstellungsdatum 18.04.2018

In Abbildung 2 ist die Übersicht des PKI-Service „cPKI“ mit den Root- und Sub-CAs, aus denen Zertifikate im Zeitraum 08. November 2016 bis zum 18. April 2018 ausgestellt wurden, grafisch dargestellt.

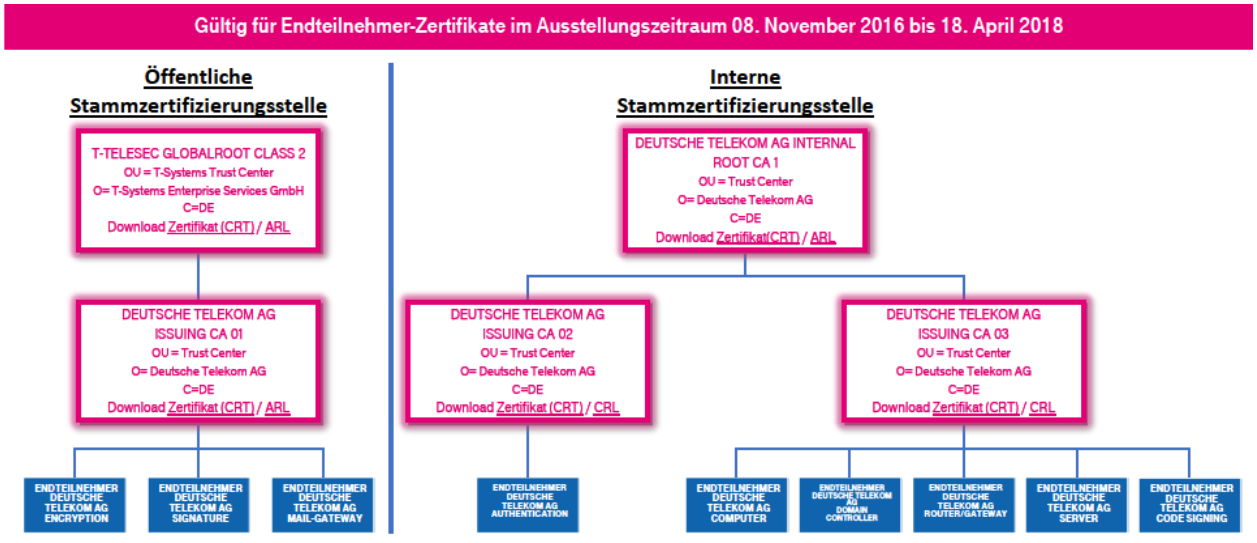

Abbildung 2: Übersicht der Root- und Sub-CAs im Zertifikatsausstellungzeitraum Zeitraum 08.11.2018 bis zum 18.04.2018

In Abbildung 3 ist die Übersicht des PKI-Service „cPKI“ mit den Root- und Sub-CAs, aus denen Zertifikate im Zeitraum April 2011 bis zum 08. November 2016 ausgestellt wurden, grafisch dargestellt.

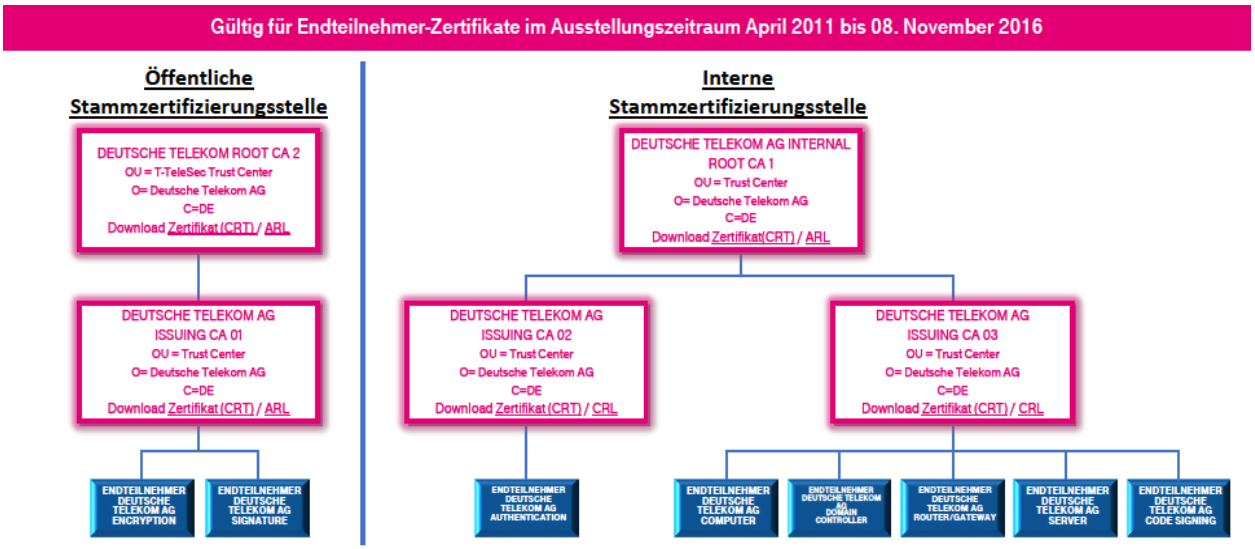

Abbildung 3: Übersicht der Root- und Sub-CAs im Zertifikatsausstellungzeitraum 04.2011 bis zum 08.11.2016

Für die jeweiligen Stammzertifizierungsstellen (Roots) bestehen jeweils eigene Zertifizierungsrichtlinien (engl. Certificate Policy, CP) und Erklärungen zum Zertifizierungsbetrieb (Certification Practice Statement, CPS).

Die Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) der DTAG Corporate Public Key Infrastructure (cPKI), im Folgenden kurz „CP/CPS“ genannt, der T-Systems beinhaltet Sicherheitsvorgaben sowie Richtlinien hinsichtlich technischer und organisatorischer Aspekte und beschreibt die Tätigkeiten des Trust Center Betreibers in der Funktion als Certification Authority (CA) und Registrierung der Endteilnehmer.

Es ermöglicht die qualitative Beurteilung der angebotenen Dienstleistung und dient als Entscheidungsgrundlage für eine Anerkennung der ausgestellten Zertifikate.

Im Einzelnen behandelt diese CPS die folgenden Regelungen:

- Veröffentlichungen und Verzeichnisdienst,
- Registrierung von PKI Teilnehmern,
- Ausstellung von Zertifikaten,
- Erneuerung von Zertifikaten (Re-Zertifizierung),
- Sperrung und Suspendierung von Zertifikaten,
- bauliche und organisatorische Sicherheitsmaßnahmen,
- technische Sicherheitsmaßnahmen,
- Zertifikatsprofile,
- Auditierung,
- Verbindliche Hinweise zur Zertifikatsnutzung und –Prüfung
- verschiedene Rahmenbedingungen.

Der formale Aufbau dieser CP/CPS folgt dem internationalen Standard RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ [RFC3647] der Internet Society.

Rechtliche und kommerzielle Aspekte der cPKI sind vertraglich im Konzern der DTAG geregelt.

Die nachfolgende Tabelle zeigt eine Übersicht der wesentlichen benutzerbezogenen Leistungsmerkmale:

Leistungsmerkmal	vorhanden
Signaturzertifikat (öffentliche Root)	X
Verschlüsselungszertifikat (öffentliche Root)	X
Authentifizierungszertifikat (interne Root)	X
Management Zertifikatslebenszyklus	X
Backup und Historie für Verschlüsselungs-zertifikate und -schlüssel	X
Self-Service Portal für Benutzer	X
Recovery von Verschlüsselungszertifikaten	X

Tabelle 1: Benutzerbezogene Leistungsmerkmale

Die nachfolgende Tabelle zeigt eine Übersicht der wesentlichen Leistungsmerkmale für Geräte und Mobile Devices aus der internen Zertifizierungsstelle:

Leistungsmerkmal	vorhanden
Authentifizierungszertifikat (interne CA) Geräte, Computer (802.1x) Zertifikate (interne CA)	X
Authentifizierung- und Signatur- Zertifikate für Benutzer auf Mobile Devices (interne CA)	X
Server-Zertifikate (interne CA)	X
Router/Gateway (interne CA)	X
Domain-Controller (interne CA)	X
Backup und Historie für Signaturzertifikate und -schlüssel für Mobule Devices (interne CA)	X
Self-Service Portal für Benutzer	X

Tabelle 2: Geräte- und Mobile Devices Bezogene Leistungsmerkmale

Personenzertifikate für interne und externe Mitarbeiter werden grundsätzlich unter Verwendung einer Smartcard (MyCard) als Schlüsselträgermedium ausgegeben. Eine Ausnahme ergibt sich bei Verwendung von Mobile Devices für Verschlüsselungszertifikate von MyCard Nutzern und Funktions- und Gruppen- Accounts, sowie Zertifikate für Maschinen und in diesem Zusammenhang benötigte Zertifikate (z.B. Authentifizierung), da das Deployment und die Nutzung softwarebasierend als sogenannte Software-Personell Security Environment (kurz SoftPSE) erfolgt.

1.1.2 Einhaltung der Baseline Requirements des CA/Browser-Forums

Das Trust Center der T-Systems stellt sicher, dass die Root-CA „Deutsche Telekom Root CA 2“ und „T-TeleSec GlobalRoot Class 2“ mit den jeweiligen untergeordneten Sub-CAs die Anforderungen und Regelungen der jeweils aktuellen veröffentlichten Version der [CAB-BR] (http://www.cabforum.org/documents.html) erfüllen und einhalten.

Des Weiteren stellt das Trust Center der T-Systems sicher, dass die Sub-CA „Deutsche Telekom AG secure email CA“ unter der öffentlichen Root CA die Anforderungen und Regelungen nach ETSI 319411-1 Policy LCP und ETSI 319401 erfüllt und einhält.

Im Falle eines Widerspruchs zwischen dem vorliegenden Dokument und den [CAB-BR] haben die Regelungen aus den [CAB-BR] Vorrang.

1.2 Name und Kennung des Dokuments

Name:	Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der cPKI
Version:	04.00
Stand	28.01.2019
OID dieser CP/CPS:	1.3.6.1.4.1.7879.13.26

Die Verwendung von weiteren von Objekt-Kennungen (Object Identifier, OID) sind in Kapitel 7.1.6 beschrieben

1.3 PKI Beteiligte

1.3.1 Zertifizierungsstellen

Die Zertifizierungsstelle (Certification Authority, CA) ist der Teil einer Public Key Infrastruktur, die Zertifikate ausstellt, verteilt und Prüfmöglichkeiten (Validierung) zur Verfügung stellt. Die Zwischenzertifizierungsstelle ihrerseits oder weitere Zwischenzertifizierungsstellen unterstehen hierarchisch einer Stammzertifizierungsstelle (Root-CA), die den „Vertrauensanker“ (Root-CA-Zertifikat) darstellt.

Für cPKI stehen, je nach Anforderung, unterschiedliche Stamm- und Zwischenzertifizierungsstellen (Root-CAs, Sub-CAs) zur Verfügung. Anforderungen an die Root-CAs sowie an die von der Root-CA ausgestellten Sub-CA-Zertifikate sind im CP/CPS der jeweiligen Root-CA dokumentiert.

Zwischenzertifizierungsstellen (Sub-CAs), die nicht mehr produktiv Endteilnehmer-Zertifikate ausstellen, werden bis auf weiteres noch für die Signatur von Sperrlisten und/oder OCSP-Antworten verwendet.

Die Stammzertifizierungsstelle (Root-CA) und die korrespondierende Zwischenzertifizierungsstelle (Sub-CA) kann variieren,

- wenn in der verwendeten Anwendung (z.B. Webbrowser) das Zertifikat der Stammzertifizierungsstelle noch nicht als vertrauenswürdig implementiert ist, oder
- wenn die verwendete Anwendung (z.B. Webbrowser) einer Validierungslogik folgt, die nicht auf die direkte Stammzertifizierungsstelle prüft.

In diesen Fällen wird optional auf eine andere definierte Stammzertifizierungsstelle referenziert.

Das Validierungsmodell basiert auf dem Schalenmodell, d.h. jedes Zertifikat ist maximal so lange gültig, wie das darüberliegende ausstellende Zertifikat gültig ist.

1.3.1.1 Stammzertifizierungsstellen

1.3.1.1.1 Öffentliche Stammzertifizierungsstelle

Das T-Systems Trust Center betreibt die „Deutschen Telekom Root CA 2“ und „T-TeleSec GlobalRoot Class 2“ Instanz für fortgeschrittene Zertifikatsdienste. Das Root-CA Zertifikat ist ein selbst-signiertes Zertifikat und wird durch T-Systems im Internet veröffentlicht. Die Veröffentlichung erlaubt eine Gültigkeitsüberprüfung aller in diesen Hierarchien ausgestellten Zertifikate über den Bereich des eigenen Intranets hinaus. Die Root-CA Instanz zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen. Im Falle der cPKI ist dies bis zum 18.04.2018 die „Deutsche Telekom AG Issuing CA 01“ und ab dem 18.04.2018 die „Deutsche Telekom AG secure email CA“

Die aktuelle Struktur der CA-Hierarchie der cPKI wird in der Abbildung 1: Übersicht des PKI-Service „cPKI“ mit den Root- und Sub-CAs ab Zertifikatsausstellungsdatum 18.04.2018 grafisch dargestellt.

Regelungen zur öffentlichen Stammzertifizierungsstelle sind in der CP bzw. CPS der „Deutschen Telekom Root CA 2“ [CP/CPS DTRCA2] und „T-TeleSec GlobalRoot Class 2“ [CP/CPS Class2] dokumentiert.

Weitere Informationen und die CP sowie das CPS der „T-TeleSec GlobalRoot Class 2“ finden sie unter https://www.telesec.de/de/public-key-infrastruktur/support/root-zertifikate/category/59-t-telesec-globalroot-class-2

In Tabelle 3 ist der vollständigen Subject Distinguished Name (Subject DN) der genannten Zertifizierungsstelle, gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch die Zertifikats-Gültigkeit dargestellt.

Aussteller (Issuer)		
Common Name (CN)	**Deutsche Telekom Root CA 2**	**T-TeleSec GlobalRoot Class 2**
Antragsteller (Subject)		
Country Name (C)	DE	DE
Organization Name (O)	Deutsche Telekom AG	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU)	T-TeleSec Trust Center	T-Systems Trust Center
Common Name (CN)	Deutsche Telekom Root CA 2	T-TeleSec GlobalRoot Class 2
Signaturhashalgorithmus:	sha1RSA	SHA-256
Schlüssellänge öffentlicher Schlüssel	2048	2048
Verschlüsselungsalgorithmus öffentlicher Schlüssel	RSA	RSA
Gültig von:	09.07.1999	01.10.2008
Gültig bis:	10.07.2019	01.10.2033
Fingerabdruckalgorithmus:	SHA-256	SHA-256
Fingerabdruck	B6 19 1A 50 D0 C3 97 7F 7D A9 9B CD AA C8 6A 22 7D AE B9 67 9E C7 0B A3 B0 C9 D9 22 71 C1 70 D3	91 E2 F5 78 8D 58 10 EB A7 BA 58 73 7D E1 54 8A 8E CA CD 01 45 98 BC 0B 14 3E 04 1B 17 05 25 52
Fingerabdruckalgorithmus	SHA-1	SHA-1
Fingerabdruck	85 a4 08 c0 9c 19 3e 5d 51 58 7d cd d6 13 30 fd 8c de 37 bf	59 0d 2d 7d 88 4f 40 2e 61 7e a5 62 32 17 65 cf 17 d8 94 e9

Tabelle 3: Subject DN „T-TeleSec GlobalRoot Class 2“

1.3.1.1.2 Interne Stammzertifizierungsstelle

Zur Ausstellung von Zertifikaten, für die eine Validierung außerhalb des Telekom Intranets nicht obligatorisch ist, wird im T-Systems Trust Center die „Deutschen Telekom Internal Root CA 1“ und „Deutsche Telekom Internal Root CA 2“ betrieben. Diese Root-CA Instanzen zertifizieren die im Kapitel 1.3.1.1.2 beschrieben Zwischenzertifizierungsstellen.

Regelungen zur internen Stammzertifizierungsstelle sind in der CP/CPS der „Deutschen Telekom Internal Root CA 1“ [CP/CPS DTIRCA1] dokumentiert.

In Tabelle sind die vollständigen Subject Distinguished Names (Subject DN) der genannten Zertifizierungsstellen, gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch die Zertifikats-Gültigkeit dargestellt.

Aussteller (Issuer)		
Common Name (CN)	Deutschen Telekom Internal Root CA 1	Deutschen Telekom Internal Root CA 2
Antragsteller (Subject)		
Country Name (C)	DE	DE
Organization Name (O)	Deutsche Telekom AG	T-Systems International GmbH
Organizational Unit Name (OU)	T-Systems Trust Center	Trust Center
Common Name (CN)	**Deutschen Telekom Internal Root CA 1**	**Deutschen Telekom Internal Root CA 2**
Signaturalgorithmus	SHA256	SHA256
Schlüssellänge öffentlicher Schlüssel	2048	2048
Verschlüsselungsalgorithmus öffentlicher Schlüssel	RSA	RSA
Gültig von:	15.11.2007	03.08.2017
Gültig bis:	16.11.2027	04.08.2037
Fingerabdruckalgorithmus:	SHA-256	SHA-256
Fingerabdruck:	E0 1A B4 F7 CE 75 0F F4 3B FE 52 13 78 79 FE 11 A0 83 66 CE 9C C5 40 75 1A 33 38 A4 9F BB 7B D4	C3 2A E6 04 47 39 1E 48 63 C2 44 55 1D EB C8 7B 40 FF 51 80 45 19 3E E4 67 33 86 57 9D 50 D0 FD
Fingerabdruckalgorithmus	SHA-1	SHA-1
Fingerabdruck	15 33 9a a2 30 f5 34 0e 7b fc aa fd 75 4a a1 4c ed d4 98 58	12 f7 14 bd ec 4d 2e 3c 27 82 ce 1f cb 8a fe 19 b8 4a ed 8c

Tabelle 4: Subject DN „Deutsche Telekom Internal Root CA 1“

1.3.1.2 Zwischenzertifizierungsstellen

1.3.1.2.1 Zertifizierungsstellen unterhalb einer öffentlichen Stammzertifizierungsstelle

Endteilnehmer-Zertifikate (z.B. für Benutzer, Mail-Gateway), deren Verwendungszweck eine „öffentliche Stammzertifizierungsstelle (Public Root)“ erfordert, werden von folgender untergeordneten Zertifizierungsstelle (Zwischenzertifizierungsstelle) ausgestellt:

- Deutsche Telekom AG Issuing CA 01
- Deutsche Telekom AG secure email CA

Im Falle, dass der Verwendungszweck von Zertifikaten nicht den Vorgaben einer „öffentlichen Stammzertifizierungsstelle“ genügen (z.B. für Computer, Router, Domain-Controller), oder Vorgaben bzw. Vorschriften (z.B. Root-Programme der Betriebssystem- und Browserhersteller, Baseline Requirements des CA/Browser-Forums [CAB-BR]) dies einschränken oder verhindern, werden diese Zertifikate von einer Zwischenzertifizierungsstelle ausgestellt, die hierarchisch der „Deutschen Telekom Internal Root CA 1“ oder „Deutschen Telekom Internal Root CA 2“ unterstehen

In Tabelle 5 ist der vollständige Subject Distinguished Name (Subject DN) der genannten Zertifizierungsstellen, gemäß den Namensformen nach Kapitel 3.1.1ff, als auch die Zertifikats-Gültigkeit dargestellt.

Der Common Name (CN) des Ausstellers (Issuer) referenziert auf die zuständige Stammzertifizierungsstelle.

Aussteller (Issuer)			
Common Name (CN)	Deutsche Telekom Root CA 2	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2
Antragsteller (Subject)			
Country Name (C)	DE	DE	DE
Organization Name (O)	T-Systems International GmbH	T-Systems International GmbH	Deutsche Telekom AG
Organizational Unit Name (OU)	T-Systems Trust Center	T-Systems Trust Center	Trust Center
Common Name (CN)	**Deutsche Telekom AG Issuing CA 01**	**Deutsche Telekom AG Issuing CA 01**	**Deutsche Telekom AG secure email CA**
Signaturalgorithmus	SHA-1RSA	SHA-256	SHA-256RSA
Schlüssellänge öffentlicher Schlüssel	2048	2048	2048
Verschlüsselungsalgorithmus öffentlicher Schlüssel	RSA	RSA	RSA
Gültig von:	14.04.2011	13.07.2016	18.01.2018
Gültig bis:	15.04.2019	14.07.2026	19.01.2028
Fingerabdruckalgorithmus:	SHA-256	SHA-256	SHA-256
Fingerabdruck:	DA ED C3 23 ED 85 FA CF B7 A0 3E E6 E3 5E B4 F6 11 9E 46 E9 22 7B B5 A3 AB 08 0A 06 85 07 7D CC	C6 19 30 77 C6 18 9D 1D FB BF 81 3B 87 DC 7C BF 04 98 AC F7 27 88 7B C7 EC 54 32 09 06 DE 9B C8	1A CF 28 AA 8C 53 03 EF E5 C3 01 18 62 39 36 B6 F5 01 F9 4D 3B B7 AD 35 B8 10 B7 64 34 5F 4F 01
Fingerabdruckalgorithmus	SHA-1	SHA-1	SHA-1
Fingerabdruck	79 a5 1c 3f 8e 83 23 72 e0 e0 9a d7 c3 3c 3f bd 5f 86 b0 3e	0b 76 71 e1 e6 68 a5 28 29 f8 a4 ef 67 7f 46 22 5c 9c e4 46	0a 0f 64 ea f7 22 fc 7c 9b 34 8b b5 09 2d ce 9e 74 27 99 73
Ausstellung von Endteilnehmer-Zertifikate	**Bis 08.11.2016**	**08.11.2016 bis 18.04.2018**	**Ab 18.04.2018**

Tabelle 5: Issuer und Subject DN „Deutsche Telekom Issuning CA 01" und „Deutsche Telekom AG secure email CA"

Von der Deutsche Telekom AG Issuing CA 01 unter der Deutsche Telekom Root CA 2 wurden Endteilnehmer-Zertifikate bis zum 08.11.2016 ausgestellt.

Von der Deutsche Telekom AG Issuing CA 01 unter der T-TeleSec GlobalRoot Class 2 wurden Endteilnehmer-Zertifikate vom 08.11.2016 bis zum 18.04.2018 ausgestellt.

Alle unter diesen CAs ausgestellten Endteilnehmer-Zertifikate behalten bis zum Ablauf dieser Zertifikate ihre Gültigkeit, es sei denn diese wurden aufgrund der in Kapitel 4.9.1 beschrieben Gründe für Widerruf/Sperrung vorzeitig gesperrt.

Endteilnehmer-Zertifikate ab dem 18.04.2018 werden durch die Deutsche Telekom AG secure email CA ausgestellt.

Relevant für die weitere Betrachtung betreffend die Einhaltung der Baseline Requirements des CA/Browser Forums sowie ETSI 319411-1 Policy LCP und ETSI 319401 sind lediglich die Deutsche Telekom AG Issuing CA 01 und Deutsche Telekom AG secure email CA, da nur diese von einer ETSI zertifizierten Stammzertifizierungsstelle, der „T-TeleSec GlobalRoot Class 2", ausgestellt wurde.

1.3.1.2.2 Zertifizierungsstelle unterhalb einer internen Stammzertifizierungsstelle

Endteilnehmer-Zertifikate (z.B. für Benutzer (SmartCard-LogOn), Computer, Authentifizierung und Signatur von Mobile Devices, Server, Code Signing, Router/Gateway, Domain-Controller), die die Verwendung einer „internen Stammzertifizierungsstelle (Internal Root)“ genügen, werden von folgenden untergeordneten Zertifizierungsstellen (Zwischenzertifizierungsstellen) ausgestellt:

- Deutsche Telekom AG Issuing CA 02
- Deutsche Telekom AG Issuing CA 03
- Deutsche Telekom AG mobile device CA

In Tabelle 6 ist der vollständige Subject Distinguished Names (Subject DN) der genannten Zertifizierungsstellen, gemäß den Namensformen nach Kapitel 3.1.1 ff, als auch die Zertifikats-Gültigkeit dargestellt.

Der Common Name (CN) des Ausstellers (Issuer) referenziert auf die zuständige Stammzertifizierungsstelle

Aussteller (Issuer)						
Common Name (CN)	Deutschen Telekom Internal Root CA 1	Deutschen Telekom Internal Root CA 1	Deutschen Telekom Internal Root CA 1	Deutschen Telekom Internal Root CA 1	Deutschen Telekom Internal Root CA 1	Deutschen Telekom Internal Root CA 2
Antragsteller (Subject)						
Country Name (C)	DE	DE	DE	DE	DE	DE
Organization Name (O)	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH
Organizational Unit Name (OU)	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center
Common Name (CN)	**Deutsche Telekom AG Issuing CA 02**	**Deutsche Telekom AG Issuing CA 02**	**Deutsche Telekom AG Issuing CA 02**	**Deutsche Telekom AG Issuing CA 03**	**Deutsche Telekom AG Issuing CA 03**	**Deutsche Telekom AG mobile device CA**
Signatur-hashalgorithmus	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256RSA
Schlüssellänge öffentlicher Schlüssel	2048	2048	2048	2048	2048	2048
Verschlüsselungs-algorithmus öffentlicher Schlüssel	RSA	RSA	RSA	RSA	RSA	RSA
Gültig von:	14.04.2011	13.07.2016	29.11.2016	14.01.2010	13.07.2016	18.01.2018
Gültig bis:	15.04.2019	14.07.2026	30.11.2026	15.01.2026	14.07.2026	19.01.2028
Fingerabdruckalgorithmus:	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256

Aussteller (Issuer)						
Fingerabdruck:	BE 31 BE E9 D6 CC C3 C2 C2 FB BD AF 37 3F FF C2 A9 A9 B6 17 AF C3 E3 72 AA 2A 68 8C 7F C6 C9 D9	3E 7C 3F C1 DC 26 83 11 A6 6C 86 22 37 8E F6 8C 58 B4 23 30 78 08 CB 4F AD 1C C9 35 9A 31 DC 42	A4 6D F4 E3 2B F5 2E 1° D5 30 5F CC A5 39 C2 CB F0 8D EE D0 76 39 CA 74 33 97 2D B7 C4 04 5E 17	23 41 6B 82 18 0F 5F FF 0A 9B 7B 13 96 4B 21 E4 71 C5 42 6° 12 92 93 15 FB 85 61 E2 E6 27 0B 62	C6 42 29 E7 89 2D F4 68 EC 59 95 08 77 43 4F FD 26 9A A8 90 A8 C7 8E 0B DC 7C C6 46 2B 1E E1 B4	38 D8 11 57 0D BD DC E5 0D 0A A4 9F 33 72 D5 22 1B BD B4 F2 A0 50 49 83 C7 17 01 0F 26 AA BA B4
Fingerabdruckalgorithmus	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1
Fingerabdruck	a4 65 65 16 29 36 52 fc b2 74 d0 50 88 e1 d4 40 9f ea 5d 70	66 e6 d5 09 80 92 7f 22 4e 2c fa 92 e5 6d fb 82 52 1d 7a 64	aa 12 85 4e eb 5f ad 13 c6 18 e0 81 8b cd 06 98 34 49 d3 b7	97 92 1a 0a e2 47 94 52 13 16 40 75 e1 28 1f 38 26 2d 11 82	a4 82 45 cd 46 0c 9a 9e b1 48 5d 80 3d 18 d0 2f f7 f8 94 a8	01 6b ab f7 5f 56 98 d0 96 a3 e0 13 61 d1 66 d9 20 df 5f 1f
Austellung von Endteilnehmer-Zertfikate	**Bis 08.11.2016**	**08.11.2016 bis 12.06.2017**	**Ab 12.06.2017**	**Bis 08.11.2016**	**Ab 08.11.2016**	**Ab 18.04.2018**

Tabelle 6: Issuer und Subject DN der internen Zertifizierungsstellen

Alle unter diesen CAs ausgestellten Endteilnehmer-Zertifikate behalten bis zum Ablauf dieser Zertifikate ihre Gültigkeit, es sei denn diese wurden aufgrund der in Kapitel 4.9.1 beschrieben Gründe für Wider-ruf/Sperrung vorzeitig gesperrt.

Endteilnehmer-Zertifikate für mobile Device werden je nach Verwendungszweck ab dem 18.04.2018 aus der internen Deutsche Telekom AG mobile device ausgestellt.

1.3.1.3 Zertifikate zur Unterstützung des PKI-Betriebs

1.3.1.3.1 Web-Server des PKI-Service „cPKI“

Der Zugriff der Endteilnehmer auf die PKI-Funktionen der cPKI erfolgt nur über das Intranet der DTAG. Der Web-Server der cPKI ist mit einem SSL-Zertifikat ausgestattet, so dass alle Aktionen über das sichere Protokoll HTTPS erfolgen. Die Funktionen werden nach erfolgreicher rollenbasierter Authentifizierung bereitgestellt.

In Abbildung 4 ist die Zertifikatshierarchie des Web-Servers „https://mycard-portal.telekom.de“ mit dem jeweiligen Zertifikat der Stammzertifizierungsstelle (Root-CA) und der Zwischenzertifizierungsstelle (Sub-CA) dargestellt. Dieser Web-Server ist nur aus dem Intranet der DTAG erreichbar.

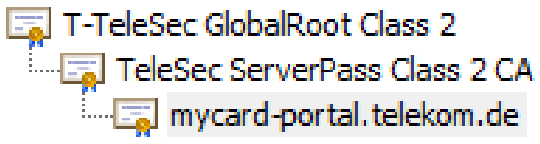

Abbildung 4: Übersicht der Zertifikatshierarchie des Webservers „mycard-portal.telekom.de"

1.3.1.3.2 OCSP-Responder des PKI-Service „cPKI“

Von jeder Sub-CA werden für die Erbringung des OCSP-Service Zertifikate für den OCSP-Responder ausgestellt. Dieser Zertifikatstyp steht ausschließlich nur dem PKI-Betreiber T-Systems zur Verfügung.

Technische Details zu OCSP sind in den Kapiteln 7.3 beschrieben.

1.3.2 Registrierungsstellen und vertrauenswürdige Datenbasis.

Eine Registrierungsstelle (Registration Authority, RA) ist eine Stelle, die die Authentifizierung von Zertifikatsantragstellern durchführt, Zertifikatsanträge bearbeitet (genehmigt, ablehnt, zurückgestellt), Sperranträge bearbeitet oder weiterleitet, ggf. Zertifikatserneuerungen als auch eine Kopie des Schlüsselmaterials (Soft-PSE) für einen Antragsteller erstellt. Grundsätzlich muss jede Registrierungsstelle gewährleisten, dass kein Unberechtigter in den Besitz eines entsprechenden Zertifikats gelangt.

Im Rahmen des PKI-Service cPKI sind folgende Registrierungsstellen etabliert:

- Interne automatische Registrierungsstelle auf Basis der HR Daten im Corporate Identity and Access Management System (cIAM) der DTAG
- Interne manuelle Registrierungsstelle im Trust Center der T-Systems

1.3.2.1 Interne automatische Registrierungsstelle

Das Zertifikatsmanagement System der cPKI verfügt über eine automatisierte Registrierungsstelle.

Voraussetzung hierfür ist, dass die Mitarbeiter der DTAG über HR in SAP-HR registriert werden und in das Corporate Identity Management System der DTAG (cIAM) hinterlegt wurden.

SAPHR und cIAM unterliegen

- Regelmäßige Durchführung von Audits mit dem Internal Control System (ICS IT) durch Externe Wirtschaftsprüfer,
- Durchführung und Freigabe in einem PRIVACY & SECURITY ASSESSMENT (PSA) Verfahren
- Durchführung von Penetrationstests durch Sicherheitsexperten der Telekom Security
- Zertifizierung nach ISO 27001

cIAM gilt daher im Konzern DTAG als vertrauenswürdige Datenbasis für das Zertifikats-Lifecyclemanagement der cPKI auf Basis der Anforderungen und Regelungen nach ETSI 319411-1 Policy LCP

Beteiligte Systeme:

- SAP HR Personalverwaltungssystem (HR-Systeme),
- CIAM (Corporate Identity & Access Management-System),
- Active Directory als zentrales Bezugsdirectory für die cPKI,
- TAdmin2 als Provisionierungsplattform für die cPKI.
- cPKI der DTAG

Siehe hierzu auch Abbildung 5: Authentifizierung einer natürlichen Person.

Die automatische Registrierungsstelle erfüllt insbesondere folgende Aufgaben:

- Entgegennahme von Zertifikatsanträgen,
- Prüfung der Anträge nach den vorgegebenen Richtlinien
- Freigabe dieser Zertifikatsanträge nach erfolgreicher Prüfung, ansonsten Ablehnung des Antrags,
- Beantragung des/der Zertifikat(e) in Folge der Freigabe eines Zertifikatsantrags,
- Authentifizierung von Antragstellern,
- Bereitstellung der Zertifikate an den Zertifikatsinhaber bzw. eine autorisierte Person
- Entgegennahme und Prüfung von Zertifikatssperrungsaufträgen
- Durchführung einer Zertifikatssperrung als Folge einer positiven Prüfung eines Sperrauftrags.

1.3.2.2 Interne manuelle Registrierungsstelle

Zusätzlich zur automatischen Registrierungsstelle verfügt die „Deutsche Telekom Issuing CA 01“ und die „Deutsche Telekom AG secure email CA“ über eine manuell betriebene Registrierungsstelle, welche für Zertifikatsnehmer (Endteilnehmer) oder aufgrund von unternehmensrechtlicher Gegebenheiten (Unternehmenssicherheit, gesetzliche Anforderungen) Kopien von Verschlüsselungszertifikaten und -schlüsseln von Zertifikatsinhabern für autorisierte Stellen (vertretende Personen) bereitstellt.

Des Weiteren prüft die manuelle Registrierungsstelle Zertifikatsaufträge die aufgrund von fehlerhaften oder nicht den Zulassungskriterien entsprechenden Daten von der automatischen Registrierungsstelle zurückgewiesen wurden, veranlasst ggf. eine Korrektur der Daten und ein neueinstellen des Auftrags.

Die manuelle Registrierungsstelle prüft zudem Zertifikatsanträge für Geräte, Router, Gateway oder Domänen-Zertifikate aus der internen Zertifizierungsstelle.

Die manuelle Registrierungsstelle erfüllt insbesondere folgende Aufgaben:

- Entgegennahme von Zertifikatsanträgen,
- Prüfung der Anträge nach den vorgegebenen Richtlinien,
- Freigabe dieser Zertifikatsanträge nach erfolgreicher Prüfung, ansonsten Ablehnung des Antrags,
- Beantragung des/der Zertifikat(e) in Folge der Freigabe eines Zertifikatsantrags,
- Entgegennahme des/der von der jeweiligen Zertifizierungsstelle erzeugten Zertifikat(e) und Bereitstellung an den Zertifikatsinhaber bzw. eine autorisierte Person,
- Entgegennahme und Prüfung von Zertifikatssperrungsaufträgen
- Durchführung einer Zertifikatssperrung als Folge einer positiven Prüfung eines Sperrauftrags.

1.3.3 Endteilnehmer (End Entity) / Zertifikatsnehmer

Im Kontext der cPKI werden unter Endteilnehmer alle Zertifikatsnutzer verstanden, auf die ein Zertifikat ausgestellt werden kann und selbst keine Rolle einer Zertifizierungsstelle repräsentieren. Diese sind im Einzelnen:

- natürliche Personen (Benutzer, Registratoren, Rolleninhaber, Pseudonym),
- Personen- und Funktionsgruppen,
- juristische Personen (z.B. Stiftungen bürgerlichen Rechts, Körperschaften des Privatrechts wie Aktien Gesellschaften, eingetragene Vereine, Gesellschaften mit beschränkter Haftung, eingetragene Genossenschaften),
- Geräte (z.B. Server, Router, Gateways, Mail-Gateways, Domain-Controller, Firewalls oder andere Geräte).

Zertifikatsberechtigte der cPKI im Kontext von natürlichen Personen sind:

- Beschäftigte der DTAG und Ihrer Tochterunternehmen,
- bei Bedarf deren jeweilige externe Mitarbeiterinnen und Mitarbeiter sowie
- bei Bedarf Geschäftspartner, die im Auftrag der Deutschen Telekom oder eines Ihrer Tochterunternehmen tätig sind.

Zertifikatsnehmer können dabei Personen mit einer persönlichen Email-Adresse, einem Pseudonym, sowie Verantwortliche von Funktionsgruppen (Funktionspostfachverantwortliche) oder Mitbenutzer von Funktionsgruppen (Zugriffsberechtigte von Funktionspostfächern) mit einer unpersönlichen Email-Adresse siehe Kapitel 1.4.1.3 und 1.4.1.4 sein.

Um den technischen Anforderungen gerecht zu werden, bietet die cPKI für die Endteilnehmer unterschiedliche Zertifikats-Typen an. Die folgende Tabelle 7 zeigt die Zuordnung der Typen zu den jeweiligen Endteilnehmern.

Zertifikatstyp	Anwendungsgebiet (Beispielhaft)	Endteilnehmer
Benutzer	Mail-Security (S/MIME), Anmeldung als TLS/SSL-Client an einer Web-basierenden Anwendung/Appliance, Anmeldung an einem Microsoft-Netzwerk, Anmeldung an einer Citrix-Appliance	natürliche Personen
Funktions- und Gruppenzertifikat	Mail-Security (S/MIME) für Funktionsmailpostfächer, Pseudonymaccounts zur Anmeldung als TLS/SSL-Client an einer Web-basierenden Anwendung/Appliance, Anmeldung an einem Microsoft-Netzwerk, Anmeldung an einer Citrix-Appliance	Personen- und Funktionsgruppen, Rolleninhaber, Pseudonyme
Domain Controller	Authentifikation der Anmeldestelle innerhalb eines Microsoft-Netzwerks	Geräte
Computer	Client Authentifikation an einem Microsoft-Netzwerk und VPN	Geräte, juristische Personen
Server	TLS/SSL-Server-Authentifikation	Geräte, juristische Personen
Router /Gateway	VPN, Authentifikation innerhalb von Router-Netzwerken	Geräte, juristische Personen
Mail-Gateway	Virtuelle Poststelle, Authentifikation Mail-Gateway/Appliance	Geräte, juristische Personen und Funktionsgruppen
Code Signing	natürliche Personen, Personen- und Funktionsgruppen, Rolleninhaber, Pseudonyme	natürliche Personen, Personen- und Funktionsgruppen, Rolleninhaber, Pseudonyme

Tabelle 7:Zuordung der Zertifikatstypen zu Endteilnehmer

In den folgenden Kapiteln wird weitestgehend der Namen des Zertifikatstyps als Synonym für den jeweiligen Endteilnehmer verwendet. D.h. unter Benutzer-Zertifikate werden die Zertifikate für natürliche Personen, unter Funktions- und Gruppen-Zertifikate werden Personen- und Funktionsgruppen, Pseudonyme und Rolleninhaber subsummiert, unter Geräte-Zertifikate werden alle Server-, Router/Gateway-, Mail-Gateway und Domain-Controller-Zertifikate verstanden!

Zertifikate für OCSP-Responder fallen auch unter Endteilnehmer, werden aber an dieser Stelle nicht weiter berücksichtigt, da sie nur zur Erbringung des Service cPKI verwendet, nicht aber dem Kunden zur Verfügung gestellt werden.

Der Verwendungszweck der Endteilnehmer-Zertifikate ist beschrieben in dem Kapitel 1.4. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

Im Gegensatz zu natürlichen Personen stimmt im Falle von Personen- und Funktionsgruppen, sowie Geräten das Subjekt (Zertifikatantragssteller) nicht mit dem Endteilnehmer überein, auf das sich das Zertifikat bezieht. Das Subjekt ist entweder der Endteilnehmer oder ein Gerät, das der Kontrolle des Endteilnehmers untersteht oder von diesem betrieben wird. Der Endteilnehmer ist Inhaber des privaten und öffentlichen Schlüssels und trägt letztendlich die Verantwortung für den Gebrauch des Zertifikats. Im Falle von natürlichen Personen stellt der Endteilnehmer gleichzeitig auch das Subjekt dar.

Als Endteilnehmer ist nicht die Deutsche Telekom als Auftraggeber oder Mandant zu verstehen. Ein Endteilnehmer ist daher nicht als Vertretungsberechtigter der DTAG oder deren Töchter oder Beteiligungen zur verstehen. Es ist aber

dennoch möglich, dass Repräsentanten auch ein Endteilnehmer-Zertifikat ausgestellt wird (z.B. Max Mustermann als Vertretungsberechtigter für die Deutsche Telekom AG).

Welche Bedeutung die Verwendung der Begriffe Endteilnehmer und Subjekt im Einzelfall haben, hängt daher vom Kontext ab, in dem die Begriffe verwendet werden.

1.3.4 Vertrauender Dritter

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

Unter vertrauende Dritte werden auch beispielsweise Software-Hersteller verstanden, die Root- und Sub-CA-Zertifikate der cPKI in die Zertifikatsspeicher integrieren.

1.3.5 Weitere Teilnehmer

Eine Personen- und Funktionsgruppe, eine juristische Person, als auch ein Gerät wird durch eine autorisierte Person verantwortet, die für diese Aufgabe von der Deutschen Telekom oder einer ihrer Töchter oder Beteiligungen bevollmächtigt ist. Die autorisierte Person (z.B. ein Funktionspostfachverantwortlicher) wird wie eine natürliche Persone identifiziert und registriert und ist verantwortlich für die sichere Verteilung, Nutzung und ggf. Sperrung des Zertifikates. Im Falle, dass die autorisierte Person nicht für die Verteilung oder Sperrung verantwortlich sein soll, wird diese Funktion auf den Rolleninhaber „Schlüsselverantwortlichen“ (siehe Kapitel 9.6.5) übertragen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Zertifikate der cPKI dürfen nur im zulässigen und geltenden gesetzlichen Rahmen verwendet werden. Dies gilt insbesondere unter Beachtung der länderspezifischen geltenden Ausfuhr- und Einfuhrbestimmungen. Des Weiteren ist eine Nutzung der Zertifikate den Mitarbeitern oder Beauftragten der DTAG nur im Rahmen ihrer dienstlichen Tätigkeit gestattet.

1.4.1.1 Sicherheitsniveau

Bei Zertifikaten mit mittlerem Sicherheitsniveau handelt es sich um Zertifikate, die sich für die Sicherung verschiedenster Geschäftsprozesse (z.B. digitale Signatur und Verschlüsselung von E-Mails) innerhalb und außerhalb Firmen, Organisationen, Behörden und Institutionen eignen, die ein mittleres Sicherheitsniveau zum Nachweis der Authentizität, Integrität und Vertraulichkeit des Endteilnehmers erfordern. Ferner sind die Zertifikate geeignet zur Endteilnehmer-Authentifizierung an Applikationen und Netzen oder zur Authentifizierung aktiven Netzwerkkomponenten untereinander.

In Tabelle 8 ist das Sicherheitsniveaus bezogen auf die Verwendungszwecke dargestellt.

Sicherheitsniveau:	Verwendungszweck:	
	Signatur und/oder Verschlüsselung	Authentifizierung
Mittel	✓	✓

Tabelle 8: Verwendung von Zertifikaten für Benutzer und Geräte

1.4.1.2 Zertifikate für Benutzer und Geräte

Die von der Corporate PKI zur Verfügung gestellten Zertifikate werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Erweiterungen „Schlüsselverwendung“ und „Erweiterte Schlüsselverwendung“ und den Festlegungen der CP/CPS eingesetzt. Voraussetzung ist aber, das ein vertrauender Dritter dem Zertifikat in angemessener Weise vertrauen kann und der Verwendungszweck nicht durch gesetzlich oder auf Grund von Einschränkungen dieser CP/CPS oder sonstigen Vereinbarungen verboten ist.

Einige Beispiele sind:

- Authentifizierung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPsec, S/MIME, XML-SIG, SOAP)
- Authentifizierung im Rahmen von Prozessen (Windows Log-On, Festplattenverschlüsselung)
- Verschlüsselung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPsec, S/MIME, XML-ENC, SOAP)
- Digitale Signatur im Rahmen von Kommunikationsprotokollen (z.B. S/MIME)

1.4.1.2.1 Benutzerzertifikate

Für natürliche Personen werden über automatisierte, gesicherte Workflows folgende Zertifikate als Trippel-Key zur Verfügung gestellt: Signatur, Verschlüsselung und Authentifizierung

Hierbei erfolgt die Authentifizierung der User durch die Personalstelle bei Einstellung des Mitarbeiters, bzw. bei Partnern und Externen Mitarbeitern durch die jeweilig verantwortlichen Bevollmächtigten.

Signatur-Zertifikat

Für das Signaturzertifikat wird ein auf der MyCard befindliches Schlüsselpaar verwendet. Dieses Schlüsselpaar wird bei der Produktion der MyCard aufgebracht, der private Teil des Schlüsselpaares ist besonders geschützt und nicht exportierbar. Die cPKI zertifiziert den öffentlichen Teil des gewählten Schlüsselpaares, gelangt jedoch niemals in den Besitz des privaten Schlüssels.

Verschlüsselungs-Zertifikat:

Für Verschlüsselung wird ein Key Pair in der cPKI erstellt und auf die MyCard aufgebracht (Schlüsselgenerierung und Distribution siehe Kapitel 6.1).
Die cPKI speichert hierbei das Schlüsselpaar und das Zertifikat geschützt in der Certification Authority ab.

Authentifizierungs-Zertifikat

Für das Authentifizierungszertifikat wird ein auf der MyCard befindliches Schlüsselpaar verwendet. Dieses Schlüsselpaar wird bei der Produktion der MyCard aufgebracht, der private Teil des Schlüsselpaares ist besonders geschützt und nicht exportierbar. Die cPKI zertifiziert den öffentlichen Teil des gewählten Schlüsselpaares, gelangt jedoch niemals in den Besitz des privaten Schlüssels.

Details und Anwendungsfälle zur Wiederherstellung von archivierten Schlüsselmaterial siehe Kapitel 4.12

1.4.1.2.2 Geräte (Computer, Server und Gateway Zertifikate)

Server und Gateway Zertifikate werden nicht durch eine CA, die den Richtlinien des CA Browserforums unterliegt, ausgestellt. Hierfür wird die interne CA3 verwendet. Näheres siehe 1.3.1

1.4.1.3 Zertifikate für Pseudonyme

Im Gegensatz zum standardmäßigen Anlegen eines Stammdatensatzes für eine natürliche Person werden für z.B. Testsysteme, Schulungen, Messerechner und Automaten, Accounts im HR-System angelegt, die nicht zu einer natürlichen Person gehören. Aus diesem Grund werden für diesen Zweck sog. Pseudonym-Accounts angelegt. Diese Accounts unterliegen bestimmten Anforderungen, die im Folgenden beschrieben werden.

Ein Pseudonym-Account hat die Eigenschaft, dass aus seinem im HR-System gepflegten Namen nicht hervorgeht, wer mit dem Account bzw. dem dahinterliegenden Zertifikat arbeitet. Dies kann in der Organisation vorkommen z. B. für Trainingsaccounts oder Funktionsaccounts für bestimmte Organisationseinheiten.

Eine Anforderung ist, dass solche Accounts einer bestimmten Nomenklatur folgen müssen, um identifizierbar zu sein und der verantwortliche Nutzer (Schlüsselverantwortlicher) hinter diesem Account leicht ermittelbar ist.

Eine eindeutige Identifizierung des Antragsstellers und des Zertifikatsinhabers muss jederzeit möglich sein.

Verantwortlich für die ordentliche Nutzung des Pseudonym-Accounts und der hierfür ausgestellten Zertifikate im Sinne eines Schlüsselverantwortlichen ist die Führungskraft bzw. der Leiter der Organisationseinheit dem der Stammsatz bzw. Accounts zugeordnet ist.

Bei deliktischem Handeln oder Straffällen wird diese Person zur Verantwortung gezogen. Dies kann arbeitsrechtliche, als auch strafrechtliche Konsequenzen zur Folge haben.

Der Zertifizierungsdiensteanbieter ist berechtigt die Identität eines Signaturschlüssel-, Verschlüsselungsschlüssel- und Authentisierungsschlüssel-Inhabers mit Pseudonym (Schlüsselverantwortlicher) an die zuständigen Stellen soweit dies der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Auflagen der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen zu übermitteln.

Zur Feststellung des Antragsstellers und der realen Identität des Zertifikatsnehmers ist die ausgebende Zertifizierungsstelle berechtigt alle hierfür erforderlichen Daten aus den Personalmanagementsystemen der DTAG (SAP HR) abzufragen bzw. in Ihren IT-Systemen zu speichern.

Die Zertifikate für Pseudonyme werden analog zu den Benutzerzertifikaten als Trippel Key ausgestellt, sind jedoch mit „PN-“ im Zertifikat als Pseudonym Zertifikate gekennzeichnet (siehe Kapitel 3.1.3)

1.4.1.4 Funktions-/Gruppenzertifikate

In bestimmten Fällen ist es erforderlich, dass verschlüsselte Nachrichten von unterschiedlichen Empfängern gelesen werden müssen.

Dies ist unter anderem der Fall:

- Wenn mehrere Personen gemeinsam eine Rolle wahrnehmen,
  z. B. im Kundenservice, Vertrieb oder einer zentralen Maileingangsstelle.
- Wenn das Zertifikat an eine Funktion nicht aber an eine Person gebunden ist.
- Wenn wegen zeitkritischer Abläufe eine Vertretung sichergestellt sein muss, der Absender diese aber nur mit großem Aufwand feststellen kann und Geschäftsprozesse durch Nicht-Erreichbarkeit gestört werden könnten.
- Wenn automatisierte IT-Prozesse verschlüsselte Mails empfangen sollen, bzw. eine automatisierte Verarbeitung durch eine Applikation erfolgt.
- Wenn automatisierte IT-Prozesse signierte Mails versenden sollen, z.B. automatisierter Rechnungsversand der DTAG

Signatur-und Verschlüsselungs-Zertifikat (Single Key)

Für Verschlüsselung und Signatur wird ein wird ein Key Pair (Single Key) in der cPKI erstellt und auf die MyCard aufgebracht (Schlüsselgenerierung und Distribution siehe Kapitel 6.1).
Die cPKI speichert hierbei das Schlüsselpaar und das Zertifikat geschützt in der Certification Authority ab.

Dazu kann ein Schlüsselpaar mit einem entsprechenden Zertifikat von einer Gruppe gemeinsam zum Signieren und verschlüsseln verwendet werden.

Die Signaturen sind dann als Integritätssicherung im Sinne eines Firmen-Stempels für die Mitglieder der Gruppe zu verstehen.

Wenn die Sicherheitsanforderungen den Anwendungsfall zulassen, bietet es sich in solchen Situationen an, ein Schlüsselpaar für mehrere Personen zu verwenden. Dazu wird ein Schlüsselpaar mit Zertifikat erzeugt. Der Zugriff auf den geheimen Schlüssel wird aber, anders als für persönliche Schlüsselpaare, mehreren Personen eingeräumt. Ob von den Gruppenmitgliedern eine oder mehrere PSEs, Hardware- oder Software-PSEs, individuelle oder gemeinsame Passwörter für den Zugriff auf den privaten Schlüssel, bzw. dem Zertifikat verwendet wird, hängt vom jeweiligen Anwendungsfall ab.

Beispiel 1:

Für ein Funktionspostfach soll ein Schlüsselpaar mit Zertifikat erstellt werden und die Mitarbeiter mit Zugriffsberechtigung auf diesem Funktionspostfach das entsprechende Schlüsselpaar für das entschlüsseln, verschlüsseln und signieren von Emails aus diesem Funktionspostfach zur Verfügung gestellt werden.

Dazu beantragt der Funktionspostfachverantwortliche (Inhaber) ein Zertifikat für dieses Funktionspostfach auf dem cPKI Portal. Hierzu ist zwingend eine Zertifikatsbasierende Anmeldung mittels der persönliche MyCard des Inhabers an das cPKI Portal erforderlich. Diese Anmeldung wird gegen die cPKI geprüft. Des Weiteren wird in den Backendsystemen der Deutschen Telekom geprüft, ob es sich tatsächlich um den Funktionspostfachverantwortliche handelt. Bei einer erfolgreichen Validierung der Anmeldedaten und der Inhaberschaft des Funktionspostfaches kann ein Zertifikat (Schlüsselpaar für Signatur und Verschlüsselung) für dieses Funktionspostfach beauftragt werden. Der Auftrag wird zur Sicherstellung der Integrität der Beauftragung mit dem persönlichen Signaturzertifikat des Postfachverantwortlichen signiert und revisionssicher in der cPKI abgespeichert.

Durch die die Erstellung eines Schlüssels für dieses Funktionspostfaches wird der Inhaber dieses Postfaches zum Schlüsselverantwortlichen.

In einem zweiten Schritt wählt der Schlüsselverantwortliche die Mitarbeiter aus, denen die PSE auf die MyCard geschrieben werden sollen.

Die ausgewählten Funktionspostfachnutzer (Mitarbeiter) werden anschließend per Mail benachrichtigt und können die Zuweisung verweigern oder annehmen. Bei Annahme wird die PSE für das Funktionspostfach auf die persönliche MyCard des Funktionspostfachnutzers geschrieben. Die Nutzung dieses Zertifikat bzw. des privaten Schlüssels auf der persönlichen MyCard des Funktionspostfachnutzers ist nur mit der persönlichen PIN der MyCard möglich, ein gemeinsames Passwort/PIN ist hiermit ausgeschlossen.

Beispiel 2:

Eine Applikation, die verschlüsselte E-Mails empfangen, versenden oder signieren soll, benötigt ein Schlüsselpaar.

Hier kommt bei der Deutschen Telekom ein Applikations-Encryption Gateway zum Einsatz (Email Encryption Gateway). Für dieses Gateway wird das Schlüsselpaar als Soft-PSE benötigt.

Der Applikationsverantwortliche muss hierzu einen schriftlichen Antrag an die RA der Deutschen Telekom stellen, nach Prüfung der Identität und der Vollmacht stellt der RA-Platz eine Software-PSE für diese Applikation aus. Diese Software-PSE wird dem Applikationsverantwortlichen, der dadurch zum Schlüsselverantwortlichen wird verschlüsselt übergeben. Die Verschlüsselung erfolgt für das persönliche Zertifikat des Schlüsselverantwortlichen. Des Weiteren wird im in einer gesonderten Mail das Passwort zur Soft-PSE ebenfalls verschlüsselt übermittelt.

Über das Applikations-Encryption Gateway wird ein Zugang für die E-Mailadresse seiner Applikation freigeschaltet.

Anschließend kann der Schlüsselverantwortliche das Schlüsselpaar in das Applikations-Encryption Gateway laden.

1.4.2 Unzulässige Zertifikatsnutzung

Zertifikate der cPKI dürfen nicht im Rahmen folgender Zwecke verwendet werden:

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

Es ist verboten Endteilnehmer-Zertifikate als CA- oder Root-CA-Zertifikate zu verwenden.

Die Zertifikate der Corporate PKI unterstützen nicht das Attribut „Nichtabstreitbarkeit (non Reputation)“ in Verbindung mit einer Identität oder Berechtigung.

1.5 Verwaltung der Richtlinie

1.5.1 Zuständigkeit für die Erklärung

Diese CP/CPS wird herausgegeben von:

T-Systems International GmbH

Telekom Security, Portfolio Management, Engineering & Operations,
Trust Center & ID-Solutions, Trust Center & ID-Solutions 1

Untere Industriestraße 20

57250 Netphen

Deutschland

1.5.2 Kontaktinformationen

T-Systems International GmbH
Telekom Security, Portfolio Management, Engineering & Operations,
Trust Center & ID-Solutions, Trust Center & ID-Solutions 1

Untere Industriestraße 20

57250 Netphen

Deutschland

Telefon: +49 (0) 1805-268204[1]

E-Mail: telesec_support@t-systems.com

Intranet und Internet: https://corporate-pki.telekom.de/

Die Meldung von Missbrauch, Kompromittierung von Zertifikaten und Schlüsseln des T-Systems 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 T-Systems frühzeitig erfolgen kann und adäquate Maßnahmen eingeleitet werden können. T-Systems meldet sich in der Regel innerhalb von 24h mit einer ersten Einschätzung über die angegebenen Kommunikationskanäle. T-Systems 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 Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP entscheidet

In Kapitel 1.5.1 ist die Organisation aufgeführt, die sich verantwortlich zeigt, dass diese CP/CPS oder Dokumente, die dieses Dokument ergänzen oder untergeordnet sind, mit der Zertifizierungsrichtlinie (Certificate Policy, CP) vereinbar sind.

1.5.4 Genehmigungsverfahren dieser CP/CPS

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

[1] Festnetz: 0,14 €/Minute, Mobilfunknetz: max. 0,42 €/Minute

Der in Kapitel 1.5.1 benannte Herausgeber ist für dieses Dokument (CP/CPS) verantwortlich. Die Freigabe erfolgt durch einen formalen Dokumentenfreigabeprozess.

Relevante Änderungsanforderungen oder Änderungen des laufenden PKI-Betriebs der cPKI werden rechtzeitig fachlich bewertet und auf die Einhaltung dieser und der übergeordneten CP/CPS der „T-TeleSec GlobalRoot Class 2“, „Deutsche Telekom Internal Root CA 1“ und „Deutsche Telekom Internal Root CA 2“ hin überprüft. Im Bedarfsfall werden die Änderungen in das jeweilige Dokument eingearbeitet.

Darüber hinaus erfolgt mindestens einmal jährlich ein Dokumentenreview, auch wenn keine inhaltlichen Änderungen vorgenommen werden müssen.

Verantwortlich für die Bewertung der Änderungsanforderung als auch Durchführung bzw. die Koordination des Reviews ist der in Kapitel 1.5.2 benannte Bereich.

Die Änderungshistorie wird entsprechend aktualisiert.

1.6 Akronyme und Definitionen

Akronyme und Begriffsdefinitionen finden Sie in Kapitel C

2 VERÖFFENTLICHUNGEN UND VERZEICHNISDIENSTE

2.1 Verzeichnisdienste (Repositories)

T-Systems betreibt für den Dienst cPKI einen Verzeichnisdienst und eine zentrale Datenablage. T-Systems ist für deren Inhalte verantwortlich.
Extrakte dieser Datenbanken stellen in aufbereiteter Form die Basis dar, um Zertifikatsinformationen und Zertifikatssperrlisten (CRL) auf dem Verzeichnisdienst zu veröffentlichen oder den Validierungsdienst Online Certificate Status Protocol (OCSP)-Responder) mit Statusinformationen zu versorgen.

Weiterhin werden für die Öffentlichkeit relevante Dokumente in Form einer zentralen Datenablage (Repository) zur Verfügung gestellt. Dies umfasst insbesondere die entsprechenden CP/CPS der beteiligten Stamm- und Zwischenzertifizierungsstellen (Root- und Sub-CAs). Dieses Verzeichnis ist 7x24h Stunden verfügbar.

T-Systems setzt geeignete Mechanismen zum Schutz der zentralen Datenablage (Repository) gegen nicht autorisierte Manipulationsversuche (hinzufügen, löschen, ändern) ein.

2.2 Veröffentlichung von Zertifikatsinformationen

T-Systems veröffentlicht in regelmäßigen Abständen Zertifikatssperrlisten (CRL), in der alle von der cPKI gesperrten Zertifikate und deren Sperrdatum und -zeitpunkt enthalten sind. Es werden nur Zertifikate gesperrt, die zum Sperrzeitpunkt gültig sind.

In der Sperrliste für Zertifizierungsstellen (CARL) werden alle gesperrten CA-Zertifikate (jedoch keine Root-CA-Zertifikate) veröffentlicht.

T-Systems veröffentlicht alle von der cPKI ausgestellten Endteilnehmer-Zertifikate auf einem internen Verzeichnisdienst im INTRANET der DTAG. Der Verzeichnisdienst hat die Aufgabe, an einem zentralen Ort alle zur Veröffentlichung anstehenden Zertifikate als auch die aktuellen Sperrinformationen per standardkonformer Sperrlisten (CRL, CARL), zur Verfügung zu stellen. Wobei die die Sperrinformationen für alle PKI-Beteiligten und die Zertifikate nur DTAG intern veröffentlicht werden. Der Zugriff auf den Verzeichnisdienst erfolgt über das Protokoll LDAP (Lightweight Directory Access Protocol) und ist hinsichtlich Zugriffsschutz konfigurierbar (öffentlich oder Benutzername/Passwort-Schutz). Des Weiteren sind die Zertifikate intern in der Global Address List des DTAG Active Directorys sowie im Konzernverzeichnis der DTAG für Mitarbeiter des Konzerns abrufbar.

Ferner stellt die cPKI einen Validierungsdienst (OCSP-Responder) zur Verfügung, der über das Internetprotokoll „Online Certificate Status Protocol“ (OCSP) einem Anfragenden den Status von cPKI-Zertifikaten zurück liefert.

Die Adresse des OCSP-Responders ist im Zertifikat eingetragen und wird zusätzlich in diesem Dokument veröffentlicht.

T-Systems veröffentlicht die aktuellen CP/CPS als auch die CA- und Root-CA-Zertifikate unter:

https://corporate-pki.telekom.de/

Das Root-CA-Zertifikat der „T-TeleSec GlobalRoot Class 2“ ist in den gängigen Zertifikatsspeichern von Betriebssystemen und Applikationen als „Vertrauensanker“ vorinstalliert bzw. wird online nachinstalliert und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten.

Die Veröffentlichung der Zertifikate ist abhängig vom Zertifikatstyp und den Regelungen gemäß Tabelle 7.

Zertifikatstyp/Aussteller:	Vorgaben:
Root-CA-Zertifikat „Deutsche Telekom Root CA 2“	Dieses Zertifikat ist in den gängigen Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert bzw. wird online nachinstalliert und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Deutsche Telekom AG Issuing CA 01	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Root CA 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Root-CA-Zertifikat „T-TeleSec GlobalRoot Class 2“	Dieses Zertifikat ist in den gängigen Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert bzw. wird online nachinstalliert und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Deutsche Telekom AG Issuing CA 01	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „T-TeleSec GlobalRoot Class 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Deutsche Telekom AG secure email CA	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „T-TeleSec GlobalRoot Class 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Root-CA-Zertifikat „Deutsche Telekom Internal Root CA 1“	Dieses Zertifikat ist nicht in den Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert, sondern muss zusätzlich nachinstalliert werden. Das Root-CA-Zertifikat unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Deutsche Telekom AG Issuing CA 02	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 1“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Deutsche Telekom AG Issuing CA 03	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 1“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Root-CA-Zertifikat „Deutsche Telekom Internal Root CA 2“	Dieses Zertifikat ist nicht in den Zertifikatsspeichern von Betriebssystemen und Applikationen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert, sondern muss zusätzlich nachinstalliert werden. Das Root-CA-Zertifikat unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.
Deutsche Telekom AG mobile device CA	Dieses Sub-CA-Zertifikat wurde von der Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 2“ ausgestellt und unterstützt dabei die Zertifikats-Validierung bei Endteilnehmer und vertrauenden Dritten. Bei Bedarf kann das Zertifikat der cPKI über das Intranet oder per Internet abgerufen werden.

Zertifikatstyp/Aussteller:	Vorgaben:
Zertifikate für Endteilnehmer aus einer CA unter der öffentlichen Root	Eine Veröffentlichung dieser Zertifikate erfolgt nur auf DTAG internen Verzeichnisdiensten, dies sind aktuell die Global Address List der DATG, dem Konzernverzeichnis der DTAG und dem internen cPKI LDAP. In Abstimmung mit dem Mandanten DTAG können jedoch die Zertifikate in weiteren Verzeichnisdiensten im Intranet der DATG veröffentlicht werden. Auf dem cPKI LDAP können von angeschlossenen Applikationen über LDAP Zertifikate gesucht werden.
Zertifikate für Endteilnehmer aus einer CA unter der internen Root	Eine Veröffentlichung dieser Zertifikate erfolgt derzeit nicht. In Abstimmung mit dem Mandanten DTAG können jedoch zusätzliche Zertifikatstypen im Intranet der DATG veröffentlicht werden.
OCSP-Zertifikate	Die Zertifikate stehen nicht zum Herunterladen zur Verfügung.

Tabelle 9: Vorgaben für die Veröffentlichung von Zertifikaten

Die o.g. Informationen werden auf der Webseite des Zertifizierungsdiensteanbieters für die cPKI unter https://corporate-pki.telekom.de/ veröffentlicht.

Zusätzlich erfolgt bei sicherheitskritischen Vorfällen eine direkte Benachrichtigung der bekannten Ansprechpartner des Auftraggebers innerhalb der DTAG in schriftlicher Form oder per E-Mail.

Änderungen der Informationssicherheitspolitik der cPKI werden den Bewertungsstellen/Auditoren (Kapitel 8 ff) und der Aufsichtsbehörde (Weiterleitung von Konzernlagezentrum der DTAG an BSI, BNetzA) mitgeteilt.

Zusätzlich zu den oben genannten CAs werden zwei Entwicklungs- und Test- und Abnahmeumgebung in gekapselten Netzwerken der DTAG betrieben (z.B. für Software-Entwickler, sowie für Tests und Abnahmen)

Diesen Umgebungen sind Produktionsnah mit allen für die cPKI erforderlichen Infrastrukturkomponenten der DTAG aufgebaut. Zertifikate und CRL und CARL stehen innerhalb dieser Umgebungen für die Zertifikatsvalidierung und der die Auskunft über den Status (gültig, gesperrt und abgelaufen) zur Verfügung.

Root, Intermediate- und Issuing CA- sowie Endteilnehmer-Zertifikate werden nicht außerhalb dieser Entwicklungs-, Test- und Abnahme Umgebungen veröffentlicht und sind nicht über das Internet erreichbar.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Aktualisierungen des CP/CPS werden wie in Kapitel 9.12 beschrieben veröffentlicht und in der Änderungshistorie vermerkt.

Das vorliegende CP/CPS wird, unabhängig von weiteren Änderungen, einer jährlichen Überprüfung (Review) unterzogen. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden.

Aktuelle Entwicklungen, Änderungen und geänderte Anforderungen (zum Beispiel durch CABF-BR) werden verfolgt und in der Releaseplanung berücksichtigt.

Verantwortlich für die Durchführung bzw. die Koordination des Reviews ist die in Kapitel 1.5.1 benannte Stelle.

Zertifikate für die eine Veröffentlichung vorgesehen ist, werden zum Zeitpunkt der Erzeugung veröffentlicht. Je nach Replikationszeit der DTAG internen Systeme wie der Global Address List kann es bis zu 12 Stunden dauern bis neu ausgestellte Zertifikate allen DTAG Usern zur Verfügung stehen. Endteilnehmerzertifikate werden nur im Intranet der DTAG veröffentlicht.

Die Sperrlisten als auch OCSP-Antworten werden wie in Kapitel 4.9.7 beschrieben veröffentlicht.

2.4 Zugänge zu Verzeichnisdiensten (Repositories)

Der Abruf der Sperrlisten (CRL, CARL) und die Nutzung des OCSP-Dienstes für die Endteilnehmer (Kapitel 1.3.3), vertrauende Dritte (Kapitel 1.3.4) oder Registrierungsstellen (Kapitel 1.3.2), unterliegen keiner Zugriffskontrolle.

Die Integrität und Authentizität der Sperrlisten und OCSP-Auskünfte wird durch die digitale Signatur mit vertrauenswürdigen Signern gewährleistet (Kapitel 4.10.1).

Das Suchen von Zertifikaten über den Verzeichnisdienst und Lesezugriff auf diese Informationen innerhalb des DTAG Netzwerkes unterliegt grundsätzlich keiner Zugriffskontrolle. Zusätzlich zu dem Verzeichnisdienst der cPKI können DTAG Mitarbeiter sich Zertifikate über die Global Address List (GAL) mittels Aufruf eines Kontakteintrages anzeigen lassen. Das Suchen von Endteilnehmer-Zertifikaten aus dem Internet ist jedoch nicht möglich.

Der lesende Zugriff durch Zertifikatsnehmer und -nutzer auf Informationen der Stamm- und Zwischenzertifizierungsstellen-Zertifikaten (Root- und Intermediate-CA) und der veröffentlichten CP/CPS (siehe Kapitel 2.1 und 2.2) über einschlägige Webseiten unterliegt keiner Zugriffskontrolle.

Die Veröffentlichung der Zwischenzertifizierungsstellen Deutsche Telekom AG Issuing CA 01 – 03, sowie Deutsche Telekom AG secure email CA und Deutsche Telekom AG mobile device CA erfolgt wie in den nachfolgenden Tabellen dargestellt:

Die Bereitstellung von Sperrlisten erfolgt über den LDAP-Server der cPKI oder das Active Directory der jeweiligen Windows-Domäne.

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA
CRL Distribution Points (CDP)			
CDP [1] http	URL=http://cpki.telekom.de/cdp/Deutsche%20Telekom%20Root%20CA%202.crl	URL=http://crl-cpki.telekom.de/rl/GlobalRoot_Class_2.crl	URL=http://crl-cpki.telekom.de/rl/GlobalRoot_Class_2.crl
CDP [2] ldap	URL=ldap://ldap-cpki.telekom.de/cn=Deutsche%20Telekom%20Root%20CA%202,ou=T-TeleSec%20Trust%20Center,o=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=LDAP://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?authorityRevocationList
CDP [3] AD	-	-	-
Deutsche Telekom AG Employee Encryption	X	X	X
Deutsche Telekom AG Employee Signature	X	X	X
Deutsche Telekom AG Employee Authentication	-	-	-
Deutsche Telekom AG External Workforce Encryption	X	X	X

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA
Deutsche Telekom AG External Workforce Signature	X	X	X
Deutsche Telekom AG External Workforce Authentication	-	-	-
Deutsche Telekom AG Funktionsgruppen Encryption	X	X	X
Deutsche Telekom AG Funktionsgruppen Signature	X	X	X
Deutsche Telekom AG Telekom Computer	-	-	-
Deutsche Telekom AG Domain Controller	-	-	-
Deutsche Telekom AG Print Server	-	-	-
Deutsche Telekom AG Code Signing	-	-	-
Deutsche Telekom AG OCSP Signing	X	X	X
Archivierung des privaten Schlüssels	X	X	X

Tabelle 10: Zuordnung der Zertifikate zu den CAs und den jeweiligen CRL Distribution Points für Zertifikate aus der öffentlichen Stammzertifizierungsstelle

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA
CRL Distribution Points (CDP)			
CDP [1] http	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_1.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_1.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_2.crl
CDP [2] ldap	URL=LDAP://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=LDAP://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList
CDP [3] AD	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Ser	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Ser	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Ser

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA
	vices,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	vices,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	vices,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint
Deutsche Telekom AG Employee Encryption	-	-	-
Deutsche Telekom AG Employee Signature	-	-	-
Deutsche Telekom AG Employee Authentication	X	-	-
Deutsche Telekom AG External Workforce Encryption	-	-	-
Deutsche Telekom AG External Workforce Signature	-	-	-
Deutsche Telekom AG External Workforce Authentication	X	-	-
Deutsche Telekom AG Funktionsgruppen Encryption	-	-	-
Deutsche Telekom AG Funktionsgruppen Signature	-	-	-
Deutsche Telekom AG Telekom Computer	-	X	-
Deutsche Telekom AG Domain Controller	-	X	-
Deutsche Telekom AG Print Server	-	X	-
Deutsche Telekom AG Code Signing	-	X	-
Deutsche Telekom AG Mobile Device Authentifizierungszertifikat für VPN	-	-	X
Deutsche Telekom AG Mobile Device Signature für Email Signatur auf Mobile Devices	-	-	X
Deutsche Telekom AG OCSP Signing	X	X	X
Archivierung des privaten Schlüssels	X	X	X

Tabelle 11: Zuordnung der Zertifikate zu den CAs und den jeweiligen CRL Distribution Points für Zertifikate aus der internen Stammzertifizierungsstelle

Bereitstellung von Zertifikatsstatusdaten über das OCSP-Protokoll

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA
Authority Information Access (AIA)			
AIA [1] ocsp (OCSP Access (1.3.6.1.5.5.7.48.1))	URL=http://ocsp-cpki.telekom.de/ocsp	URL=http://ocsp-cpki.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr
AIA [2] http (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=http://corporate-pki.telekom.de/aia/Deutsche%20Telekom%20Root%20CA%202.crt	URL=http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	URL=http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer
AIA [3] ldap (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Root%20CA%202,OU=T-TeleSec%20Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=LDAP://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
AIA [4] AD (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	-
Deutsche Telekom AG Employee Encryption	X	X	X
Deutsche Telekom AG Employee Signature	X	X	X
Deutsche Telekom AG Employee Authentication	-	-	-
Deutsche Telekom AG External Workforce Encryption	X	X	X
Deutsche Telekom AG External Workforce Signature	X	X	X
Deutsche Telekom AG External Workforce Authentication	-	-	-
Deutsche Telekom AG Funktionsgruppen Encryption	X	X	X
Deutsche Telekom AG Funktionsgruppen Signature	X	X	X
Deutsche Telekom AG Telekom Computer	-	-	-

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA
Deutsche Telekom AG Domain Controller	-	-	-
Deutsche Telekom AG Print Server	-	-	-
Deutsche Telekom AG Code Signing	-	-	-
Deutsche Telekom AG OCSP Signing	X	X	X

Tabelle 12: Zuordnung der Zertifikate zu den CAs und den jeweiligen AIA URIs für Zertifikate aus der öffentlichen Stammzertifizierungsstelle

Bereitstellung von Zertifikatsstatusdaten über das OCSP-Protokoll

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA
Authority Information Access (AIA)			
AIA [1] ocsp (OCSP Access (1.3.6.1.5.5.7.48.1))	URL=http://ocsp-cpki.telekom.de/ocspr	URL=http://ocsp-cpki.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr
AIA [2] http (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer
AIA [3] ldap (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate
AIA [4] AD (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority
Deutsche Telekom AG Employee Encryption	-	-	-
Deutsche Telekom AG Employee Signature (nur Mobile Devices)	-	-	X

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA
Deutsche Telekom AG Employee Authentication	X	-	X
Deutsche Telekom AG External Workforce Encryption	-	-	-
Deutsche Telekom AG External Workforce Signature	-	-	X
Deutsche Telekom AG External Workforce Authentication	X	-	X
Deutsche Telekom AG Funktionsgruppen Encryption	-	-	-
Deutsche Telekom AG Funktionsgruppen Signature	-	-	-
Deutsche Telekom AG Telekom Computer	-	X	-
Deutsche Telekom AG Domain Controller	-	X	-
Deutsche Telekom AG Print Server	-	X	-
Deutsche Telekom AG Code Signing	-	X	-
Deutsche Telekom AG Mobile Device Authenti-fizierungszertifikat für VPN	-	-	X
Deutsche Telekom AG Mobile Device Signature für Email Signatur auf Mobile Devices	-	-	X
Deutsche Telekom AG OCSP Signing	X	X	X

Tabelle 13: Zuordnung der Zertifikate zu den CAs und den jeweiligen AIA URIs für Zertifikate aus der internen Stammzertifizierungsstelle

Weitere Informationen hierzu sind unter https://corporate-pki.telekom.de/ abrufbar.

Bereitstellung der Zertifikate zum Bezug der öffentlichen Schlüssel zur Datenverschlüsselung über den LDAP-Server der Corporate PKI NG, der Global Address List oder das X.500 Konzernverzeichnis.

Diese Verzeichnisse sind nur im Intranet der DTAG erreichbar.

Quelle	URL
LDAP-Server der Corporate PKI der DTAG	ldap://corporate-pki.telekom.de:389/C=DE
Global Address List der AD Domänen EMEA1 und EMEA2	

Tabelle 14: Schnittstellen zur Bereitstellung der Zertifikate zum Bezug der öffentlichen Schlüssel zur Datenverschlüsselung

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

Ein Distinguished Name (DN) ist innerhalb der Corporate PKI der DTAG, ein eindeutiger Name für Verzeichnisobjekte nach dem X.500-Standard. Mit dem Distinguished Name ist eine eindeutige Unterscheidbarkeit von Personen und Systemen gegeben. Der DN soll unterstützen, dass kein digitales Zertifikat für verschiedene Personen mit dem gleichen Namen ausgestellt wird.

Innerhalb eines Zertifikates ist zu unterscheiden nach

- IssuerDistinguishedName (Issuer DN)
- SubjectDistinguishedName (Subject-DN)

Der Issuer DN repräsentiert den eindeutigen Namen der ausstellenden Zertifizierungsstelle (CA) und ist in dem Kapitel 1.3.1 grafisch dargestellt. Es gelten aber die Namensformen analog zum Subject-DN.

3.1.1 Namensformen

Für alle Zertifikatsanträge wird die Identität des Zertifikatnehmers geprüft, bzw. über die vertrauenswürdige Datenbasis (cIAM) verifiziert (siehe Kapitel 3.2.3.)

Abhängig vom Zertifikatstyp (Kapitel 1.3.3 und 7.1) werden die entsprechenden Informationen in unterschiedliche Pflichtfelder (mandatory fields) oder optionale Felder (xxxx) aufgenommen, die gemäß X.509v3-Standard vorgesehen sind.

Für alle Zertifikatstypen müssen zumindest die folgenden Felder ausgefüllt sein:

- Country Name (C)
- Organization Name (O)
- Das Subjektfeld muss für natürliche Personen und Pseudoyme folgenden Attribute gemäß der Empfehlung ITU-T X.520[6] enthalten:
- - countryName;
- - Wahl zwischen Vor- und Nachname oder Pseudonym; und
- CommonName.

Server-Zertifikate werden nur unter der internen CA ausgestellt, jedoch müssen aufgrund von internen Vorgaben der DTAG zusätzlich folgenden Felder ausgefüllt sein:

- Locality Name (L), oder
- State or Province Name (S)

Details zu den Inhalten des Issuer DN und des Subject DN können dem Kapitel 7 entnommen werden.

In optionalen Feldern (z.B. OU3, FQDN), die keine Informationen beinhalten (leere Felder) oder nicht relevant sind, ist die Verwendung von Füllzeichen (Metazeichen), wie beispielsweise "-", ".", „*“ oder " " (Zwischenraum, Space), verboten.

3.1.1.1 Konventionen für die Bestandteile des „Subject-DN“

In diesem Kapitel werden Konventionen für Subject-DN (Antragsteller) festgelegt, die für alle Endteilnehmer-Zertifikate gelten. Im Folgenden werden die englischen Begriffe verwendet, die heute in diesem Umfeld gebräuchlich sind.

Innerhalb des Subject-DN sind folgende Zeichen erlaubt:
A – Z, a – z, ä, ö, ü 0 – 9, ( ) + - . / : = ? @ und Leerzeichen (Space, Blank)

Auf Grund der unterschiedlichen Kodierungsregeln der jeweiligen Zertifikatsfelder dürfen in einigen Eingabefeldern nicht alle o.g. Zeichen verwendet werden (z.B. keine Umlaute (ä, ö, ü) in E-Mail-Adresse).

3.1.1.1.1 Country Name (C)

Dieses Pflicht-Attribut enthält die weltweite Landeskennung. Festgelegt ist ein aus zwei Buchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist. Dieses Feld spezifiziert das Land, in welchem der Zertifikatsinhaber niedergelassen ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer gleichwertiger Verzeichnisse (T-SIS) oder Dokumente verifiziert.

Beispiele:

C = DE für Deutschland

C = US für Vereinigte Staaten von Amerika

Weitere Details finden Sie hier:

http://www.unece.org/cefact/locode/subdivisions.html

http://www.nationsonline.org/oneworld/country_code_list.htm

Im Rahmen der Prüfung der „erlaubten Internet-Domänen“ (Kapitel 3.2.2) werden die Attribute Country Name (C), Organization Name (O) (Kapitel 3.1.1.1.2) als festes Wertepaar in die Konfiguration der cPKI aufgenommen.

3.1.1.1.2 Organization Name (O)

Dieses Pflicht-Attribut enthält den Organisationsnamen (z.B. Firma, Institution, Behörde) des Zertifikatsinhabers. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer gleichwertiger Verzeichnisse oder Dokumente verifiziert.

Beispiele:

O = Musterfirma GmbH

O = Deutsche Telekom AG

O = DTAG

Im Rahmen der Prüfung der „erlaubten Internet-Domänen“ (Kapitel 3.2.2)) werden die Attribute Organization Name (O), Country Name (C) (Kapitel 3.1.1.1.1) als festes Wertepaar in die Konfiguration der cPKI aufgenommen.

Im Falle, dass der Antragsteller keiner eindeutige Organisation zugeordnet werden kann, ist das Feld mit „Deutsche Telekom AG“, bzw. „DTAG“ zu füllen, da nur Zertifikatsanträge von Mitarbeiter, bzw. Beauftragten der des Deutschen Telekom Konzerns, bzw. einer seiner Töchter oder Beteiligungen verarbeitet werden.

3.1.1.1.3 Organizational Unit Name 1 (OU1)

Dieses Pflicht-Attribut OU1 enthält bei User die Corporate ID (CID) des Mitarbeiters, Diese ID wird verwendet um bei gleichen Vor- und Nachnamen eine Eindeutigkeit zu erreichen. Die CID wird in CIAM beim Anlegen des Mitarbeiterstammdatensatzes erzeugt und begleitet den Mitarbeiter während des gesamten Beschäftigungs- bzw. bei Externen Mitarbeitern während Ihres Beauftragungsverhältnisses.

Bei Gruppen, Funktions-, Rollenzertifikaten ist in OU1 FMB oder GRP eingetragen.

Die Eindeutigkeit bei Gruppen, Funktions-, Rollenzertifikaten ist hier über den SAM Account Name im CN gegeben (siehe Kapitel 3.1.1.1.7).

Beispiel:

OU = C-123456

OU = FMB, OU = GRP

3.1.1.1.4 Organizational Unit Name 2 (OU2)

Dieses Pflicht-Attribut enthält bei Endanwender-, Gruppen-, Funktions-, Rollen- und den Employee-Typ.

Beispiele:

OU = Employee

OU = External Workforce

OU = Internal

OU = ssl-vpn

3.1.1.1.5 Organizational Unit Name 3 (OU3)

Mit diesem Attribut können natürliche Personen- und Gruppen, Funktions-, Rollenzertifikaten sowie Benutzerzertifikate für Mobile Devices unterschieden werden

Beispiele:

OU = Person (natürliche Person oder Pseudonym)

OU = Users (Gruppen, Funktions-, Rollenzertifikaten)

OU = Mobile (Benutzerzertifikate für Mobile Devices)

3.1.1.1.6 Organizational Unit Name (OU4)

Dieses Attribut wird bei Gruppen, Funktions-, Rollenzertifikaten, zusätzlich zum Attribut C (Country), zur Kennzeichnung der weltweiten Landeskennung verwendet. Festgelegt ist ein aus zwei Buchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist.

Beispiele:

OU = DE

Dieser Wert wird auf Basis der aus dem Active Directory der DTAG ausgelesen Attribute gesetzt.

3.1.1.1.7 Given Name

Abhängig vom Zertifikatstyp enthält das Pflicht-Feld „Given Name“ den Vornamen des Endteilnehmers (siehe Kapitel 1.3.3). Dies sind für

- Benutzer-Zertifikate der Vorname, wie dieser in der vertrauenswürdigen Datenbasis „cIAM“ hinterlegt ist.

Beispiele:

G = Max>

- Das Attribut GivenName wird nicht gesetzt, wenn ein Pseudonymattribut vorhanden ist oder es sich um Gruppen-, Funktions-, Rollenzertifikate handelt.

3.1.1.1.8 Surname

Abhängig vom Zertifikatstyp enthält das Pflicht-Feld „Surname“ den Nachnamen des Endteilnehmers (siehe Kapitel 1.3.3).

Dies sind für

- Benutzer-Zertifikate. Hier wird der Nachname, wie dieser in der vertrauenswürdigen Datenbasis „cIAM“ hinterlegt ist eingetragen.

Beispiele:

SN = Mustermann>

Das Attribut Surname wird nicht gesetzt, wenn ein Pseudonymattribut vorhanden ist oder es sich um Gruppen-, Funktions-, Rollenzertifikate handelt.

3.1.1.1.9 Pseudonym

Abhängig vom Zertifikatstyp kann statt der Pflicht-Felder „GivenName und Surname“ des Endteilnehmers das Pseudonym Feld vorhanden sein. (siehe Kapitel 1.3.3).

Dies sind für

- Benutzer-Zertifikate können statt des realen Vor- und Nachnamens, ein Pseudonym enthalten, wie dieser in der vertrauenswürdigen Datenbasis „cIAM“ hinterlegt ist.

Beispiele:

PN = PN- <Pseudonym>

Das Pseudonym Attribut wird nicht gesetzt, wenn ein Vor- und Nachnameattribut vorhanden ist oder es sich um Gruppen-, Funktions-, Rollenzertifikate handelt.

3.1.1.1.10 Common Name (CN)

Abhängig vom Zertifikatstyp enthält das Pflicht-Feld „Common Name“ den Namen des Endteilnehmers (siehe Kapitel 1.3.3). Dies sind für

- Benutzer-Zertifikate der Vor- und Nachname,
- Gruppen-, Funktions-, Rollenzertifikate die Bezeichnung mit Präfix FMB oder GRP sowie als Suffix den SAM Account Name aus dem Active Directory
- Server-Zertifikate der Server-Name (FQDN),
- Router-Zertifikate die IP-Adresse,
- Mail-Gateway-Zertifikate der Server-Name (FQDN) und
- Domain-Controller-Zertifikate der Server-Name (FQDN).

Bei Server-, Router-, Mail-Gateway und Domain-Controller-Zertifikaten wird der Common Name nach Zertifikatserzeugung in die Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name, Kapitel 3.1.1.2 ff) aufgenommen.

Für Server-Zertifikate gilt: Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur ganz links im FQDN akzeptiert. Wildcard-Zeichen in Verbindung mit Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

Beispiele:

CN = Max Mustermann

CN = web1.telekom.de

CN = <IP-Adresse>

CN = FMB-Funktionspostfach technischer Support.S09876543

CN = PN- <Pseudonym> (siehe auch Kapitel 3.1.3)

Zur Kennzeichnung von Zertifikaten für Gruppen-, Funktions-, Rollenzertifikate bzw. Verwendung von Pseudonymen sind dem Common Name folgende Kennungen voranzustellen (siehe auch Kapitel 3.1.3).

- Präfix „FMB-“ oder „GRP-“ kennzeichnet Gruppen-, Funktions-, Rollenzertifikate
- Präfix „PN-“ kennzeichnet das Pseudonym

Abweichend von Benutzerzertifikate und Zertifikate für Pseudonyme wird bei Gruppen-, Funktions-, Rollenzertifikate die Eindeutigkeit nicht über die OU1=CID sondern über den Suffix <.SAM Account Name> hergestellt.

Einschränkungen: Zertifikate für Computer, Server, Router, Mail-Gateway und Domain-Controller werden nur aus einer internen Zertifizierungsstelle (siehe Kapitel 1.3.1.2.2) ausgestellt.

Für Server der DTAG die öffentlich erreichbar sind, steht das Produkt „ServerPass“ zur Verfügung. Nähere Informationen zu ServerPass siehe: https://www.telesec.de/de/serverpass

3.1.1.1.11 E-Mail-Address (E)

Das Pflicht-Attribut „E-Mail-Adresse“ enthält bei

- Benutzer-Zertifikaten die E-Mail-Adresse des Zertifikatsinhabers (S/MIME) oder die E-Mail-Adresse der Personenvereinigungen, Gruppen, Funktionen und Rollen, usw.,
- Geräte (Server, Router/Gateway, Mail-Gateway, Domain-Controller) die E-Mail-Adresse eines Administrators oder eines Funktionspostfachs.

Die E-Mail-Adresse besteht aus einem Lokalteil (local part) und einem Domänenteil (domain part). Als Lokalteil wird der Teil einer E-Mail-Adresse bezeichnet, der sich vor dem @-Zeichen befindet und die Adresse innerhalb der Domain des E-Mail-Providers eindeutig bezeichnet. Der Domänenteil befindet sich nach dem @-Zeichen und es gelten die Syntaxregeln des DNS.

Beispiel:

E = max.mustermann@telekom.de

E = PKI_FMB_TESTBOX2@telekom.de

3.1.1.1.12 Locality Name (L)

Dieses Attribut wird aktuell nur für Serverzertifikate aus der internen CA verwendet. Dieses Pflicht-Feld enthält den Namen der Stadt, in dem die Organisation (z.B. Firma, Institution, Behörde) gemeldet ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer vergleichbarer Verzeichnisse oder Dokumente verifiziert.

Beispiele:

L = Berlin,

L = München,

L =Frankfurt/Main

Im Rahmen der Prüfung der „erlaubten Internet-Domänen“ (Kapitel 3.2.2) werden die Attribute Locality Name (L), Country Name (C) (Kapitel 3.1.1.1.1), Organization Name (O) (Kapitel 3.1.1.1.2) und State or Province Name (S) (Kapitel 3.1.1.1.9) als festes Wertepaar (Tupel) in die Konfiguration der cPKI aufgenommen.

3.1.1.1.13 State or Province Name (S)

Dieses Attribut wird aktuell nur für Serverzertifikate aus der internen CA verwendet, Dieses Pflicht-Feld enthält den Namen des Gliedstaats oder der territorialen Verwaltungseinheit (z.B. Bundesland, Kanton, Departement), in dem die Organisation (z.B. Firma, Institution, Behörde) niedergelassen bzw. gemeldet ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder anderer vergleichbarer Verzeichnisse oder Dokumente verifiziert.

Folgende Schreibweisen sind erlaubt:

- Vollschreibweise des „State or Province Name“ (Subdivision Name).
  Beispiele:
  S = “Berlin”,

S = “Bayern”,
S = “Hessen”

- Nach einer anerkannten Abkürzung des „State or Province Name“ (Subdivision Name).
  Beispiele:
  S= “NW” für Nordrhein-Westfalen,
  S = “BRU“ für Région de Bruxelles-Capitale,
  S = “75“ für Paris

Weitere Details finden Sie hier:
http://www.unece.org/cefact/locode/subdivisions.html
z.B.: https://www.iso.org/obp/ui/#iso:code:3166:DE (durch Änderung der Landeskennung gemäß ISO 3166-1 (im Beispiel „DE“) können andere länderspezifische „State or Province Name (Subdivision)“ selektiert werden).

Im Rahmen der Prüfung der „erlaubten Internet-Domänen“ (Kapitel 3.2.2) werden die Attribute State or Province Name (S), Country Name (C) (Kapitel 3.1.1.1.1), Organization Name (O) (Kapitel 3.1.1.1.2) und Locality Name (L) (Kapitel 3.1.1.1.8) als festes Wertepaar (Tupel) n die Konfiguration der cPKI aufgenommen.

3.1.1.1.14 Street Address (STREET)

Dieses Attribut wird aktuell nur für Serverzertifikate aus der internen CA verwendet. Dieses optionale Feld enthält den Straßennamen, an dem die Organisation (z.B. Firma, Institution, Behörde) gemeldet ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder vergleichbarem Verzeichnisse oder Dokumente verifiziert.

Beispiel:

STREET = Musterstraße 17

STREET = 5. Avenue

3.1.1.1.15 Postal Code (PostalCode)

Dieses Attribut wird aktuell nur für Serverzertifikate aus der internen CA verwendet, Dieses optionale Feld enthält die Postleitzahl der Stadt, in dem die Organisation (z.B. Firma, Institution, Behörde) gemeldet ist. Diese Angaben werden anhand eines öffentlichen Verzeichnisses (z.B. Handelsregisterauszug) oder vergleichbarem Verzeichnisse oder Dokumente verifiziert.

Beispiel:

PostalCode = 57250

PostalCode = AZ23G7

3.1.1.1.16 Subject-DN Serial Number (SN)

Das Attribut SN findet innerhalb der cPKI keine Anwendung

3.1.1.1.17 Unstructured Name

Weitere Informationen zum „unstructured name“ (Unstrukturierter Name) sind in Kapitel 3.1.1.2.3 dargestellt.

3.1.1.2 Konventionen für die Bestandteile „Subject Alternative Name“ (SAN)

Die Einträge im Feld „Alternativer Antragstellername“ (Subject Alternative Name (SAN)) sind abhängig von den jeweiligen Zertifikatstypen (Benutzer, Server, Router/Gateway, Domain-Controller und Mail-Gateway). Die Erweiterung „Subject Alternative Name“ muss mindestens einen Eintrag enthalten. Die Einträge im SAN stammen aus Pflichtfeldern wie

- Common Name (Kapitel 3.1.1.1.6)
- E-Mail-Adresse (Kapitel 3.1.1.1.7)

- User Principal Name (Kapitel 3.1.1.2.2)
- DNS-Name (Kapitel 3.1.1.2.3)
- IP-Adresse (Kapitel 3.1.1.2.4)

als auch optionalen Feldern wie

- E-Mail-Adresse (Kapitel 3.1.1.1.7)
- DNS-Name (Kapitel 3.1.1.2.3)

Einschränkungen von Zertifikatsinhalten sind in Kapitel 3.1.1.1.6 beschrieben.

3.1.1.2.1 RFC822-Name

Der RFC822-Name entspricht der E-Mail-Adresse. Optional kann in einem Benutzer-Zertifikat bis zu drei (3) weiteren E-Mail-Adressen aufgenommen werden. Der bzw. die E-Mail-Adresse(n) werden automatisch in den Subject Alternative Name (SAN) übernommen.

3.1.1.2.2 User Principal Name (Prinzipalname)

Das Feld „User Principal Name“ (UPN) im Benutzer-Zertifikat ist optional, außer als Pflichteintrag im Smartcard-LogOn-Zertifikat (Triple-Key). Der „User Principal Name“ stellt einen benutzerfreundlichen (d.h. leicht zu merkenden) Name dar, der zur Windows-Anmeldung an der Domäne bzw. Active Directory dient. Dieser besteht aus einem Benutzerkontonamen (auch Anmeldenamen genannt) und der Domäne, in der das Benutzerkonto gespeichert ist („Benutzerkontonamen“@„Domänenname“).

Der UPN kann, muss aber nicht der E-Mail-Adresse entsprechen.

Bei Benutzer-und Gruppen, bzw. Funktions-Zertifikaten wird der UPN in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name, Kapitel 7.1.2.3) als „Prinzipalname“ angezeigt.

Beispiele:

Prinzipalname = max.mustermann@telekom.de

Prinzipalname = max.mustermann@local-server.com

RFC822-Name = PKI_FMB_TEST @telekom.de

Der UPN kann jedoch wie folgt lauten:
Prinzipalname = S01234567@emea1.cds.t-internal.com

3.1.1.2.3 DNS-Name

Der vollständige Name einer Domäne (auch absolute Adresse genannt) wird als Fully Qualified Domain Name (FQDN) bezeichnet und kennzeichnet eine exakte Position in der Baumstruktur der DNS-Hierarchie. Das Feld „FQDN“ besteht mindestens aus Top-Level und weiteren Sub-Domains.

Beispiele:

FQDN = www.example.com

FQDN = s-server.pki.example.de

Bei Server-Zertifikaten wird der FQDN als Pflichtfeld im Subject-DN als „Common Name“ eingetragen und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „DNS-Name“ angezeigt.

Optional können in einem Server-Zertifikat bis zu vier (4) weiteren Server-Namen aufgenommen werden. Die Server-Namen werden automatisch als „DNS-Name“ in den Subject Alternative Name (SAN) übernommen.

Bei Router-Zertifikaten wird das optionale Feld FQDN als „unstructured name“ im Subject-DN aufgenommen und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „DNS-Name“ angezeigt.

3.1.1.2.4 IP-Adresse

Bei Router-Zertifikaten wird die IP-Adresse als Bestandteil des „Common Name“ im Subject-DN und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „IP-Adresse“ angezeigt.

3.1.1.2.5 Anderer Name (Other Name)

Bei Domain-Controller-Zertifikaten wird das Pflichtfeldes „Microsoft-GUID“ (MSGuid) als Eintrag „DNS-Objekt-Guid“ unter „Other Name“ in die Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) angezeigt.

3.1.2 Aussagekraft von Namen

Der Name muss den Endteilnehmer bzw. Zertifikatsnehmer mit allgemein verständlicher Wortbedeutung enthalten, als auch eindeutig und nachprüfbar sein.

Im Falle von Zertifikaten für Gruppen-, Funktions-, Rollenzertifikate und Pseudonymen kann T-Systems vom Mandanten DTAG verlangen, die wahre Identität des Zertifikatsinhabers berechtigten Dritten offenzulegen.

3.1.3 Pseudonymität bzw. Anonymität der Zertifikatsinhaber

Benutzer-Zertifikate, die ein Pseudonym enthalten, werden mit dem Präfix „PN-“ im Common Name (CN) kenntlich gemacht (siehe auch Kapitel 3.1.1.1.7).

Benutzer-Zertifikate für Gruppen-, Funktions-, Rollenzertifikate, werden mit dem Präfix „FMB-“ oder „GRP-“ im Common Name (CN) sowie zusätzlich in Organisation Unit (OU) mit dem Eintrag FMB oder GRP gekennzeichnet.

Beispiele:

Pseudonym:

CN=PN-Novalis
CN=PN-George Sand

Gruppen-, Funktions-, Rollenzertifikate:

CN = FMB-Trust Center Test.S09750343
OU = FMB

Alternativ kann statt FMB auch die Bezeichnung GRP verwendet werden.

Beispiel:

CN=GRP-Technischer Support
OU=GRP

Die Wahl von Pseudonymen oder Gruppen-, Funktions-, Rollenbezeichnungen unterliegt verschiedenen Namenseinschränkungen. Ausgeschlossen werden Namen die Berechtigungen suggerieren (wie z.B. Telekom CA), die der Zertifikatsinhaber nicht besitzt, sowie politische Parolen, anstößige Namen oder Verletzung von Markenrechten.

Das Trust Center der DTAG behält sich vor, die Vergabe eines Pseudonyms abzulehnen. Die Ablehnung bedarf keiner Begründung.

Für nähere Details zur Ausstellung von Zertifikate für Pseudonym und Personen- und Funktionsgruppen siehe Kapitel 1.4.1.3 und 1.4.1.4

3.1.4 Regeln zur Interpretation verschiedener Namensformate

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

T-Systems stellt sicher, dass das Benutzer-Zertifikate (von verschiedenen Benutzern) mit gleichem Subject-DN (siehe Kapitel 3.1.1.1 ff) nur einmal innerhalb der cPKI vorkommen. Dies wird durch den Eintrag der Corporate ID (CID) im Subject-DN (siehe Kapitel 3.1.1.1.3) gewährleistet.

Bei Gruppen-, Funktions-, Rollenzertifikate wird die Eindeutigkeit durch den Surffix SAM Account Name im CN gewährleistet (siehe Kapitel 3.1.1.1.7). Das Trennzeichen zwischen Funktionsbezeichnung und Sam Account Name ist ein Punkt Zeichen (Dot).

Für Benutzer können ein, zwei oder drei Zertifikate mit demselben eindeutigen Subject-DN ausgestellt sein, die sich jedoch in der Schlüsselverwendung bzw. erweiterten Schlüsselverwendung und der Zertifikatsseriennummer unterscheiden. Durch die Erneuerung können zeitlich begrenzt auch mehrere nicht gesperrte Zertifikate mit dem gleichen Subject-DN und gleicher Schlüsselverwendung vorhanden sein.

Zertifikate für Geräte mit gleichem Subject-DN (siehe Kapitel 3.1.1 ff) können mehrfach vorkommen.

3.1.6 Erkennung, Authentifizierung und Rolle von Warenzeichen

Für die Namenswahl von Warenzeichen, Markenrechte usw. in Zertifikaten (z.B. Organization Name (O), Organizational Unit Name (OU)) gilt besondere Sorgfaltspflicht. Es liegt in der Verantwortung des Auftraggebers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. oder die Rechte des geistigen Eigentums von Dritten verletzen. Die Zertifizierungsstelle der cPKI ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Auftraggebers.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Methode zum Besitznachweis des privaten Schlüssels

Der Zertifikatsinhaber muss bei einem Neuauftrag gegenüber der Zertifizierungsstelle in geeigneter Weise nachweisen, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist. Der Besitznachweis ist durch die Methode PKCS#10 erbracht. Diese Anforderung gilt nicht, wenn die Schlüsselerzeugung durch die Zertifizierungsstelle selbst stattfindet z.B. bei Schlüsselpaaren für das Verschlüsselungszertifikat (siehe Kapitel 3.2.3.3). In diesem Fall ist die Zuordnung zwischen öffentlichem und geheimem Schlüssel implizit gegeben.

3.2.2 Authentifizierung der Organisations- und Domänenidentität

Grundvoraussetzung für die Nutzung der cPKI ist die Einrichtung eines PKI-Mandanten innerhalb des PKI Dienstes der cPKI.

Der cPKI Dienst wird alleinig durch den Mandanten DTAG genutzt. Alle Benutzer der DTAG gehören einer Organisation der DTAG an oder stehen in einem definierten Vertragsverhältnis zur DTAG.

Die T-Systems stellt bei der Authentifizierung von Organisationen sicher, dass verwendete Namen geprüft werden.

T-Systems führt folgende Prüfungen durch:

- Feststellung der Existenz der Organisation durch entsprechende aktuelle Organisationsdokumente der DTAG (z.B. T-SIS), die von einer zuständigen Konzern-Stelle ausgestellt wurden und die Existenz der Organisation bestätigen.
- Prüfung des/der Domänennamen gegen eine Whitelist von „erlaubten Domänen“ vor Ausstellung von Zertifikaten.
- Technische Beschränkung der erlaubten Domänen (Domain Constraints) in der Zertifizierungsstelle secure email CA (siehe Kapitel 7.1.5).

Organisationsänderungen (z.B. Umfirmierung) sind dem Herausgeber (siehe Kapitel 4.9.1) dieser CP/CPS unverzüglich schriftlich anzuzeigen. T-Systems wird, in diesem Falle keine weiteren Zertifikate auf diese Organisation ausstellen. Zertifikatserneuerungen werden ab der Organisationsänderung (z.B. Umfirmierung) auf die dann gültige Organisation ausgestellt.

T-Systems wird, im Falle der unter Kapitel 4.9.1 genannten Sperrgründe ausgestellte Zertifikate unverzüglich zu sperren.

Zur Erfüllung und Einhaltung der [CAB-BR] wird T-Systems die Authentifizierung der Identität der jeweiligen Organisation spätestens nach 27 Monaten wiederholen. Für Domänen, die für andere Zertifikatstypen Verwendung finden, erfolgt die Überprüfung nach max. 825 Tage (siehe auch Kapitel 3.3). Hierzu erfolgt ein Abgleich mit Telekom - Subsidiaries Information System (T-SIS).

Aufgabe und Ziel von T-SIS ist es, für den internen wie externen Bedarf Grundinformationen zu den Telekom-Konzerngesellschaften zur Verfügung zu stellen. T-SIS stellt die Grundinformationen hierzu tagesaktuell zur Verfügung. Sämtliche Informationen sind für jeden beliebigen Stichtag abrufbar. Innerhalb der Grundinformationen der legalen Einheiten kann die Historie auch weiter zurückverfolgt werden.

Die in T-SIS hinterlegten Informationen werden von der Rechtsabteilung der DTAG freigegeben und tagesaktuell durch die Deutsche Telekom Services Europe (DTSE) gepflegt.

Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

Für alle dem Konzern Deutsche Telekom AG zugehörigen Organisationen oder einer externen Organisation die zu dem Konzern Deutsche Telekom AG in einem definierten Vertragsverhältnis steht, wird im Zertifikat O=DTAG oder O=Deutsche Telekom AG gesetzt.

Die Bezeichnung DTAG ist eine unter Registriernummer 30118939 eingetragene Marke der Deutsche Telekom AG.

3.2.3 Authentifizierung der Identität von Endteilnehmern

Die Authentifizierung der Identität bzw. Identifikation von Endteilnehmern (siehe Kapitel 1.3.3) wird im Konzern der DTAG durch HR bei Einstellung des Mitarbeiters durchgeführt und der Mitarbeiter im SAP HR System der DTAG angelegt.

Bei Externen Mitarbeitern erfolgt dies durch einen Kostenstellenverantwortlichen bzw. durch einen von diesem beauftragten Mitarbeiter. Alle Mitarbeiter die eine Authentifizierung der Identität bzw. Identifikation eines Externen Mitarbeiters durchführen dürfen sind von der DTAG geschult, die Schulung muss mittels eines Teilnehmer-Zertifikats nachgewiesen werden und in SAP HR hinterlegt sein. Ohne diese Hinterlegung ist kein Anlegen von externen Mitarbeitern möglich.

Die Authentifizierung von Pseudonyme erfolgt dezentral durch einen Kostenstellenverantwortlichen bzw. durch einen von diesem beauftragten Mitarbeiter, in dessen Bereich oder Abteilung das Pseudonym Anwendung findet. Es gilt der gleiche Prozess wie für externe Benutzer. Des Weiteren übernimmt der KostV die Schlüsselverantwortung für das auf das Pseudonym ausgestellte Zertifikats- und Schlüsselmaterial (siehe hierzu Kapitel 1.4.1.3).

Die Daten der authentifizierten internen oder externen Mitarbeiter sowie von Pseudonyme werden anschließend von SAP HR an cIAM übermittelt.

So wird von diesen Stellen bei Einstellung von internen Mitarbeitern oder Beauftragung externer Mitarbeiter im SAP HR System ein Stammdatensatz für eine Person angelegt, gespeichert und für das Corporate Identity Management System (CIAM) bereitgestellt. CIAM erzeugt Aufträge zur Generierung oder Aktualisierung von Benutzerdatensätzen an Folgesysteme (wie TAdmin2 und Email Backbone (EMBB)). Die Provisionierung oder Aktualisierung der Datensätze erfolgt durch TAdmin2 an die folgenden Systeme: Active Directory, Exchange, RemoteAccess, cPKI. Darüber hinaus erfolgt durch diese Systeme auch die Verwaltung des Lebenszyklus (Änderung, Sperrung, Löschung) von Stammdatensätzen und den damit verknüpften weiteren Datenattributen. Jedes dieser Systeme gewährleistet dabei Vertraulichkeit, Verfügbarkeit und Integrität von erzeugten, verarbeiteten oder abgelegten Daten, sowie deren sichere Übergabe an andere Systeme.

Die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Daten zu einer natürlichen Person basiert auf definierten Prozessen in der Personalverwaltung des Konzerns Deutsche Telekom. Eine Übersicht der Systeme, welche im Kontext der cPKI und der Identifizierung von natürlichen Personen als Endteilnehmer zu betrachten sind, zeigt die nachfolgende Grafik. CIAM gilt daher im Konzern DTAG als vertrauenswürdige Datenbasis für das Zertifikats-LifeCycle Management der cPKI auf Basis der Anforderungen und Regelungen nach ETSI 319411-1 Policy LCP (siehe auch Kapitel 1.3.2ff).

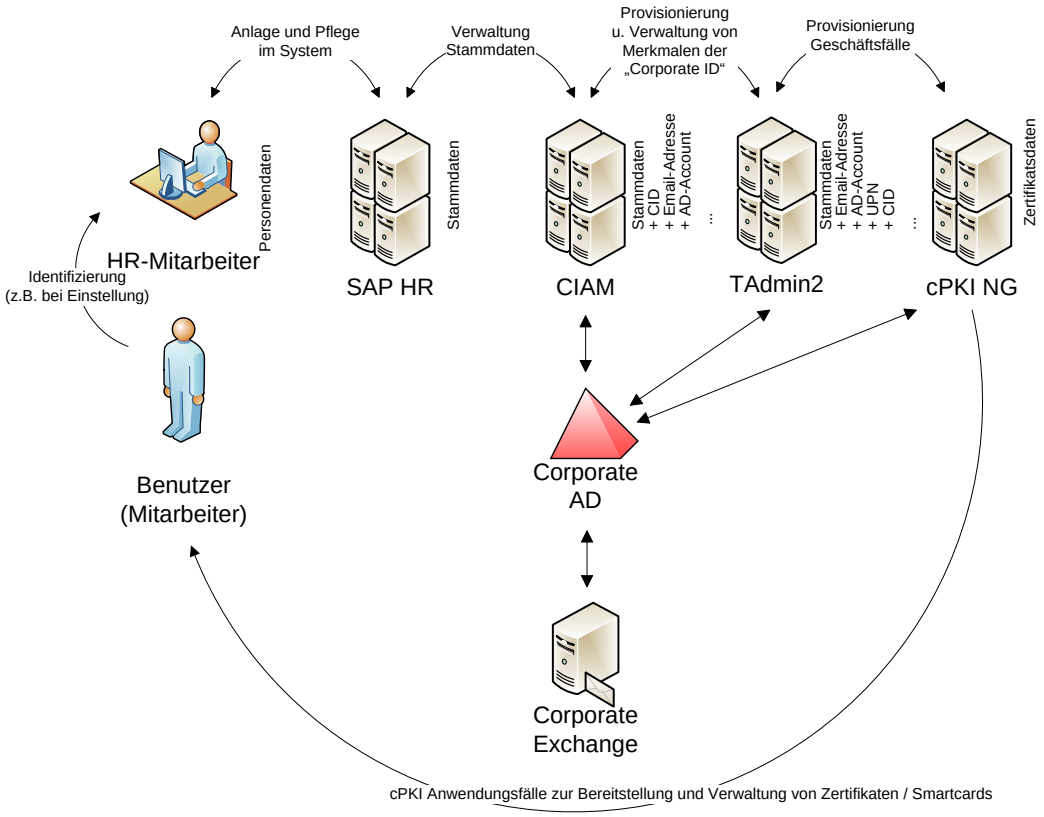

Abbildung 5: Authentifizierung einer natürlichen Person

Für Benutzer-Zertifikate steht eine automatische Erneuerungsfunktion zur Verfügung, die beliebig häufig zur Verfügung gestellt wird. Hierzu wird vom LifeCycle Management der cPKI ein Auftrag zur Zertifikatserneuerung erzeugt. In jedem Fall werden für alle Zertifikatserneuerung die aktuellen Daten aus cIAM verwendet, damit ist sichergestellt das etwaige zertifikatsrelevante Änderungen bei der Zertifikatserneuerung berücksichtigt werden. Für Geräte-Zertifikate steht keine Erneuerungsfunktion zur Verfügung.

Die Identifizierung und Überprüfung von juristische Personen erfolgt durch die RA-Mitarbeiter des Trust Centers.

3.2.3.1 Registrierung von DTAG internen Benutzer

Die Registrierung von internen Benutzern (natürliche Person) erfolgt auf Basis der vertrauenswürdigen Datenbank cIAM

3.2.3.2 Registrierung von externen Benutzern die für die DTAG tätig sind.

Die Registrierung von externen Benutzern (natürliche Person) erfolgt auf Basis der vertrauenswürdigen Datenbank cIAM

3.2.3.3 Registrierung von Personen- und Funktionsgruppen

Die Registrierung von Personen- und Funktionsgruppen erfolgt durch den Besitzer des Personen- und Funktionsgruppen Accounts. Hierzu muss sich der Besitzer des Personen- und Funktionsgruppen Accounts mit seinem Authentifizierungszertifikat an die cPKI anmelden. Die cPKI überprüft anhand des Zertifikats ob der angemeldete Benutzer tatsächlich der Besitzer handelt. Somit ist sichergestellt, dass ein Zertifikat durch den tatsächlichen Besitzer der Personen- und Funktionsgruppen Adresse beantragt werden kann (siehe hierzu Kapitel 1.4.1.4).

3.2.3.4 Registrierung von Pseudonyme

Die Registrierung von Pseudonyme erfolgt auf Basis der vertrauenswürdigen Datenbank cIAM.

Die Schlüsselverantwortung für das auf das Pseudonym ausgestellte Zertifikats und Schlüsselmaterial übernimmt der KostV in dessen Bereich oder Abteilung das Pseudonyme Anwendung findet. (siehe hierzu Kapitel 1.4.1.3).
Registrierung von Geräten

Die Registrierung von Computer (802.1x) erfolgt automatisch mittels Autoenrollment bei Aufnahme des Computers in die Domäne EMEA1 und EMEA2

Die Registrierung von anderen Geräten (Server, Router/Gateway, Mail-Gateway und Domain-Controller) erfolgt zentral oder dezentral durch den jeweiligen Administrator der Geräte. Hierzu muss der Administrator einen Antrag bei der Zertifizierungsstelle stellen (siehe hierzu Kapitel 1.4.1.2.2).

3.2.3.5 Registrierung von juristische Personen

Die Registrierung von juristischen Personen erfolgt durch den manuellen RA-Platz des Trust Centers.

3.2.4 Nicht überprüfte Teilnehmerangaben

Nicht verifizierte Informationen sind Informationen, die ohne Prüfung ins Zertifikat übernommen werden und umfassen:

- sonstige Informationen, die im Zertifikat als nicht verifiziert gekennzeichnet sind (z.B. Schlüsselverwendung, erweitere Schlüsselverwendung).

Zertifikate, die unter der Sub-CA „Deutsche Telekom AG Issuing CA 01“, „Deutsche Telekom AG Issuing CA 02“ und „Deutsche Telekom AG secure email CA“ ausgestellt werden, enthalten von T-Systems verifizierte Informationen. Alle Informationen die in das Zertifikat übernommen werden stammen aus den Backend Systemen der DTAG und sind als validiert anzusehen.

Überprüfung der Berechtigung:
Ein Benutzer ist zum Erhalt von Zertifikaten berechtigt, wenn er einen gültigen Arbeitsvertrag bei der DTAG oder eines ihrer Tochterunternehmen besitzt oder eine definierte Vertragsbeziehung besteht (externe Mitarbeiter sowie Partner) und in den Backend-Systemen der Deutschen Telekom (SAP HR, CIAM, Corporate-AD, TAdmin2) administriert ist.

Zertifikate, die unter der Sub-CA „Deutsche Telekom AG Issuing CA 03“,“ und „Deutsche Telekom AG mobile device CA“ ausgestellt werden, können nicht verifizierte Informationen enthalten.

3.2.5 Überprüfung der Berechtigung

3.2.5.1 Sicherstellung der Authentizität des Zertifikatsantrags

Zur Feststellung der Authentizität der Daten aus SAP HR, cIAM und TAdmin2 werden bei den genannten Systemen

- Regelmäßige Durchführung von Audits mit dem Internal Control System (ICS) durch Externe Wirtschaftsprüfer,
- Durchführung und Freigabe in einem PRIVACY & SECURITY ASSESSMENT (PSA) Verfahren
- Durchführung von Penetrationstests durch Sicherheitsexperten der Telekom Security
- Zertifizierung nach ISO 27001

3.2.5.2 Prüfung von Domänen und IP-Adressen

Die Zertifikatsausstellung ist auf Domänen der Deutschen Telekom beschränkt, hierzu ist eine Beschränkung auf zugelassene Maildomänen in der „Deutsche Telekom AG secure email CA“ mittels Domain Constraints (Namenseinschränkungen) und zusätzlich im Zertifikatsmanagement der cPKI implementiert.

Die DTAG teilt der T-Systems die Domänen mit, auf die Zertifikate ausgestellt werden sollen, damit T-Systems diese nach Prüfung als „erlaubte Internet-Domänen“ in die PKI-Konfiguration des Mandanten aufnehmen und pflegen kann.

Die Prüfung erfolgt auf Basis vom Auftraggeber Bereitgestellten Dokumenten.

Des Weiteren werden die angebenden Domänen gegen das Office 365 Azure AD (Cloud) validiert. Für die im Office 365 Azure AD der DTAG hinterlegten Domänen wurde durch Microsoft eine Prüfung vorgenommen, dass die DTAG sich auch im Beitz dieser Domänen befindet.

Alle relevanten Domänen wurden durch Microsoft geprüft.

Nach Prüfung durch T-Systems werden die „zugelassenen Domänen“ in die „Deutsche Telekom AG secure email CA“ und in die PKI-Konfiguration der cPKI aufgenommen bzw. entfernt.

Namensänderung(en) dieser Domäne(n) und/oder Besitzrechte dieser Domäne(n) sind unverzüglich schriftlich T-Systems anzuzeigen.

Für interne Zertifizierungsstellen erfolgt die Einschränkung der zugelassenen Domains nur im Zertifikats Management der cPKI.

Zur Erfüllung und Einhaltung der [CAB-BR] wird T-Systems die Verwendungsrechte der Domäne(n) spätestens nach 825 Tagen überprüfen. T-Systems ist berechtigt dazu eine vollständige Liste, aller auf die DTAG und ihren Töchtern und Beteiligungen registrierten Domänen, beim Kunden anfordern.

3.2.6 Kriterien für Interoperabilität

Verwendet eine Sub-CA in einem von ihr signierten Zertifikat eine Policy-OID, welche die Erfüllung und Einhaltung der [CAB-BR] repräsentiert (siehe Kapitel 7.1.6.2), muss das jeweilige CP oder CPS der Sub-CA eine explizite Zusicherung enthalten, dass alle von der Sub-CA ausgestellten Zertifikate, welche diese Policy OID enthalten, in Übereinstimmung mit und Einhaltung von den [CAB-BR] ausgestellt und verwaltet werden.

Unter dem PKI-Service „cPKI“ werden keine weiteren Sub-CA Zertifikate ausgestellt. Dies wird durch die Basiseinschränkungen der Sub-CAs (Einschränkung der Pfadlänge=0) gewährleistet.

3.3 Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung

Um durchgehend eine authentische und sichere Kommunikation anbieten zu können, muss sich der Endteilnehmer vor Ablauf eines gültigen Zertifikats ein neues Zertifikat beschaffen. Ob für die Folgebeauftragung ein neues Schlüsselpaar benötigt wird, ist abhängig von der eingesetzten Applikation und dem verwendeten Schlüsselspeicher (Smartcard/MyCard, Soft-PSE).

Schlüsselerneuerung für MyCards

Bei einer Folgebeantragung kann die aktuelle Smartcard mit den darauf befindlichen Schlüsselpaar verwendet werden, sofern technische Vorgaben (z.B. unsichere Krypto-Algorithmen) oder funktionale Beschränkungen dies nicht verbieten oder verhindern. Andernfalls ist ein Folge-Zertifikat auf einer neuen Smartcard auszustellen. Es gelten die Regelungen wie in den Kapiteln 3.2.3 ff und 4.2.1 beschrieben. Sofern die Smartcard eine interne Schlüsselgenerierung unterstützt, können bei einer Folgebeauftragung neue Schlüsselpaare verwendet werden.

Schlüsselerneuerung für Soft-PSE

Bei Folgebeauftragungen als Soft-PSE werden im Allgemeinen neue Schlüsselpaare erzeugt, für bestimmte Geräte (z.B. Web-Server) kann aber auch der vorhandene Schlüssel erneut verwendet werden. Ob eine Schlüsselerneuerung stattfindet, liegt im Ermessen des Zertifikatsnehmers. Die Regelungen in Kapitel 6.1 müssen beachtet werden.

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Vor der Zertifikatsaufstellung wird die Existenz des Users in den relevanten Systemen der DTAG und die Richtigkeit der Daten geprüft.

Es werden für alle Verwendungszwecke neue Zertifikate ausgestellt. Bei Verschlüsselungszertifikaten wird in jedem Fall neues kryptographisches Schlüsselmaterial erzeugt.

3.3.2 Identitätsprüfung und Authentifizierung bei Schlüsselerneuerungen nach Zertifikatssperrung

Eine Zertifikatserneuerung eines gesperrten Zertifikats ist nicht möglich.
Es steht nur die Option Replace zur Verfügung.

Vor der Zertifikatsaufstellung wird die Existenz des Users in den relevanten Systemen der DTAG und die Richtigkeit der Daten geprüft.

Bei Benutzerzertifikaten werden für alle Verwendungszwecke neue Zertifikate ausgestellt. Hierbei Verschlüsselungszertifikaten werden in jedem Fall neue kryptographische Schlüsselmaterial erzeugt.

3.3.3 Identitätsprüfung nach Ablauf des Gültigkeitszeitraums

Nach Ablauf des Gültigkeitszeitraumes ist die Zertifikatserneuerung nicht möglich. Es steht nur die Option der Prüfung durch den manuellen Registrationsplatz zur Verfügung. Dieser kann nach der beschriebenen Identitätsprüfung die Zertifikatserneuerung in der cPKI neu aktivieren.

3.4 Identifizierung und Authentifizierung von Sperraufträgen

Die Authentifizierung von Sperranträgen erfolgt mittels einer im System durch den Zertifikatsinhaber hinterlegte Frage bzw. Antwort. Nach Verifizierung der geheimen Antwort durch den Service Desk erfolgt eine Sperrung bzw, ein Replace. Ein Replace hat ebenfalls eine umgehende Sperrung aller Zertifikate des Users zur Folge.
Im Falle der Sperrung wird das Zertifikat in eine Sperrliste aufgenommen.

Die Sperrung von Zertifikaten telefonisch beim Service Desk beauftragt werden. Für eine telefonische Erteilung von Sperraufträgen sind die innerhalb des Konzerns DTAG kommunizierten Eingangskanäle des jeweils zuständigen Service Desks zu verwenden.

Falls der Verdacht auf missbräuchlichen Einsatz eines Zertifikats besteht, kann dies unter Angabe der ausstellenden Zertifizierungsstelle, des Common Name und der Emailadresse oder der Seriennummer im Zertifikat, sowie der Beschreibung des Missbrauchs dem Service Desk mitgeteilt werden. Dieser Fall wird von T-Systems geprüft und bewertet. Im Falle einer begründeten missbräuchlichen Zertifikatsverwendung ist T-Systems berechtigt und verpflichtet, das Zertifikat umgehend zu sperren (Kapitel 4.9.1 und 4.9.2).

Missbrauchsfälle können gemeldet werden über:
- Telefon (siehe Kapitel 1.5.2)
- E-Mail (siehe Kapitel 1.5.2)
- Internet: https://corporate-pki.telekom.de/ „Kontakt | Zertifikatsmissbrauch melden“
- Durch Mitarbeiter des DTAG Konzerns bei den kommunizierten Eingangskanälen der jeweils zuständigen Service Desks sowie an 24h Stunden dem Konzernlagezentrum der DTAG.

4 BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsantrag

4.1.1 Wer kann Zertifikate beantragen?

Für die Beantragung von Zertifikaten gelten folgende Voraussetzungen:

- Antragsteller ist Mitarbeiter der DTAG, einer Tochter, Beteiligung oder steht in einem Vertragsverhältnis mit DTAG und ist in diesem Auftrag für die DTAG tätig.
- Der Antragsteller ist in cIAM angelegt und verfügt über ein aktives Beschäftigungsverhältnis.
- Der Antragsteller verfügt über ein aktives Domänen Konto und eine E-Mail-Adresse aus einer erlaubten Mail-Domäne.
- Der Zertifikatsantrag durch den Antragsteller wird mittels des Klicks auf den Link in Mail an den Benutzer und der anschließenden Anmeldung an dem WebPortal durchgeführt.
- Der Antragsteller akzeptiert die Nutzungsbedingungen der Corporate PKI der DTAG durch Anklicken des Links zur Personalisierung und Aktivierung der myCard in der Enrollmentmail.
- Erfolgreiche Anmeldung des Antragsstellers an das cPKI Webportal.
- Besitz einer MyCard (Smartcard der DTAG).
- Für Computer, dieser muss ein Computerkonto in einer erlauben AD-Domäne besitzen.
- optional: Zugangsdaten für die SCEP- und REST Schnittstelle

Folgende Personen können einen Zertifikatsantrag stellen:

- Autorisierte Personen, die als Subjekt des Zertifikats erscheinen (interne oder externe Mitarbeiter der DTAG mit aktivem Vertrag).
- Autorisierte Personen von Personen- und Funktionsgruppen, juristischen Personen und Geräten.
- Autorisierte Personen die Berichtigt sind Pseudonym Accounts zu beauftragen.
- Organisationen, vertreten durch Handlungsbevollmächtigte der DTAG

Als autorisierte Personen werden natürliche Personen verstanden, die über geeignete Anmeldedaten verfügen und die o.g. Voraussetzungen erfüllen.

4.1.2 Registrierungsprozess und Verantwortlichkeiten

4.1.2.1 Automatische Registrierungsstelle

Die Registrierung der Teilnehmer erfolgt über vorgelagerte Identifizierungs-, Authentifizierungs- und Provisionierungprozesse in der IT Infrastruktur der Deutschen Telekom.

Konkret bedeutet dies, dass die Verarbeitung der Registrierungsdaten sowie deren Verifikation bereits durch die Vorsysteme geschehen ist. Auf Basis der vertrauenswürdigen Daten aus cIAM erfolgt danach die Ausstellung der Zertifikate. Sieh hierzu Kapitel 1.3.2 und 3.2.3

Die Verantwortung für die Korrektheit der Daten wird durch die jeweils erfassende bzw. für den Betrieb der jeweiligen Systeme verantwortlichen Stelle übernommen.

Die Einrichtung und weitere Pflege der „erlaubten Internet-Domänen“ basieren auf einer erfolgreichen Authentifizierung der Identität von Organisationen, die in Kapitel 3.2.2 beschrieben ist.

Der Zertifikatsantrag durch den Antragsteller wird mittels des Klicks auf den Link in Enrollmentmail und der anschließenden Anmeldung an dem WebPortal durchgeführt. Mit dem anklicken des Links zur Aktivierung und Personalisierung der MyCard wird der Zertifikatsantrag an die die Corporate PKI der DTAG auf Basis der Daten aus der vertrauenswürdigen Datenbank (cIAM) durchgeführt und der der Endteilnehmer erkennt die Nutzungsbedingungen der Corporate PKI Deutsche Telekom (cPKI) an und erklärt, dass er diese gelesen und verstanden hat. Der entsprechende Hinweis und der Link zu den Nutzungsbedingungen ist in der Enrollmentmail enthalten.

4.1.2.2 Manuelle Registrierungsstellen

4.1.2.2.1 Registrierungsstellenmitarbeiter Trust Center

Die manuelle Registrierungsstelle zur Wiederherstellung von im Trust Center sicher abgelegtem Schlüsselmaterial und Zertifikate für juristische Personen erfolgt durch geschultes uns sicherheitsüberprüftes Personal des Trust Centers.

Zur Wiederherstellung sind mehrere unterschiedliche Personen mit unterschiedlichen Rollen und Berechtigungen erforderlich.

- Recovery Manager
- Recovery Approver
- Recovery Operator

Ablauf im Detail:

1. Der Antragsteller füllt ein standardisiertes Formular für die Wiederherstellung eines bestimmten Verschlüsselungsschlüssels für einen bestimmten Benutzer aus und leitet den Vorgang zur Autorisierung durch Unternehmenssicherheit, Datenschutz und Betriebsrat weiter. Nach Autorisierung und digitaler Signierung aller Beteiligten wird der Antrag per Mail verschlüsselt und signiert an die ausführende Stelle (Trust Center) gesendet.
2. Der Recovery Manager überprüft folgende Punkte: Auftragseingang, Autorisierung des Vorgangs, digitale Signaturen, Antragstellerdaten, Benutzerdaten und Versanddaten.
3. Der Recovery Manager meldet sich mit seiner MyCard an die cPKI an und startet den Workflow "Wiederherstellung Zertifikat". Dieser Auftrag muss durch den Recovery Approver genehmigt werden. Der Recovery Approver wird per E-Mail zur Genehmigung des Auftrages aufgefordert.
4. Der Recovery Approver meldet sich mit seiner MyCard an der cPKI an und startet den Workflow „Genehmigen Wiederherstellung Zertifikat“. Nach der Genehmigung wird der Recovery Operator per E-Mail informiert, dass es einen genehmigten Wiederherstellungsauftrag gibt.
5. Der Recovery Operator meldet sich mit seiner MyCard an der cPKI an und startet den Workflow "Ausführen Wiederherstellung Zertifikat". MyID selektiert die wiederherzustellenden Zertifikate aus der cPKI. Die Verschlüsselungsschlüssel werden auf einer eigens dafür vorgesehenen Smartcard (Wiederherstellungskarte) gespeichert. Vom Server wird eine Benutzer-PIN für die Smartcard vergeben und ebenfalls auf der Karte gespeichert.
6. Die cPKI erzeugt automatisch ein Schreiben, welches vom Recovery Operator zusammen mit der Smartcard an den Antragsteller versendet wird. Weiterhin schickt der Recovery Operator eine verschlüsselte E-Mail mit der Information zur Benutzer-PIN an den Antragsteller.
7. Der Wiederherstellungsprozess wird in der cPKI geloggt. Das Antragsformular wird archiviert.
   Alle Auftragsvorgänge werden mit der persönlichen digitalen Signatur des entsprechenden Rollenträgers signiert.

4.1.2.2.2 Endteilnehmer inkl. Registrierungsstellenmitarbeiter

Alle Endteilnehmer erkennen das Dokument „Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS))“ in seiner aktuellen Version an und verpflichten sich die dort beschriebenen Regelungen einzuhalten.

Ferner verpflichtet sich der Endteilnehmer und Registrierungsstellenmitarbeiter,

- dass die im Zertifikatsantrag stehenden Angaben wahr und korrekt sind,
- zu einer Übermittlung des öffentlichen Schlüssels und der Zertifikatsdaten an T-Systems zur Zertifikatserzeugung,
- einen Nachweis über den Besitz des privaten Schlüssels zu führen, der in Verbindung mit dem zertifizierten öffentlichen Schlüssel steht,
- zur Einhaltung der "Datenschutzanforderung - Zugriff auf die persönliche Kommunikations- und Ablageumgebung" der DTAG

Die o.g. Pflichten gelten ebenfalls für den TSP, der in seinem Namen Zertifikate ausstellt.

Die T-Systems behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Endteilnehmer abzuschließen.

4.1.2.3 Manuelle Registrierungsstelle für Zertifikate aus der internen CA

Die manuelle interne Registrierungsstelle kann nur für Zertifikate aus den internen CAs Deutsche Telekom Issuing CA 01“ und die „Deutsche Telekom AG secure email CA“ ausstellen.

Die Registrierung erfolgt durch

- einen anderen geeigneten Prozess (z.B. Beantragung über die Benutzer-Webseite, Mail-, SCEP- Schnittstelle), aus dem die Identität des Endteilnehmers eindeutig hervorgeht. Die Subjektdaten des Zertifikats dürfen auf einem integreren Datenbestand des Mandanten basieren. Die Generierung des Datenbestands ist auf Anfrage der Zertifizierungsstelle darzulegen.
- für Geräte durch den Administrator als Schlüsselverantwortlichen. Berechtigte Administratoren werden durch das das Trust Center authentisiert. Der Administrator muss über das in dem Zertifikat genannte Gerät Kontrolle ausüben bzw. es betreiben.
- Mitarbeiter des Trust Centers

Die Registrierungsstelle verpflichtet sich folgende Tätigkeiten durchzuführen:

- Es sind die Namensformen gemäß Kapitel 3.1.1 ff einzuhalten.
- Für Geräte-Zertifikate ist, abhängig vom Zertifikatstyp, der Domänenteil (domain-part) der E-Mail-Adresse oder DNS-Name (Top-Level-Domain und weiteren Sub-Domains des FQDN), auf die in der PKI-Konfiguration eingetragenen „erlaubten Internet-Domänen“ zu prüfen.
- Im Falle, dass der Auftraggeber über weitere Domänen verfügt, auf die Zertifikate ausgestellt werden sollen, ist T-Systems über die zusätzlichen Domänen zu informieren, nach erfolgreicher Domänenprüfung werden diese in die PKI-Konfiguration aufgenommen (siehe auch Kapitel 3.2.2).
- Im Falle gleiche Namensgebung muss die Registrierungsstelle eine Eindeutigkeit herstellen.
- Es dürfen nur Daten der DTAG (Country Name (C), Organization Name (O), Organizational Unit Name, Domänenteil der Mail-Address und ggf. User Principal Name (UPN), Top-Level- und weitere Sub-Domains des Fully Qualified Domain Name (FQDN), siehe auch Kapitel 3.1.1 ff) verwendet werden.

4.1.2.4 Manuelle Registrierungsstelle für juristische Personen

Der Betrieb der manuellen Registrierungsstelle zur Ausstellung von Zertifikaten für juristische Personen erfolgt durch geschultes uns sicherheitsüberprüftes Personal des Trust Centers.

Die Registrierung und Ausstellung von Zertifikaten erfolgt auf Basis eines standardisierten Zertifikatantragsformulars.

4.2 Bearbeitung von Zertifikatsanträgen

Die folgende Prozessbeschreibung gilt auch für den TSP selbst, wenn dieser in seinem Namen Zertifikate ausstellt.

4.2.1 Durchführung von Identifikation und Authentifizierung

4.2.1.1 Automatische Registrierungsstelle

Die Identifikation und Authentifizierung der Endteilnehmer erfolgt im Rahmen der etablierten HR-Prozesse durch Stellen des Personalmanagements (DTSE) im Konzern DTAG (siehe Kapitel 3.2.3). Die SAP-HR Daten werden nach Anlage des Stammdatendatensatzes an cIAM übertragen.

Der SubjectDN von Zertifikaten basiert auf dem Datenbestand des Corporate Identity and Access Managements (cIAM), welche auf den SAP-HR Daten beruhen und durch das System CIAM zusätzlich um Informationen (z.B. Email-Adresse, CorporateID) ergänzt werden und an TAdmin2 zur Anlage des User-Accounts, des Mailpostfaches und zur Beauftragung (Zertifikatsantrag) der cPKI übergeben.

Die cPKI nimmt die Zertifikatsanträge in elektronischer Form von TAdmin2 als antragstellender Instanz entgegen und prüft diese auf Integrität. Irreführende Antragsdaten werden gegenüber dem antragstellenden System abgelehnt. Anschließend erfolgt eine elektronische Überprüfung der E-Mail-Adresse mittels Versand einer Email, welche eine URL und ein Einmalpasswort für die Erzeugung bzw. den Abruf von Zertifikaten durch einen Benutzer enthält. Auf diese Weise wird sichergestellt, dass der Endteilnehmer Besitzer der E-Mail-Adresse ist. Darüber hinaus wird der Domänenteil der E-Mail-Adresse (optional auch der UPN) auf die in der PKI-Konfiguration eingetragenen „zugelassenen Mail-Domänen“ sowie den im CA Zertifikat hinterlegten Namenseinschränkungen geprüft.

Bei Zertifikatsanträgen für Geräte oder Personen- und Funktionsgruppen ist zusätzlich die natürliche Person (z.B. Administrator) zu authentisieren, die über das in dem Zertifikat genannte Gerät oder der Personen- und Funktionsgruppe die Kontrolle ausübt bzw. es betreibt.

Für Geräte-Zertifikate ist, abhängig vom Zertifikatstyp, der Domänenteil der E-Mail-Adresse oder DNS-Name (Top-Level-Domain und weiteren Sub-Domains des FQDN), auf die in der PKI-Konfiguration eingetragenen „erlaubten Mail-Domänen“ zu prüfen.

Bei Funktionszertifikaten wird die reale Identität des verantwortlichen Antragstellers oder Vertreters mittels zertifikatsbasierender Anmeldung am Portal der cPKI und Prüfung des Eigentümers von Funktionspostfächern im Active Directory geprüft.

Die Ausstellung Endteilnehmerzertifikate basieren auf einer erfolgreichen Authentifizierung an dem Webportal der cPKI. Hierzu ist mindestens die Anmeldung mit dem Domänen Account des Endteilnehmers sowie die Eingabe eines Auftragsbezogenen One Time Passwortes (OTP) erforderlich. Bei weiteren Zertifikatstypen, wie z.B. Zertifikate für FMB ist eine Authentifizierung des Schlüsselverantwortlichen nur mittels Zertifikat der persönlichen Smartcard möglich.

4.2.1.2 Manuelle Registrierungsstelle

Die Manuelle Registrierungsstelle stellt für die in Kapitel 1.3.2.2 beschrieben Sonderfälle Zertifikate oder Schlüsselmaterial bereit:

Hierzu erfolgt die Authentifizierung der Endteilnehmer durch die Registratoren des TSP (siehe Kapitel 1.3.2.2)

Handelt es sich um einen Zertifikatsantrag für eine juristische Person muss durch den Antragsteller in geeigneter Weiße den Nachweis erbringen, dass dieser berechtigt ist für eine juristische Person ein Zertifikat zu beantragen.

Die Registrierungsstelle verpflichtet sich folgende Tätigkeiten durchzuführen:

- Die Registrierung erfolgt durch
  - persönliches Erscheinen des Endteilnehmers, seines Vertreters oder eines Schlüsselverantwortlichen, der sich durch Vorlage geeigneter Identifikationsdokumente ausweisen kann und für die ordnungsgemäße Erstellung des Zertifikatsantrages als auch für die Installation des Zertifikats verantwortlich ist, oder
  - einen anderen geeigneten Prozess (z.B. Beantragung über die Benutzer-Webseite, Mail-, SCEP- oder Schnittstelle), aus dem die Identität des Endteilnehmers eindeutig hervorgeht. Die Subjektdaten des Zertifikats dürfen auf einem integren Datenbestand der DTAG basieren. (siehe Kapitel 1.3.2.1)

- Bei Zertifikatsanträgen für Geräte oder Personen- und Funktionsgruppen ist zusätzlich die natürliche Person (z.B. Administrator) als Schlüsselverantwortlichen zu authentisieren, die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt.
- Der Registrierungsstellenmitarbeiter nimmt den Zertifikatsantrag in elektronischer Form entgegen, prüft diesen auf Integrität und Authentizität und die im Antrag enthaltenen Angaben gegenüber vom Antragsteller vorgelegten Digitalen Signatur oder eindeutigen Identifikationsdokumenten (z.B. Unternehmensausweis, Personalausweis [2] und der vertrauenswürdigen Datenbank der DTAG (cIAM)) auf Authentizität (Echtheit, Glaubwürdigkeit), Integrität (Unversehrtheit), Korrektheit, Wahrheit und Vollständigkeit. Zur Authentifizierung der Antragsdaten dürfen zuverlässige interne oder öffentliche Datenquellen verwendet werden.
- Im Falle, dass der Auftraggeber über weitere Domänen verfügt, auf die Zertifikate ausgestellt werden sollen, ist T-Systems über die zusätzliche Domäne zu informieren. Nach erfolgreicher Domänenprüfung werden diese in die PKI-Konfiguration der cPKI aufgenommen (siehe auch Kapitel 3.2.2).
- Irreführende Antragsdaten sind gegenüber dem Antragsteller abzulehnen.
- Im Falle, dass die Antragsdaten nicht mit den Daten des Mandanten (Country Name (C), Organization Name (O), Organizational Unit Name, Domänenteil der E-Mail-Adresse und ggf. User Principal Name (UPN), Top-Level- und weitere Sub-Domains des Fully Qualified Domain Name (FQDN), siehe auch Kapitel 3.1.1 ff) übereinstimmen, ist eine Vollmacht oder ein Berechtigungsdokument des Antragstellers erforderlich.
- Die vom Antragsteller vorgelegten eindeutigen Identifikationsdokumente und Anträge sind als Kopie revisionssicher mindestens 7 Jahre zu archivieren. Dieses Archiv ist vor unbefugtem Zugriff zu schützen. Hierzu werden die Dokumente elektronisch im Management System der cPKI revisionssicher abgespeichert.
- Im Falle von Audits oder anderen Prüfungen (z.B. Stichprobenprüfungen) sind die Registrierungsdokumente durch den TSP dem Auditor offen zu legen.
- Die Registrierungsstellenmitarbeiter sind verpflichtet, verdächtige Schlüsselkompromittierungen, Zertifikatsmissbrauch oder andere zertifikatsbetreffende Betrugsfälle oder -versuche unverzüglich über die Meldewege des TSP zu melden.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Durch die Vergabe einer Referenznummer (Correlation ID) bei der Zertifikatsbeauftragung wird die eindeutige Zuordnung von einem ausgestellten Zertifikat zu den entsprechenden Aufträgen hergestellt.

4.2.2.1 Automatische Registrierungsstelle

Zertifikatsanträge werden bei Dateninkonsistenzen und fehlenden Berechtigungen automatisch abgelehnt. Bei korrekten Aufträgen erfolgt eine automatisierte Annahme der Anträge und der weitere Bearbeitungsprozess wird angestoßen.

4.2.2.2 Manuelle Registrierungsstellen

Nur nach erfolgreicher Registrierung des Zertifikatsnehmers wird ein Zertifikatsantrag weiterbearbeitet (siehe Kapitel 3.2.3, 4.1.2.4 und 4.2.1.2). Abhängig vom Zertifikatstyp (Kapitel 3.2.3) stellt der Registrator über seine Webseite den Zertifikatsantrag in elektronischer Form ein oder genehmigt den bereits in elektronischer Form vorliegenden Antrag.

Ein Zertifikatsauftrag muss abgelehnt werden, wenn

- der Zertifikatsantrag und die Identifikation nicht vollständig, wahr oder korrekt sind,
- der Zertifikatsantrag und die Identifikation aus einer nicht integren Quelle stammen,

[2] Die Zugangsnummer auf der Vorderseite sollte aus Sicherheitsgründen geschwärzt werden, da sie bei Online-Funktionen verwendet werden kann.

- der Zertifikatsantrag und die Identifikation zu keinem eindeutigen positiven Registrierungsergebnis führen,
- der öffentliche Schlüssel die Mindestschlüssellänge von 2048 Bit unterschreitet,
- der Public Exponent nicht den Vorgaben der [CAB-BR] entspricht,
- die Untersuchung auf Debian-Schwäche positiv ausfällt,

Im Falle einer Ablehnung des Auftrags wird der Beauftragte (Techn. Ansprechpartner) des Zertifikatsnehmers unter Angabe von Gründen per E-Mail benachrichtigt.

4.2.3 Bearbeitungsdauer von Zertifikatsaufträgen

4.2.3.1 Automatische Registrierungsstelle

Die Bearbeitung des Zertifikatauftrags beginnt innerhalb eines angemessenen Zeitraums nach Erhalt der Beauftragung. Der Teilnehmer hat nach Annahme des Zertifikatsantrags 21 Tage Zeit sich auf dem cPKI Portal anzumelden und das Enrollment der Zertifikate durchzuführen. Sollte ein Teilnehmer bis zum Ende dieser Frist seine Zertifikate nicht abgerufen haben, wird der entsprechende Auftrag storniert und der Benutzer Account gesperrt.

4.2.3.2 Manuelle Registrierungsstellen

4.2.3.2.1 Registrierungsstellenmitarbeiter Trust Center

Die Bearbeitung von Zertifikatanträgen auf Basis des Dokuments „cPKI Beantragung Key Backup“ oder „Zertifikatsantrag für juristische Personen“ erfolgt innerhalb eines angemessenen Zeitraums nach Erhalt der vollständigen Unterlagen.

Die Bearbeitung von Zertifikatsaufträgen die durch den die automatische Registrierungsstelle abgelehnt wurden beträgt Auftragseingang + 1 AT.

4.2.3.3 Manuelle Registrierungsstelle für Zertifikate aus der internen CA

Die Bearbeitungsdauer von Zertifikatsanträgen für Geräte-Zertifikate (außer Autoenrollment für 802.1x Computer Zertifikate) obliegt der Zuständigkeit und Verantwortung des jeweiligen registrierten Geräte Administrators die Kontrolle über das Gerät ausübt bzw. es betreibt.

4.3 Zertifikatsausstellung

Die folgende Prozessbeschreibung gilt auch für den TSP selbst, wenn dieser in seinem Namen Zertifikate ausstellt.

4.3.1 Maßnahmen der Zertifizierungsstelle während der Ausstellung von Zertifikaten

4.3.1.1 Automatische Registrierungsstelle

Nach der Genehmigung des Zertifikatsantrags prüft das Zertifikatsmanagement den Zertifikatsantrag auf die in der PKI-Konfiguration sowie das CA-System auf den in den im CA Zertifikat eingetragenen Namensbeschränkungen eingetragenen „zugelassenen Email-Domänen“. Bei positivem Prüfungsverlauf erhält der Endteilnehmer eine Mail mit einem One-Time Password (OTP) sowie der URL zum cPKI Portal. An dem cPKI Portal muss sich er User bei Erstausstellung der Zertifikate mittels seines AD-Accounts und der in der Mail genannten OTP authentifizieren.

Nach erfolgreicher Anmeldung und OTP Verifizierung, erfolgt die Prüfung, dass eine neue mit PIN Sigel versehene Smartcard (myCard) sich im Kartenleser befindet. In der Folge vergibt der Endteilnehmer zwei Fragen und Antworten und setzt eine 6-stellige Smartcard-PIN. Die Zertifikate werden unmittelbar danach ausgestellt und auf die Smartcard (myCard) geschrieben. (Schlüsselgenerierung Siehe Kapitel 6.1)

Bei einer Zertifikatserneuerung kann die Anmeldung alternativ auch mit dem Teilnehmerzertifikat für Authentifizierung oder den beiden vergebenen Fragen und Antworten erfolgen. Die auf den Endteilnehmer registrierte Smartcard

(myCard) kann bei einer Zertifikatserneuerung weiterverwendet werden. Hierzu wird die Seriennummer der gesteckten Smartcard gegen die im Zertifikatsmanagement System hinterlegte Smartcard geprüft. Eine andere sich nicht im Null-Pin Status (PIN-Sigel) befindliche Smartcard kann nicht benutzt werden und wird vom PKI System abgelehnt.

4.3.1.2 Manuelle Registrierungsstellen

4.3.1.2.1 Registrierungsstelle TSP

Nach der Genehmigung des KeyBackup-Antrags wird das KeyBackup unmittelbar auf die Smartcard geschrieben.

Nach Genehmigung des Zertifikatsantrags für juristische Personen wird das Zertifikat unmittelbar als Soft-PSE erstellt.

Es werden über diese Registrierungsstelle, außer den genannten Zertifikaten für juristische Personen, keine weiteren neuen Zertifikate aus der öffentlichen Zertifizierungsstelle ausgestellt.

4.3.1.3 Manuelle Registrierungsstelle für Zertifikate aus der internen CA

Nach der Genehmigung des Zertifikatsantrags prüft das CA-System den Zertifikatsantrag auf die in der PKI-Konfiguration eingetragenen „erlaubten Internet-Domänen“. Im Falle einer Gutprüfung wird das Zertifikat unmittelbar ausgestellt.

Im Falle, dass im Zertifikatsantrag Informationen enthalten sind, die nicht mit den „erlaubten Internet-Domänen“ übereinstimmen, wird die Zertifikatsaustellung nicht durchgeführt und der zuständige registrierte Geräte Administrator wird per Hinweismeldung informiert.

4.3.2 Benachrichtigung von Endteilnehmern

4.3.2.1 Automatische Registrierungsstelle

Der Zertifikatsinhaber erhält nach der Annahme des Zertifikatsantrags eine Benachrichtigung in Form einer E-Mail. In dieser E-Mail ist eine URL und ein OTP (One-Time Password = Einmalpasswort) enthalten.

Der Zertifikatsinhaber ruft die URL auf, gibt das OTP an entsprechender Stelle ein und steckt die Karte in den am Benutzer-PC angeschlossenen Kartenleser.

Die MyCard wird daraufhin unter Eingabe der PIN durch den jeweiligen Zertifikatsinhaber personalisiert, d.h. sein Zertifikat wird aus der entsprechenden CA bereitgestellt und auf die Karte geschrieben.

Im Falle, dass das Verschlüsselungszertifikate einem Gruppen- oder Funktions- Mitglied oder einem Vertreter (Deputy) zugewiesen werden soll, erfolgt ebenfalls eine Benachrichtigung an den Vertreter.

Der Vertreter erhält eine Benachrichtigung in Form einer E-Mail. In dieser E-Mail ist eine URL enthalten.

Das Gruppen- oder Funktions- Mitglied bzw. der Vertreter ruft die URL auf und steckt die Karte in den am Benutzer-PC angeschlossenen Kartenleser.

Die Personell Security Environment (PSE) des zur Vertretenden wird nach Eingabe der PIN auf die MyCard geschrieben.

Nach erfolgreichem Aufbringen des Zertifikats wird dem Endteilnehmer auf dem cPKI eine Erfolgsmeldung mit den Details zu dem ausgerollten Zertifikat(en) angezeigt.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme durch den Zertifikatsinhaber

Das folgende Verhalten stellt die Annahme eines Zertifikats dar:

- Das Herunterladen und Installieren eines Zertifikats auf Basis einer Mitteilung oder deren Anhang durch den Endteilnehmer.
- Die Annahme des Schlüsselmaterials inkl. PIN bzw. Passwort (Smartcard oder Soft-PSE), dass für den Endteilnehmer ausgestellt wurde.

- Falls der Endteilnehmer nicht innerhalb einer vom der DTAG definierten Frist nach Erhalt des Zertifikats Einwände gegen das Zertifikat oder seinen Inhalt gegenüber dem Trust Center erhebt.
- Kein Widerspruch gegenüber dem Trust Center innerhalb einer von der DTAG definierten Frist nach Erhalt des Zertifikats bzw. des Inhalts des Zertifikats erfolgt.
- Verwendung des Zertifikats.

Durch Annahme des Zertifikats erkennt der Zertifikatsinhaber die Regelungen des vorliegenden Dokumentes an und versichert, dass sämtliche Angaben und Erklärungen in Bezug auf die im Zertifikat enthaltenden Informationen der Wahrheit entsprechen.

4.4.2 Veröffentlichung der Zertifikate durch die Zertifizierungsstelle

Die Veröffentlichung von Zertifikaten erfolgt über das Corporate Active Directory der DTAG sowie einen Verzeichnisdienst der cPKI. Dabei gelten folgende Regelungen:

- Die Veröffentlichung der Zertifikate ist abhängig vom Zertifikatstyp und den Regelungen gemäß Tabelle 9: Vorgaben für die Veröffentlichung von Zertifikaten
- Es können zusätzlich bestimmte Zertifikattypen (siehe Tabelle 9) nach Absprache veröffentlicht werden.
- Es können nach Absprachezusätzliche Daten wie z.B. die MyCard Seriennummer oder CID. im Verzeichnisdienst der cPKI veröffentlicht werden.
- Der Verzeichnisdienst der cPKI sowie das Corporate Active Directory der DTAG sind nur aus dem Intranet der DTAG abfragbar.

4.4.3 Benachrichtigung über die Zertifikatsausstellung durch die Zertifizierungsstelle an weitere Instanzen

Es können Benachrichtigung per E-Mail oder Notifikationen über Systemschnittstellen (approval notification) an weitere Instanzen und Personen (z.B. Registratoren, Administratoren, Besitzer von Funktionsgruppen, Funktionsgruppen, IT-Systeme) erfolgen.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Das Zertifikat und der zugehörige private Schlüssel darf nur entsprechend den Nutzungsbedingungen (Terms of Use) dieser CP/CPS, dem DTAG Internen Bezugsvertrag (Subscriber Agreement) verwendet werden.

Die Verwendung des privaten Schlüssels, mit dem dazu gehörigen zertifizierten öffentlichen Schlüssel, ist erst gestattet, nachdem der Endteilnehmer das Zertifikat angenommen hat (Kapitel 4.4.1).

Die Zertifikatsnutzung wird durch die Vorgaben und Verwendungszweck der DTAG internen Regelungen bestimmt. Die technische Zertifikatsverwendung ist im Zertifikat als Attribut „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ definiert.

Alle Endteilnehmer und Registratoren sind verpflichtet,

- ihre privaten Schlüssel vor unbefugtem Gebrauch schützen,
- den privaten Schlüssel nach Ablauf des Gültigkeitszeitraums oder der Sperrung des Zertifikats nicht mehr benutzen, außer zur Einsichtnahme verschlüsselter Daten (z.B. Entschlüsselung von E-Mails).

Für Zertifikate von Personen- und Funktionsgruppen, juristischen Personen und Geräte gelten darüber hinaus folgenden Anforderungen:

- Der Schlüsselverantwortliche (Kapitel 1.3.3 und 1.4.1.4) ist für das Kopieren bzw. Weitergeben der Schlüssel an den/die Endteilnehmer verantwortlich.
- Der Schlüsselverantwortliche muss den/alle Endteilnehmer zur Einhaltung dieser CP/CPS im Umgang mit dem privaten Schlüssel verpflichten.
- Temporäre Zertifikatssperrungen können auf Personen aus dem Kreise der Endteilnehmer übertragen werden.
- Endgültige Zertifikatssperrungen können nur durch den Schlüsselverantwortlichen veranlasst werden, hierzu muss der Schlüsselverantwortliche die Details zu Sperranlässen und die zur Sperrung benötigte Frage und Antwort mitteilen.
- Nach dem Ausscheiden einer Person aus dem Kreise der Endteilnehmer (z.B. Kündigung des Vertragsverhältnisses) muss ein Missbrauch des privaten Schlüssels durch den Benutzer oder Schlüsselverantwortlichen verhindert werden, indem das Zertifikat diesem Benutzer entzogen wird. Sollte ein Entziehen des Zertifikats nicht möglich sein, ist das Zertifikat umgehend zu sperren.
- Eine Übertragung der Verantwortung an einen neuen oder zusätzlichen Schlüsselverantwortlichen für Pseudonyme erfolgt im HR-System der DTAG und ist dort zu dokumentieren. Der neue Schlüsselverantwortliche ist gemäß dieser CP/CPS zu identifizieren und zu registrieren, seine Autorisierung als Schlüsselverantwortlicher muss nachgewiesen werden.
- Eine Übertragung der Verantwortung an einen neuen oder zusätzlichen Schlüsselverantwortlichen für Funktionsgruppen (Funktionspostfächer) erfolgt im cPKI System und wird dort dokumentiert. Der neue Schlüsselverantwortliche wird gemäß dieser CP/CPS identifiziert, seine Autorisierung als Schlüsselverantwortlicher (Besitzer des Postfachs) wird gegen das Active Directory der DTAG geprüft.

Eine Sperrung des Zertifikats ist umgehend vorzunehmen, wenn die Angaben im Zertifikat nicht mehr korrekt sind oder der private Schlüssel kompromittiert wurde (Siehe hierzu Kapitel 4.9).

4.5.2 Nutzung des Zertifikats durch vertrauende Dritte

Jeder vertrauende Dritte, der ein Zertifikat einsetzt, das von der cPKI ausgestellt wurde, sollte

- vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen,
- vor der Nutzung des Zertifikats dessen Gültigkeit überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie), den Gültigkeitszeitraum und die Sperrinformationen (CRL, OCSP) des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit der vorliegenden Zertifizierungsrichtlinie einsetzen. T-Systems ist nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich,
- den technischen Verwendungszweck prüfen, der durch das im Zertifikat angezeigte Attribut „Schlüsselverwendung“ und ggf. „erweiterte Schlüsselverwendung“ festgelegt ist.

Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Abhängig vom Zertifikatstyp wird der Zertifikatsnehmer, Antragsteller, Vertreter oder weitere Instanzen über die Erneuerung des Zertifikats per E-Mail benachrichtigt (renewal notification), dort sind die relevanten Zertifikats-Informationen enthalten.

Der Versand dieser Benachrichtigung erfolgt 30 Kalendertage vor Ablauf des Zertifikats und wird mehrfach wiederholt, bis das Zertifikat erneuert wurde oder abgelaufen ist.

Bei einer Zertifikatserneuerung wird dem Zertifikatsnehmer ein neues Zertifikat mit neuer Seriennummer, neuem Gültigkeitszeitraum und gleichen Subject-DN (soweit dich keine Änderungen seit dem letzten Zertifikatsantrag ergeben haben, siehe Kapitel 3.1.1.1) ein neues Zertifikat ausgestellt.

Eine Zertifikatserneuerungsfunktion ist nur für Benutzer-Zertifikate und Computerzertifikate (Autoenrollment für Computer in der DTAG Domäne) implementiert. Bei Zertifikatserneuerungen für Computerzertifikate erhält der Benutzer des Gerätes keine Benachrichtigung (Autoenrollment)

Für andere Zertifikatstypen bedarf es einer Zertifikatsneubeantragung, auch wenn dazu auf die ursprünglichen technischen Antragsdaten zurückgegriffen werden kann.

Eine Zertifikatserneuerung für Smartcards ist auch nach Ablauf der Gültigkeit des vorhandenen Zertifikats möglich. Eine Erneuerung eines abgelaufenem Soft-PSE Zertifikats ist nicht möglich. Eine Erneuerung eines gesperrten Zertifikats ist grundsätzlich nicht möglich.

Eine Zertifikatserneuerung kann, abhängig vom Schlüsselmaterial Smartcard oder Soft-PSE, mit oder ohne neuer Schlüsselgenerierung erfolgen. Bei der Verwendung des gleichen Schlüsselpaares wird jedoch vorausgesetzt, dass die eindeutige Zuordnung von Zertifikatsnehmer und Schlüssel erhalten bleibt, keine Kompromittierung des Schlüssels vorliegt und die kryptographischen Parameter (z.B. Schlüssellänge) für die Gültigkeitsdauer des neuen Zertifikats noch ausreichend sind.

4.6.1 Gründe für eine Zertifikatserneuerung

Sofern keine Gründe (z.B. Vertragskündigung, Kündigung des Arbeitsverhältnisses, Beurlaubung) dagegensprechen, muss sich der Benutzer vor Ablauf seines gültigen Zertifikats ein neues Zertifikat beschaffen, um die Kontinuität der Zertifikatsnutzung gewährleisten zu können.

Zur Zertifikatserneuerung muss das Zertifikat inkl. privatem Schlüssel vorliegen.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Eine Zertifikatserneuerung darf nur der Benutzer oder Schlüsselverantwortliche beauftragen.

Der Benutzer oder Schlüsselverantwortliche muss in einem aktiven Arbeitsverhältnis, bzw. in einer laufenden Beauftragung bei Externen Mitarbeitern stehen. Des Weiteren ist ohne einem aktiven Domänen-Account im Active Directory der DTAG keine Zertifikatserneuerung möglich.

4.6.3 Bearbeitung von Zertifikatserneuerungen

Das Erneuerungsverfahren muss gewährleisten, dass nur berechtigte Zertifikatsnehmer (Benutzer, Schlüsselbeauftragte) diesen Prozess durchführen können.

Als Authentifizierungsmerkmal wird bei der Erneuerung von Endteilnehmer-Zertifikaten der Besitz des vollständigen Schlüsselmaterials (Zertifikat und privater Schlüssel) vorausgesetzt.

Die Erneuerung von Zertifikaten erfolgt durch den Zertifikatsinhaber selbst. Der Endteilnehmer kann für eine Übergangsfrist von max. 24h Stunden über zwei gültige Zertifikate verfügen. Darüber hinaus gelten die Regelungen aus Kapitel 3.3.

4.6.4 Benachrichtigung des Antragstellers nach Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.6.6 Veröffentlichungen der erneuerten Zertifikate durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3

4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

Die Schlüsselerneuerung von Zertifikaten stellt eine weitere Antragsform zur Ausstellung eines neuen Zertifikats unter Verwendung eines neuen Schlüsselpaares dar. Zertifikatsinhalt und Identifikationsdaten bleiben unverändert.

Ob eine Schlüsselerneuerung unterstützt wird, hängt von den technischen Vorgaben der Anwendung ab (z.B. Web-Server) ab.

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Zur Erhöhung des Sicherheitsaspekts kann eine Schlüsselerneuerung sinnvoll sein, um bspw. bei Verwendung in Software gespeicherten Schlüsseln (PKCS#12, .pfx Dateien, Software PSE) mögliche Risiken für den Zugriff auf private Schlüssel zu minimieren. Kapitel 4.6.1

4.7.2 Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beauftragen?

Es gelten die Regelungen von Kapitel 4.6.2.

4.7.3 Bearbeitung von Schlüsselerneuerungsanträgen

Es gelten die Regelungen von Kapitel 3.3 und 4.6.3.

4.7.4 Benachrichtigung des Zertifikatsinhabers über die Ausstellung mit neuem Schlüsselmaterial

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.7.5 Annahme einer Zertifikatserneuerung mit neuem Schlüsselmaterial

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.7.6 Veröffentlichung eines Zertifikats mit neuem Schlüsselmaterial durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.7.7 Veröffentlichung eines Zertifikats mit neuem Schlüsselmaterial durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Gründe für Zertifikatsänderung

Das Ausstellen eines neuen Zertifikats ist zwingend erforderlich, wenn sich die Zertifikatsinhalte (mit Ausnahme des öffentlichen Schlüssels) gegenüber dem bisherigen ausgestellten Zertifikat ändern bzw. geändert haben. (z.B. C, O, OU, CN, E-Mail, siehe auch Kapitel 3.1.1).

Bei Zertifikatsdaten für Zertifikate unter der öffentlichen CA sind die Inhalte dieser Zertifikate, insbesondere Daten des Zertifikatsinhabers, in den Bezugssystemen SAP HR, CIAM, Corporate AD und TAdmin2 vorgehalten und es wird durch die Automatischen Workflows sichergestellt, dass bei einer Änderung von Zertifikatsrelevanten Inhalten die cPKI einen Änderungsantrag erhält, was in jedem Falle zu einer Neuausstellung von Zertifikaten führt, siehe auch Kapitel 3.2 und 4.1.2.

4.8.2 Wer darf eine Zertifikatsänderung beauftragen?

Es gelten die Regelungen gemäß Kapitel 4.6.2.

4.8.3 Ablauf der Zertifikatsmodifizierung

Wenn sich Zertifikatsinhalte ändern (siehe Kapitel 3.1 ff), ist eine erneute Authentifizierung gegenüber der cPKI erforderlich (siehe Kapitel 3.2). Das vorhergehende Zertifikat ist umgehend zu sperren.

4.8.4 Benachrichtigung des Zertifikatsinhabers über die Ausstellung eines Zertifikats

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.8.5 Annahme einer Zertifikatserneuerung mit geänderten Zertifikatsdaten

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.8.6 Veröffentlichung eines Zertifikats mit geänderten Daten durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.8.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserstellung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Umstände für eine Sperrung

4.9.1.1 Gründe für eine Sperrung eines Endteilnehmer-Zertifikats

Die folgenden Gründe erfordern die Zertifikatssperrung durch den Zertifikatsnehmer und deren Veröffentlichung in der Zertifikatssperrliste (CRL):

- Der private Schlüssel wurde kompromittiert, verloren, gestohlen oder offengelegt (dies gilt nicht im Zusammenhang mit einer Schlüsselsicherung) oder es besteht ein dringender Verdacht, dass dies geschehen ist (siehe auch Akronyme und Begriffsdefinition Kapitel A2 Kompromittierung),

- die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr aktuell, ungültig oder falsch oder entsprechen nicht den Bestimmungen der Namensgebung (siehe auch Kapitel 3.1 ff und 4.8.1),
- der zertifizierte Schlüssel (öffentliche Schlüssel) oder die damit verwendeten kryptografischen Algorithmen und Parameter entsprechen nicht mehr den aktuellen Anforderungen,
- es liegt ein Missbrauch, Missbrauchsverdacht durch zu der Nutzung des Schlüssels berechtigten Personen vor,
- es liegt eine unbefugte Nutzung oder der Verdacht einer unbefugten Nutzung des Schlüssels von nicht berechtigten Personen vor,
- Verwendung und Handhabung des Zertifikats im Widerspruch zu vertraglichen Regelungen oder dieser CP/CPS,
- Sperrung des zu erneuernden Zertifikats nach dem Zertifikatserneuerungsprozess,
- bei Vertragsbeendigung bzw. -kündigung zwischen der DTAG und Endteilnehmer, sofern nichts anderes vereinbart ist,
- gesetzliche Vorschriften oder richterliche Urteile begründen eine Zertifikatssperrung,
- das Zertifikat wird nicht mehr benötigt bzw. der Zertifikatnehmer verlangt ausdrücklich die Sperrung des Zertifikats.
- Der Zertifikatsinhaber verlässt das Unternehmen und benötigt daher kein Zertifikat mehr (Temporäre Sperrung erfolgt zum Austrittsdatum, Enggültige Sperrung erfolgt 30 Tage nach Austrittsdatum),

Das T-Systems Trust Centers oder der Service Desk der DTAG sperrt Endteilnehmerzertifikate innerhalb von 24 Stunden und veröffentlicht diese in der Zertifikatssperrliste (CRL) und OCSP-Datenbank, wenn mindestens einer der Gründe vorliegt:

- Der Zertifikatnehmer, Schlüsselbeauftragte oder eine sonstige verantwortliche Person ruft am Sperrservice an und gibt den Auftrag zur Sperrung. Hierzu ist die Authentifizierung mittels einer Frage und Geheimen Antwort erforderlich.
- Der Auftraggeber oder eine verantwortliche Kontaktperson informiert darüber, dass der zugrundeliegende Zertifikatsrequest nicht autorisiert war und die Autorisierung auch nachträglich nicht gegeben wird.
- Der Zertifizierungsstelle liegen Beweise vor, dass der private Schlüssel des Zertifikatsnehmers kompromittiert wurde oder nicht mehr den Anforderungen in Kapitel 6.1.5 und Kapitel 6.1.6 entspricht.
- Der Zertifizierungsstelle liegen Beweise vor, dass das Zertifikat missbräuchlich eingesetzt wurde.
- Bekanntwerden des Abhandenkommens des privaten Schlüssels (z.B. Verlust, Diebstahl, Weitergabe an eine nicht autorisierte Person oder beauftragte Drittpartei (Delegated Third Party)).

Die Zertifizierungsstelle sperrt ein Zertifikat innerhalb von 5 Tagen, wenn mindestens einer der folgenden Gründe vorliegt:

- Die Zertifizierungsstelle erlangt Kenntnis von einer oder mehreren schwerwiegenden Vertragsverletzungen des Zertifikatsnehmers.
- Die Zertifizierungsstelle erlangt Kenntnis darüber, dass das Nutzungsrecht für einen FQDN oder eine IP-Adresse erloschen ist. (Z.B. ein Gericht untersagt die Nutzung, eine Vollmacht läuft aus usw.)
- Die Zertifizierungsstelle erlangt Kenntnis, dass ein Wildcard-Zertifikat für die Authentisierung eines missverständlichen untergeordneten FQDN, der betrügerisch verwendet wird.
- Die Zertifizierungsstelle erlangt Kenntnis von einer relevanten Änderung in den Zertifikatseinträgen.
- Die Zertifizierungsstelle erhält Kenntnis davon, dass das Zertifikat nicht regelkonform herausgegeben wurde, wie es in den Anforderungen des CA-Browserforums oder der anzuwendenden CP oder CPS beschrieben ist.
- Die Zertifizierungsstelle stellt fest, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist.
- Die Zertifizierungsstelle stellt den Betrieb ein und hat keine Regelungen getroffen, dass im Falle einer Betriebseinstellung der Sperrsupport durch eine andere CA weitergeführt wird.

- Der Nachweis der CA-Browserforum-Konformität der CA hat seine Gültigkeit verloren. Ein Sperrgebot gilt nicht, wenn die Zertifizierungsstelle Vorsorge getroffen hat, dass die CRL und der OCSP-Dienst weiter gepflegt und bereitgestellt werden.
- Die CA erlangt Kenntnis von einer möglichen Kompromittierung des privaten Schlüssels einer Sub-CA, der zur Zertifikatsausstellung genutzt wird.
- Die CP und/oder CPS der herausgebenden Zertifizierungsstelle sieht eine Sperrung vor.
- Die Inhalte oder das Format des Zertifikats stellt aus technischer Sicht ein inakzeptables Risiko für Anwendungssoftware-Hersteller oder vertrauende Dritte dar z.B., wenn das CA-Browserforum ein solches Risiko aufzeigt und deshalb das Zertifikat gesperrt und ersetzt werden sollte.
- Gesetzliche Vorschriften oder richterliche Urteile oder eine Weisung einer Aufsichtsführenden Behörde liegt vor.

4.9.1.2 Gründe für die Sperrung eines Sub-CA-Zertifikats

Das T-Systems Trust Center sperrt ein Sub-CA-Zertifikat innerhalb von 7 Tagen, wenn mindestens einer der folgenden Gründe vorliegt:

- Der Zertifikatsnehmer oder ein Bevollmächtigter erteilt schriftlich die Sperrung des Zertifikats.
- Die zertifikatsausstellende Instanz oder ein Bevollmächtigter fordert schriftlich die Sperrung des Zertifikats.
- Der Zertifikatsnehmer teilt der Zertifizierungsstelle (CA) mit, dass der Zertifikatsauftrag nicht autorisiert war oder die Vollmachten oder Nutzungsrechte zwischenzeitlich erloschen sind.
- Der zertifizierte öffentliche oder/und der damit verbundene private Schlüssel oder die damit verwendeten kryptografischen Algorithmen und Parameter entsprechen nicht mehr den aktuellen Anforderungen.
- Es liegt ein Missbrauch oder Verdacht auf Missbrauch des Zertifikats durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen vor.
- Die Verwendung und Handhabung des Zertifikats steht im Widerspruch dieser CP/CPS.
- Gesetzliche Vorschriften oder richterliche Urteile erfordern die Sperrung.
- Der private Schlüssel wurde kompromittiert, verloren, gestohlen, offengelegt oder es besteht ein dringender Verdacht, dass dies geschehen ist.

4.9.2 Wer kann eine Sperrung beauftragen?

Die folgenden Personen und Institutionen sind in der Regel berechtigt, die Sperrung eines Zertifikates zu initiieren:

- cIAM mittels des IT-Prozesses „Employee leave"
- Autorisierte Personen, die als Subjekt des Zertifikats erscheinen.
- Autorisierte Personen von Personen- und Funktionsgruppen, juristischen Personen und Geräten (z.B. Mitarbeiter Personalmanagement).
- Autorisierte Personen die als Schlüsselverantwortliche oder Sperrberechtigte auftreten
- Autorisierte Personen des T-Systems Trust Centers.
- Jede natürliche Person, die einen Verdacht auf missbräuchlichen Einsatz eines Zertifikats anzeigen möchte.

Die folgenden Personen sind in der Regel berechtigt, die Sperrung eines Sub-CA-Zertifikates zu initiieren:

- Autorisierte Person(en) des cPKI Services (z.B. Change Advisory Board der T-Systems)

4.9.3 Ablauf einer Sperrung

Zur Sperrung autorisierte Personen können die Sperrung eines Zertifikates telefonisch 7 Tage die Woche beauftragen. Die Authentisierung und Autorisierung einer Person geschieht dabei in geeigneter Art und Weise (z.B. Anruf beim Help-Desk und Identifizierung des Anrufenden mittels Frage/Antwort).

Sind die Voraussetzungen zur Sperrung erfüllt, wird die Sperrung vorgenommen, und das gesperrte Zertifikat in die Certificate Revocation List (kurz CRL) aufgenommen.

Der Zertifikatsinhaber wird über die Durchführung der Sperrung in geeigneter Weise (via E-Mail) informiert.

Des Weiteren erfolgen Sperrungen über automatische Workflows über das WCF Interface der cPKI z.B. bei Beendigung des Beschäftigungsverhältnisses eines Mitarbeiters oder Beendigung der Beauftragung eines Externen Mitarbeiters. Hierzu wird durch HR oder einem Bevollmächtigten ein zum Austrittsdatum in HR und cIAM hinterlegt. Dieses Datum wird mittels eines Suspend Auftrags über die WCF Schnittelle an das cPKI LifeCycle Management weitergegeben und die Zertifikate zu diesem Austrittsdatum temporär gesperrt. 4 Wochen nach dem Austrittstermin erfolgt über cIAM/TAdmin2 die Initiierung der endgültigen Sperrung der Endteilnehmer-Zertifikate über einen Revoke Auftrag.

4.9.3.1 Sperrvarianten

Je nach Rolle und Berechtigung stehen den Teilnehmern dieser PKI unterschiedliche Sperrvarianten an 7 Tagen der Woche zur Verfügung. Zertifikatssperrungen sind möglich über

- die Sperrservice-Webseite des T-Systems Service Desk
- der WCF-Schnittstelle (Aufträge aus cIAM über TA2)
- den Sperrservice des TSP (Nur für Geräte)
- REST-Schnittstelle (für Geräte (Mobile Devices) und Benutzer Authentifizierungs- sowie dem Signaturzertifikat auf Mobile Device aus der internen Zertifizierungsstelle)
- das Zertifikats LifeCycle Management der cPKI für die Sperr-Operatoren des Sperrservice des TSP)

Tabelle 15 stellt die Sperrvarianten in Abhängigkeit zu den Zertifikatstypen dar.

Zertifikatstyp:	Benutzer-Webseite:	Sperrservice-Webseite des DATG Service Desks:	WCF-Interface	Für Geräte Sperrservice Sperrservice des TSP	REST-Schnittstelle.	cPKI Life Cycle Management für Sperr-Operatoren des TSP
Benutzer	✗	✓	✓	✗	✓	✓
Geräte (z.B. Server, Router/Gateway)	✗	✗	✗	✓	✓	✗

Tabelle 15: Sperrvarianten

Unabhängig von o.g. Sperrvarianten behält sich das T-Systems Trust Center vor, Zertifikate bei Vorliegen von mindestens einem, der in Kapitel 4.9.1.1 aufgeführten Sperrgründe, zu sperren.

4.9.3.2 Sperrung von Endteilnehmer-Zertifikaten

Eine Zertifikatssperrung kann an 7 Tage der Woche durch eine in Kapitel 4.9.2 aufgeführte Rolle oder Instanz initiiert werden. Dabei reicht das Vorliegen von mindestens einem in Kapitel 4.9.1 aufgeführten Sperrgrund.

In jedem Fall sind Inhalte des Subject-DN des Zertifikatsinhabers (z.B. Mailadresse oder CID) erforderlich, um das zu sperrende Zertifikat selektieren zu können. Bei Endteilnehmer Zertifikaten für E-Mail erfolgt die Authentifizierung zur Sperrung am Service Desk über die nur dem Zertifikatsinhaber bekannte Frage und Antwort.

Die Sperrung ist endgültig. Mit dem täglichen Zyklus des CA-Systems (Kapitel 4.9.7) wird das Zertifikat in der Zertifikatssperrliste (CRL) veröffentlicht. Nach der Zertifikatssperrung stehen die Sperrinformationen per OCSP unmittelbar zur Verfügung.

Die Zertifizierungsstelle sperrt, Zertifikate bei Vorliegen von mindestens einem der in Kapitel 4.9.1 aufgeführten Sperrgründe zu sperren.

T-Systems bietet Endteilnehmern, vertrauenden Dritten (z.B. Software-Hersteller) und anderen Teilnehmern die Möglichkeit an, verdächtige Schlüsselkompromittierungen, Zertifikatsmissbrauch oder andere zertifikatsbetreffende Betrugsfälle oder -versuche zu melden, siehe auch Kapitel 3.4.

Innerhalb von 24 Stunden nach Eingang eines Missbrauchsverdachts beginnt T-Systems mit den Nachforschungen, um entscheiden zu können, ob weitere Maßnahmen (z.B. Sperrung) eingeleitet werden.

Innerhalb dieser 24 Stunden wird ein erster Bericht des Sachverhalts und der Analyseergebnisse erstellt und dem Zertifikatsinhaber sowie der Person, die das Problem gemeldet hat, als Rückmeldung gegeben. Nach Ansicht der Fakten und Umgebungsparameter wird die Zertifizierungsstelle mit dem Zertifikatsnehmer/Beauftragten oder der meldenden Person die Analyseergebnisse besprechen und entscheiden, inwiefern eine Zertifikatssperrung notwendig wird. I

n diesem Zusammenhang wird das Datum der Sperrung festgelegt. Der Zeitraum zwischen Erhalt des Zertifikatsproblemreports bzw. Sperrwunsches bis zur veröffentlichten Sperrung darf die in Kapitel 4.9.1 geforderten Fristen für eine Sperrung nicht überschreiten.

Das weitere Vorgehen wird anhand folgender Kriterien bestimmt:

- Um welches konkrete Problem handelt es sich?
- Liegen bereits weitere Missbrauchsfälle für dieses Zertifikat oder diesen Kunden vor?
- Wer hat den Missbrauchsverdacht eingereicht? (zum Beispiel die Meldung von offizieller Behördenstelle im Zusammenhang mit einer strafrechtlichen Verfolgung oder illegalen Aktivitäten)
- Liegt ein Verstoß gegen gesetzliche Vorschriften vor?

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 Zertifikatsinhaber und vertrauende Dritte)
- Die Anzahl der Meldungen zu diesem Zertifikatsproblem oder von diesem Zertifikatsinhaber
- Die Entität welche die Meldung eingestellt hat (z.B. eine Meldung durch eine Strafverfolgungsbehörde wird mit erhöhter Priorität eingestuft) und
- Die bezugnehmende Gesetzgebung

T-Systems verfügt bei einer hoch priorisierten Zertifikats-Problemmeldung jederzeit über die Möglichkeit intern zu reagieren und zu entscheiden, ob eine Weiterleitung an eine Strafverfolgungsbehörde erforderlich ist oder ein Zertifikat, das Gegenstand einer solchen Meldung ist, zu sperren.

4.9.3.3 Sperrungen von Benutzer-Zertifikaten

Die Sperrung von Benutzer-Zertifikaten erfolgt über folgende Rolleninhaber und Webseiten bzw. Schnittstelle (Kapitel 4.9.3):

- Durch den Benutzer über den Service Desk der DTAG.
- Durch cIAM über TAdmin2 und der Schnittstelle zur cPKI.
- Durch Sperr-Operatoren des TSP

4.9.3.4 Sperrungen von Geräte-Zertifikaten

Die Sperrung von Geräte-Zertifikaten erfolgt über folgende Rolleninhaber und Webseiten bzw. Schnittstelle (Kapitel 4.9.3):

- Durch den Geräteadministrator über den Sperrservice des TSP für Geräte-Zertifikate.
- Optional: REST-Schnittstelle.
- Durch den Sperr-Operator des Sperrservice des TSP

4.9.3.5 Sperrung von Zertifikaten zur Unterstützung des PKI-Betriebs

Zur Unterstützung des PKI-Betriebs cPKI werden die in Kapitel 1.3.1.3.1 und 1.3.1.3.2 beschriebenen Web-Server- und OCSP-Zertifikate eingesetzt.

Aufforderungen für diese Zertifikatssperrungen werden über den Service Desk der DTAG an den TSP gemeldet.

4.9.3.6 Sperrung von externen Web-Server-Zertifikaten

T-Systems verpflichtet sich zu einer Sperrung des Web-Server-Zertifikats der cPKI-Webseiten (Kapitel 1.3.1.3.1), sobald der Verdacht einer Schlüsselkompromittierung besteht. T-Systems behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. Die Sperrung wird über eine Zertifikatssperrliste (CRL) bekannt gegeben. Ein gesperrtes Web-Server-Zertifikat wird unverzüglich durch ein neues ersetzt.

T-Systems sperrt den Zugang zum Web-Server, wenn dessen Sicherheit durch eine Sperrung dieses Zertifikats gefährdet ist.

4.9.3.7 Sperrung des OCSP-Responder-Zertifikats

T-Systems verpflichtet sich zu einer Sperrung des OCSP-Responder-Zertifikats (Kapitel 7.3ff), sobald der Verdacht einer Schlüsselkompromittierung besteht. T-Systems behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. Die Sperrung wird über eine Zertifikatssperrliste (CRL) bekannt gegeben. Ein gesperrtes OCSP-Zertifikat wird unverzüglich durch ein Neues ersetzt.

4.9.3.8 Sperrung von Sub-CA-Zertifikaten

T-Systems verpflichtet sich zu einer Sperrung des Sub-CA-Zertifikats (Kapitel 1.3.1.2 ff), sobald der Verdacht einer Schlüsselkompromittierung besteht oder Vorgaben dies erfordern.

Es besteht ein interner Geschäftsprozess der T-Systems zur Sperrung von Sub-CA-Zertifikaten.

4.9.4 Fristen für einen Sperrauftrag

4.9.4.1 Service Desk des Trust Centers

Nach Eingang eines vollständigen Sperrauftrags (nur bei Zertifikats-Missbrauchsfällen) beim Service Desk des Trust Centers sperrt T-Systems das Endteilnehmer-Zertifikate innerhalb von 24 Stunden und veröffentlicht diese in der Zertifikatssperrliste (CRL) und OCSP-Datenbank.

4.9.4.2 Service Desk der DTAG

Die Einhaltung von Fristen für Sperraufträgen liegt in der Verantwortung des Service Desks der DTAG (Delegated Third Party). Sobald für Endteilnehmer-Zertifikate ein Sperrgrund gemäß Kapitel 4.9.1 vorliegt, muss der Sperrauftrag so schnell als möglich innerhalb einer wirtschaftlich angemessenen Frist vom Endteilnehmer, Schlüsselverantwortlichen oder Sperrberechtigten gestellt werden.

4.9.5 Bearbeitungsfristen der Zertifizierungsstelle für Sperranträge

Die Sperrung durch den Endteilnehmer, Schlüsselverantwortlichen und Sperrberechtigten erfolgt telefonisch über die jeweils gültige Rufnummer des DTAG Service Desks. Dieser steht täglich von 08 bis 18 Uhr auch an Wochenenden zur Verfügung und wird unmittelbar nach Eingang des Sperrwunsches den Sperrvorgang auslösen. Die entsprechenden Schnittstellen (WCF und REST) stehen den angeschlossenen Systemen 7x24h zur Verfügung. Der Sperrvorgang wird unmittelbar an die angeschlossenen Systeme weitergegeben. Der OCSP-Dienst, der auf diese Systeme zugreift, verfügt damit über den aktuellen Zertifikatsstatus.

4.9.6 Überprüfungsvorgaben für vertrauende Dritte

Vertrauende Dritte müssen die Möglichkeit erhalten, den Status von Zertifikaten überprüfen zu können. Zu diesem Zweck kann der OCSP-Responder genutzt werden, der den aktuellen Status eines Endteilnehmer-, Registrator- oder OCSP-Responder-Zertifikat übermittelt.

Eine weitere Methode, wie ein vertrauender Dritter überprüfen kann, ob ein Zertifikat gesperrt ist, ist die Prüfung der aktuellen Zertifikatssperrliste (CRL), die auf dem Verzeichnisdienst der cPKI veröffentlicht wird (siehe Kapitel 2.2).

Gesperrte CA-Zertifikate (außer Root-CA-Zertifikate) werden in der standardisierten Zertifikatssperrliste (CARL) veröffentlicht und können daher mit standardkonformen Anwendungen geprüft werden.

4.9.7 Veröffentlichungsfrequenz von Sperrinformationen

Die Zertifikatssperrliste (CRL) als auch Zertifizierungsstellen-Sperrliste (CARL) wird, wie im Kapitel 2.3 beschrieben, über den Verzeichnisdienst publiziert.

Die Zertifikatssperrliste (CRL), in der Zertifikats-Sperrungen von Endteilnehmern aufgeführt sind, wird mindestens einmal pro Tag automatisch vom CA-System aktualisiert und über den Verzeichnisdienst veröffentlicht. Innerhalb dieses automatischen Zyklus kann das Trust Center die Zertifikatssperrliste (CRL) manuell generieren.

In den Sperrlisten für Zertifizierungsstellen (CARL) werden alle gesperrten CA-Zertifikate (keine Root-CA-Zertifikate) veröffentlicht, die von der jeweiligen Stammzertifizierungsstelle (Root-CA) ausgestellt wird. In Abbildung 1 bis Abbildung 3 sind die jeweiligen Stamm- und untergeordneten Zertifizierungsstellen (Sub-CA) grafisch dargestellt. Die Aktualisierung der CARL erfolgt alle 6 Monate oder ereignisbezogen, die Veröffentlichung erfolgt über den entsprechenden Verzeichnisdienst.

Gesperrte Zertifikate, die außerhalb des Gültigkeitszeitraums liegen, werden aus der Sperrliste entfernt.

Die OCSP-Datenquelle (repository) wird spätestens nach fünfzehn (15) Minuten aktualisiert. Die OCSP-Antworten haben eine maximale Gültigkeit von fünf (5) Tage.

Die OCSP Status Informationen werden Event basiert aktualisiert, d.h. ein Sperr Event an der CA ist in einem Zeitraum < 15 Minuten auch im OCSP online. OCSP und CRL beruhen beide auf den Daten der jeweiligen CA, daher ist die Konsistenz der verschiedenen Auskunftsdienste zum Zeitpunkt der Erstellung der CRL‘s sichergestellt.

4.9.8 Maximale Latenzzeit von Sperrlisten

Die Latenzzeit der Zertifikatssperrliste (CRL) nach automatischer Generierung beträgt wenige Minuten.
Die Latenzzeit für die Zertifizierungsstellen-Sperrliste (CARL) nach manueller Generierung beträgt wenige Minuten.

4.9.9 Online Verfügbarkeit von Sperr-/Statusinformationen

Zusätzlich, zu den Sperrinformationen über CRL und CARL (Kapitel 2.3, 4.9.7), stellt T-Systems Online-Informationen zum Zertifikatsstatus via OCSP bereit. Die URL des OCSP-Responders ist im Zertifikat in der Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)“ (siehe Kapitel 7.1.2.9) aufgeführt.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

Vertrauende Dritte müssen den Status eines Zertifikats überprüfen, dem sie vertrauen möchten. Für den Abruf aktueller Statusinformationen steht der OCSP-Dienst (OCSP-Responder) zur Verfügung. Eine weitere Möglichkeit der Statusabfrage liefert die aktuelle Zertifikatssperrliste (CRL).

4.9.11 Andere verfügbare Formen der Veröffentlichung von Sperrinformationen

Abhängig vom Zertifikatstyp wird der Zertifikatsnehmer, Antragsteller, Vertreter oder eine weitere Instanz über die Sperrung des Zertifikats per E-Mail benachrichtigt (revoke notification).

4.9.12 Besondere Anforderungen bezüglich der Kompromittierung privater Schlüssel

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu sperren (Kapitel 4.9.1).

4.9.13 Umstände einer Suspendierung

Gründe für die Suspendierung von Zertifikaten können sein:

- temporäre Nicht-Verfügbarkeit eines Zertifikatsträgermediums (z.B. MyCard vergessen),
- längere geplante Abwesenheit von Mitarbeitern,
- der Verdacht der unerlaubten Verwendung des Zertifikatsträgermediums,
- die Ausführung des Prozesses „Employee Leave“ im System cIAM sein, woraufhin der User für 30 Tage suspendiert wird, bevor eine Revoke Auftrag zur endgültigen Sperrung erfolgt.

4.9.14 Wer kann eine Suspendierung beantragen?

- cIAM über TAdmin2 mittels des IT-Prozesses „Employee leave”
- Autorisierte Personen, die als Subjekt des Zertifikats erscheinen.
- Autorisierte Personen von Personen- und Funktionsgruppen, juristischen Personen und Geräten (z.B. Mitarbeiter Personalmanagement).
- Autorisierte Personen die als Schlüsselverantwortliche oder Sperrberechtigte auftreten
- Autorisierte Personen des T-Systems Trust Centers.

4.9.15 Verfahren der der Suspendierung

Autorisierte Personen können die temporäre Sperrung eines Zertifikates telefonisch beim Service Desk der DTAG beauftragen. Die Authentisierung und Autorisierung einer Person geschieht dabei in geeigneter Art und Weise.

Sind die Voraussetzungen zur Suspendierung erfüllt, wird eine temporäre Sperrung vorgenommen und das gesperrte Zertifikat in die Sperrinformationen übernommen. Mit dem täglichen Zyklus des CA-Systems (Kapitel 4.9.7) wird das Zertifikat in der Zertifikatssperrliste (CRL) veröffentlicht. Nach der Zertifikatssperrung stehen die Sperrinformationen per OCSP unmittelbar zur Verfügung.

Der Zertifikatsinhaber wird über die Durchführung der Suspendierung per E-Mail informiert.

Unabhängig davon behält sich das T-Systems Trust Center als Betreiber der cPKI vor, Zertifikate bei Vorliegen von mindestens einem, der in Kapitel 4.9.1, 4.9.13 aufgeführten Sperrgründe, zu temporär oder auch endgültig zu sperren.

4.9.16 Beschränkung des Suspendierungszeitraums.

Die maximale Sperrdauer einer Suspendierung über den automatischen Registrierungsplatz (cIAM) beträgt 30 Kalendertage, diese kann abhängig von der Zertifikatsgültigkeit verkürzt werden. Insofern die Zertifikatsgültigkeit nicht abgelaufen ist, erfolgt nach Ablauf von 30 Kalendertagen die Beauftragung von cIAM über TAdmin2 zur endgültige Sperrung.

Suspendierungen über Service Desk führen nicht automatisch zu einer endgültigen Sperrung der Zertifikate nach einem bestimmten Zeitraum. Die Gültigkeit Suspendierung ist in diesem Fall durch die Zertifikatsgültigkeit begrenzt.

4.10 Statusauskunftsdienste von Zertifikaten

Der Status von Endteilnehmer-Zertifikaten ist ermittelbar via OCSP-Dienst (Kapitel 2.1 und 2.2) und per Zertifikatssperrliste (CRL).

4.10.1 Betriebseigenschaften

Die von der cPKI ausgegebenen OCSP-Antworten von Endteilnehmer-Zertifikaten entsprechen den Vorgaben des RFC 6960.

Die OCSP-Antworten werden von einem OCSP-Responder signiert, dessen Zertifikat seinerseits von einer Zwischenzertifizierungsstelle (Sub-CA) signiert wurde, welche das betreffende Endteilnehmer-Zertifikat ausgestellt hat. In Abbildung 1 bis Abbildung 3 sind die jeweiligen Zuordnungen der Endteilnehmer zu den ausstellenden Stamm- und untergeordneten Zertifizierungsstellen (Sub-CA) grafisch dargestellt.

Die OCSP-Antwort enthält einen der folgenden Stati:

- gut (good) bedeutet:
  - es ist ein Aussteller(Issuer) des PKI-Services und
  - das Zertifikat ist gültig (innerhalb der Zertifikatslaufzeit) und
  - das Zertifikat ist nicht gesperrt.
- gesperrt (revoked) bedeutet:
  - es ist ein Aussteller (Issuer) des PKI-Services und
  - das Zertifikat ist gültig (innerhalb der Zertifikatslaufzeit) und
  - das Zertifikat wurde gesperrt.
- unbekannt (unknown) bedeutet:
  - das Zertifikat ist ungültig (außerhalb der Zertifikatslaufzeit) oder
  - das Zertikat ist gültig, wurde aber nicht von dem angefragten Aussteller (Issuer) des PKI-Services ausgestellt oder
  - das Zertikat ist gültig, wurde aber nicht von dem Aussteller (Issuer) des PKI-Services ausgestellt.

Das Zertifikat des OCSP-Responders enthält die in Kapitel 7.3.2 beschriebene Erweiterung.

Die von der cPKI ausgegebenen Zertifikatssperrlisten (CRL) entsprechen den Vorgaben des RFC 5280. Die Zertifikatssperrlisten (CRL) werden von der jeweiligen Sub-CA, die Sperrlisten für Zertifizierungsstellen (CARL) werden von der jeweiligen Root-CA ausgestellt, signiert und auf dem LDAP-Verzeichnisdienst veröffentlicht. In Abbildung 1 bis Abbildung 3 sind die jeweiligen Zuordnungen der Endteilnehmer zu den ausstellenden Stamm- und untergeordneten Zertifizierungsstellen (Sub-CA) grafisch dargestellt.

Gesperrte Zertifikate werden erst nach dem Ablauf der Gültigkeit aus der Zertifikatssperrliste (CRL) entfernt.

T-Systems hat Mechanismen zum Schutz des Sperrstatus-Dienstes (CRL, CARL, OCSP) gegen unbefugte Versuche implementiert, um Manipulationen an Sperrstatusinformationen (hinzufügen, löschen, ändern) zu verhindern.

Der TSP bietet kein OCSP-Stapling an.

4.10.2 Verfügbarkeit des Dienstes

Der OCSP-Dienst als auch die CRL/CARL auf dem LDAP-Verzeichnisdienst stehen 7x24h Stunden zur Verfügung. Die Antwortzeit des OCSP-Responders und LDAP-Verzeichnisdienst beträgt unter normalen Betriebsbedingungen weniger als 10 Sekunden.

4.10.3 Optionale Funktionen

Der OSCP-Responder unterstützt die GET-Methode.

4.11 Beendigung des Vertragsverhältnisses / Einstellung des Betriebs

Im Falle einer Vertragskündigung durch den Kunden oder der T-Systems als Betreiber der cPKI erfolgt zunächst unmittelbar die Deaktivierung der zur Verfügung gestellten Zertifikatstypen. Dies hat zur Folge, dass eine Neubeantragung als auch Erneuerung von Endteilnehmer-Zertifikaten nicht mehr möglich ist. Darüber hinaus werden Zertifikate nach dem Kündigungsdatum gesperrt und verlieren ihre Gültigkeit.
Sämtliche Funktionen zur Anmeldung an der jeweiligen Webseite, Neuausstellung, Erneuerung und Sperrung von Zertifikaten werden unterbunden; eine Zertifikats-Validierung über die Zertifikatssperrliste (CRL) und OCSP wird aber weiterhin unterstützt.

Im Fall der Einstellung des Betriebes der cPKI werden die nachfolgenden Maßnahmen ergriffen:

- Information aller Zertifikatsnehmer sowie vertrauenden Parteien mit einer Vorlauffrist von mindestens drei Monaten.
- Sperrung aller Benutzerzertifikate sowie der Zertifikate der Zertifizierungsstellen.
- Vernichtung der privaten Schlüssel der Zertifizierungsstellen.
- Veröffentlichung der entsprechenden CA- und Root-CA-Sperrlisten.

Einzelvertraglich kann zusätzlich hierzu jedoch eine gesonderte Übergangsregelung in schriftlicher Form getroffen werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

Die im Rahmen der cPKI verwendeten Schlüsselpaare der Zwischenzertifizierungsstellen (Sub-CA) (siehe Abbildung 1 bis Abbildung 3) werden auf einem sicherheitsüberprüften Hardware Security Module (HSM) gespeichert und in sicherer Umgebung betrieben. Die Speicherung des Schlüsselmaterials auf weiteren HSMs erfolgt ausschließlich zur Schlüsselsicherung (Key-Back-Up) und dient zur Wiederherstellung und Aufrechterhaltung des Dienstes durch qualifiziertes und sicherheitsgeprüftes Personal (Trusted Role) des Trust Centers. Eine Schlüsselhinterlegung (Escrow) bei Dritten (z.B. Treuhänder, Notar) ist nicht vorgesehen.

Darüber hinaus erfolgt für Endteilnehmer-Verschlüsselungszertifikate eine Schlüsselsicherung (Key-Back-Up) in der CA Datenbank in der Betriebsumgebung des Trust Centers. Der Zugriff ist mit einem Schlüssel aus dem HSM abgesichert.

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Eine Schlüsselwiederherstellung ist gebunden an die Zustimmung des Zertifikatsinhabers. Die Wiederherstellung von Verschlüsselungsschlüsseln bzw. -zertifikaten ist dabei beschränkt auf eine Bereitstellung für die Zertifikatsinhaber selbst (MyCard oder mobile Endgeräte) und für von Zertifikatsinhabern ausdrücklich autorisierte Vertreter (MyCard). Die Autorisierung von Aufträgen für die Wiederherstellung von Verschlüsselungsschlüsseln erfolgt ausschließlich nach vorheriger Authentifizierung und Berechtigungsprüfung des Antragstellers.

Eine Schlüsselwiederherstellung an Dritte ohne Zustimmung des Zertifikatsinhabers ist gebunden an die Zustimmung der im Konzern verantwortlichen Stellen für IT-Sicherheit, Datenschutz und Personalvertretung gemäß BetrVG. Hierzu ist die Zustimmung aller genannten Stellen erforderlich.

Abläufe und Policies im Rahmen von Wiederherstellungsprozessen siehe hierzu Kapitel 4.1.2.2

Der Betrieb der cPKI erfolgt in der zertifizierten Hochsicherheitsumgebung des T-Systems Trust Center. Alle Funktionen und Prozesse unterliegen strengen Sicherheitsmaßgaben, welche in einem Betriebskonzept (nicht öffentlich verfügbar) dokumentiert sind.

4.12.2 Sitzungsschlüsselkapselung und Richtlinien für die Wiederherstellung

Nicht anwendbar.

5 GEBÄUDE, VERWALTUNGS- UND BETRIEBSKONTROLLEN

Das T-Systems Trust Center ist in einem speziell geschützten Gebäude untergebracht und wird von fachkundigem Personal betrieben. Alle Prozesse für die Generierung und Verwaltung von Zertifikaten der dort betriebenen Zertifizierungsstellen sind genau definiert. Alle technischen Sicherheitsmaßnahmen sind dokumentiert.

Die folgenden Aussagen gelten für die vom T-Systems Trust Center betriebenen Zertifizierungsstellen.

Die angewendeten physikalischen, organisatorischen und personellen Sicherheitsmaßnahmen sind im Sicherheitsrahmenkonzept des Trust Centers [SRK TC] festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen.

Die für den operativen Betrieb notwendigen Sicherheitsmaßnahmen sind in dem Service- und Organisations-Handbuch sowie den Betriebsleitfaden des Trust Centers beschrieben.

Die Anforderungen aus [ETSI EN TSP] Kapitel 5, 6.3 und 7.3 sind umgesetzt, d.h. es sind Festlegungen

- zur Risikobewertung im Rahmen des ISMS,
- zu den Richtlinien zur Informationssicherheit,
- zum Asset-Management

beschrieben.

Das Management genehmigt die Risikobewertung und akzeptiert das identifizierte Restrisiko.

5.1 Physikalische Kontrollen

5.1.1 Standort und bauliche Maßnahmen

T-Systems betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Rechenzentren (Twin Core) besteht.

Die Errichtung und der Betrieb des Trust Centers erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Verbandes der Schadenversicherer e.V. (VdS) / neu: Gesamtverband der Deutschen Versicherungswirtschaft (GDV), der einschlägigen DIN-Normen zu Brandschutz, Rauchschutz und Angriffshemmung. Das Trust Center ist sicherheitstechnisch vom VdS / GDV abgenommen.

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

5.1.2 Räumlicher Zutritt

Im Trust Center gilt eine Zutrittsregelung die die Zutrittsrechte für Mitarbeiter, Mitarbeiter von Fremdfirmen und Gästen in den einzelnen Sicherheitszonen regelt. Der Zutritt ist zwischen den Sicherheitsbereichen nur über Personenvereinzelungsanlagen möglich. Der kontrollierte Zutritt zu den verschiedenen Sicherheitsbereichen ist weiter mit einem rechnergesteuerten Zutrittskontrollsystem geschützt. Gäste werden nur in Ausnahmefällen und nach vorheriger Anmeldung empfangen. Hier gelten besondere Sicherheitsvorschriften.

5.1.3 Stromversorgung und Klimatisierung

Die Ansaugöffnungen für die Außenluft sind so angeordnet, dass keine Schadstoffe wie Staub und Schmutz, ätzende, giftige oder leicht brennbare Gase eindringen können. Die Systeme werden mit einem sehr geringen Außenluftanteil betrieben. Die erforderlichen Zuluftöffnungen sind zugangsgeschützt. Zum Schutz gegen Luftverunreinigung durch

schwebende Partikel sind Filter installiert. Die Frischluftansaugung wird ständig auf aggressive Gase überwacht. Im Notfall (z.B. Brand in der Umgebung) wird die Außenluftansaugung automatisch durch Luftklappen verschlossen.

Zum Ausfallschutz der Energieversorgung ist eine unabhängige Wechselspannungsversorgung entsprechend VDE-Vorschriften installiert. Sie bietet Schutz gegen Spannungsschwankungen, unterbrechungsfreie Kurzzeitüberbrückung, eine Langzeitüberbrückung mit zwei getrennten, ortsfesten Notstromaggregaten deren Leistung die der Volllast-Leistungsaufnahme des Rechenzentrums entspricht.

5.1.4 Wassergefährdung

Das Trust Centers liegt in einer geschützten Lage, d.h. es liegt nicht in der Nähe von Gewässern und Niederungen (Hochwassergefahr).

5.1.5 Brandschutz

Die geltenden Brandschutzbestimmungen (z.B. DIN 4102, Auflagen der örtlichen Feuerwehr, Vorschriften über Feuerresistenz, VDE-gerechte Elektroinstallation) werden eingehalten. Alle Brandschutztüren besitzen automatische Schließeinrichtungen. In Absprache mit der Feuerwehr wird nur in äußersten Notfällen mit Wasser gelöscht.

Brandabschnitte sind durch feuerbeständige Bauteile gesichert. Durchgänge durch Brandschutzwände sind mit selbsttätig schließenden Brandschutztüren ausgestattet

In Bereichen mit Doppelböden sowie abgehängten Decken sind Brandschutzwände durchgehend bis zum Geschoßboden bzw. zur Geschoßdecke ausgeführt.

In alle Systemräume, Systemoperatorräume, Archivräume, USV-Räume sowie weitere ausgewählte Räume sind Brandfrühesterkennungssysteme (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut. Die Brandbekämpfung erfolgt mit inertem Gas.

5.1.6 Aufbewahrung von Datenträgern

Alle Datenträger, die Produktions-Software und -daten, Audit-, Archiv- oder Sicherungs-Informationen 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. Kryptographische Geräte werden vor ihrer Entsorgung gemäß den Richtlinien des Herstellers physisch vernichtet. Andere Abfälle werden gemäß den regulären Entsorgungsrichtlinien von T-Systems entsorgt.

5.1.8 Externe Datensicherung

T-Systems führt routinemäßige Sicherungskopien von kritischen Systemdaten, Audit-Protokolldaten und anderen vertraulichen Informationen durch. Sicherungskopien werden räumlich getrennt von den Ursprungsdaten gelagert.

5.2 Organisatorische Maßnahmen

Die organisatorischen Maßnahmen sind im Sicherheitsrahmenkonzept [SRK TC] und Sicherheitskonzept der cPKI [Siko cPKI] dokumentiert und werden durch das Betriebskonzept des Trust Centers umgesetzt. Die relevanten Anforderungen aus [ETSI EN TSP] Kapitel 7.4 b, c, d, e sind umgesetzt.

5.2.1 Vertrauenswürdige Rollen

Vertrauenswürdige Personen sind alle Personen (T-Systems Mitarbeiter, Auftragnehmer, und Berater) mit Zugang zu oder Kontrolle über Authentifizierungs- oder kryptografische Abläufe, die erhebliche Auswirkungen auf Folgendes haben können:

- die Validierung von Informationen in Zertifikatsaufträgen,
- die Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatsaufträgen, Sperraufträgen oder Erneuerungsaufträgen,
- die Vergabe oder den Widerruf von Zertifikaten, einschließlich Personal, das Zugang und Zugriff auf die Datenbanksysteme hat,
- den Umgang mit Informationen oder Aufträgen von Endteilnehmern.

Vertrauenswürdige Personen sind insbesondere:

- Mitarbeiter des Trust Centers (z.B. Systemadministration),
- Mitarbeiter kryptografischer Abteilungen,
- Sicherheitspersonal,
- zuständiges technisches Personal und
- für die Verwaltung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

Die oben genannten vertrauenswürdigen Personen müssen die in diesem Dokument festgelegten Anforderungen (Kapitel 5.3.1) erfüllen.

Ebenfalls müssen diese vertrauenswürdigen Personen frei von Interessenskonflikten gestellt werden, damit die ausgeübten Rollen unbefangen und vorurteilsfrei ausgeübt werden können. Die Mitarbeiter verpflichten sich zur Anerkenntnis und Einhaltung des vom Konzern vorgegebenen „Code of Conduct“.

Das Change Advisory Board des T-Systems Trust Centers ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten und CP/CPS der von T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.2.2 Anzahl involvierter Personen pro Aufgabe

Die Aufrechterhaltung des Betriebs der Zertifizierungsstelle und des Verzeichnisdienstes 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 durchgeführt.

Den Systemadministratoren des Trust Centers stehen im Störungsfalle zusätzlich, Service Desk Rechte, Registrator- oder Trust-Center-Operatorrechte zum Zwecke der Störungsbeseitigung zur Verfügung.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

5.2.3.1 Mitarbeiter des Trust Centers

Mitarbeiter der internen Registrierungsstelle der T-Systems, die als besonders vertrauenswürdige Personen eingestuft sind und besonders vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer T-Systems-internen Sicherheitsüberprüfung (siehe Kapitel 5.3.2).

T-Systems stellt sicher, dass Mitarbeiter einen vertrauenswürdigen Status erlangt haben und die Zustimmung der Abteilung erteilt wurde, bevor diese Mitarbeiter

- Zugangsgeräte und Zugang zu den erforderlichen Einrichtungen erhalten,

- die elektronische Berechtigung zum Zugriff auf die cPKI und andere IT-Systeme erhalten,
- zur Durchführung bestimmter Aufgaben im Zusammenhang mit diesen Systemen zugelassen werden.

Die Mitarbeiter des Trust Centers werden nach positiver Prüfung formell vom Leiter des Trust Centers ernannt.

5.2.3.2 Mitarbeiter des Kunden die Authentifizierungen bzw, Identifizierungen von Personen vornehmen

Der Auftraggeber muss gewährleisten, dass nur vertrauenswürdige Personen Tätigkeiten zur Authentifizierung von Personen, Gruppen, bzw. Funktionsgruppen wahrnehmen. Dies betrifft insbesondere HR, Mitarbeiter der vertragswidrigen Datenbasis cIAM sowie Beauftragte, die externe Mitarbeiter in den HR Systemen anlegen.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Folgende Rollen unterliegen einer Funktionstrennung und werden daher von verschiedenen Mitarbeitern begleitet:

- Die Erstellung, Installation oder Vernichtung von Sub-CA- und Root-CA-Zertifikaten,
- Sicherung und Rücksicherungen von Datenbanken und HSMs.
- Wiederherstellung von Schlüsselmaterial

5.3 Personelle Maßnahmen

T-Systems setzt umfassende personelle Sicherheitsmaßnahmen um, die einen hohen Schutz ihrer Einrichtungen und der Zertifizierungsdienste gewährleisten. Im Trust Center ist der Einsatz von qualifiziertem geschultem Personal obligatorisch die personellen Maßnahmen sind im Sicherheitsrahmenkonzept [SRK TC] und im Sicherheitskonzept der cPKI [Siko cPKI] dokumentiert.

Das Personal unterliegt keinem Kostendruck oder Mengengerüst oder sonstigen Zwängen deren Einhaltung möglicherweise mit den Qualitätsanforderungen bei der Prüfung von Antragsunterlagen konkurrieren würde.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

5.3.1.1 Mitarbeiter der T-Systems

Für den Betrieb der in Kapitel 1 beschriebenen PKI-Dienstleistungen verlangt T-Systems von seinen Mitarbeitern, die eine vertrauenswürdige Rolle einnehmen sollen, entsprechende Nachweise über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.

In regelmäßigen Abständen ist ein neues polizeiliches Führungszeugnis der T-Systems vorzulegen.

5.3.1.2 Mitarbeiter der DTAG die Authentifizierungen, bzw. Identifizierungen von Personen vornehmen

Der Auftraggeber muss gewährleisten, dass das eingesetzte Personal die Tätigkeiten der Authentifizierungen, bzw. Identifizierungen von Personen in Bezug auf Fachkunde und Zuverlässigkeit durchführen kann. Die Qualifikation und Maßnahmen zur Zuverlässigkeitsprüfung müssen auch gegenüber Auditoren nachweisbar sein (siehe hierzu Kapitel 1.3.2.1).

5.3.2 Sicherheitsüberprüfung

5.3.2.1 Mitarbeiter der T-Systems

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt T-Systems eine

Sicherheitsüberprüfung durch mit folgendem Inhalt durch:

- Überprüfung und Bestätigung der bisherigen Beschäftigungsverhältnisse,
- Überprüfung von Arbeitszeugnissen,
- Bestätigung des höchsten oder maßgebenden Schul-/Berufsabschlusses,
- polizeiliches Führungszeugnis.

Sofern die in diesem Abschnitt festgelegten Anforderungen nicht erfüllt werden können, macht T-Systems 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 führt, 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 führen oder eine Kündigung beinhalten.

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

5.3.2.2 Mitarbeiter der DTAG die Authentifizierungen, bzw. Identifizierungen von Personen vornehmen

Nicht anwendbar

5.3.3 Schulungs- und Fortbildungsanforderungen

5.3.3.1 Mitarbeiter der T-Systems

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

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

- fortgeschrittene PKI-Kenntnisse,
- Verfahrensweisen nach ITIL,
- Daten- und Fernmeldegeheimnis,
- Informationsschutz,
- Zutrittsschutz,
- Antikorruption,
- Datenschutz

- Sicherheits- und Betriebsrichtlinien und –verfahren von T-Systems,
- Verwendung und Betrieb eingesetzter Hardware und Software,
- Meldung von und Umgang mit Störungen und Kompromittierungen und
- Verfahren für die Schadensbehebung im Notfall (Disaster Recovery) und Geschäftskontinuität (Business Continuity).

Mitarbeiter, welche mit der Validierung von Zertifikatsaufträgen befasst sind, erhalten zusätzlich Schulungen in den folgenden Bereichen:

- Richtlinien, Verfahren und aktuelle Entwicklungen zu Validierungsmethoden
- Inhalte und insbesondere relevante Änderungen des vorliegenden CP/CPS
- Relevante Anforderungen und Vorgaben aus den [CAB-BR]
- Allgemeine Bedrohungs- und Angriffsszenarien bzgl. der Validierungsmethoden (z.B. Social Engineering)

Die Schulungen sind schriftlich zu dokumentieren und die Lerninhalte jährlich mit einer Prüfung (examination) zu bestätigen.

5.3.3.2 Mitarbeiter der DTAG die Authentifizierungen, bzw. Identifizierungen von Personen vornehmen

T-Systems stellt dem Auftraggeber entsprechende Schulungsunterlagen zur Verfügung, aus der die Funktionen, Prozesse und begleitende Dokumentation ersichtlich sind.

Der Auftraggeber ist verpflichtet, neue Mitarbeiter vor Übernahme der Registrierungstätigkeit entsprechend den Anforderungen zu schulen. Diese Schulung ist schriftlich zu dokumentieren und auf Anfrage der T-Systems oder einem beauftragten Dritten nachzuweisen.

5.3.4 Nachschulungsintervalle und -anforderungen

5.3.4.1 Mitarbeiter der T-Systems

Das Personal der T-Systems erhält im erforderlichen Umfang und den erforderlichen Abständen Auffrischungsschulungen und Fortbildungslehrgänge.

5.3.4.2 Mitarbeiter der DTAG die Authentifizierungen, bzw. Identifizierungen von Personen vornehmen

Im Falle, dass T-Systems neue Schulungsunterlagen bereitstellt, die relevante Schulungsthemen beinhalten, ist der Auftraggeber verpflichtet, eine gesonderte Schulung durchzuführen und Verfahrensanweisungen anzupassen. Diese Schulung ist schriftlich zu dokumentieren und auf Anfrage der T-Systems oder einem beauftragten Dritten nachzuweisen.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzrotation

Nicht anwendbar.

5.3.6 Sanktionen bei unerlaubten Handlungen

5.3.6.1 Mitarbeiter der T-Systems

Die T-Systems behält sich vor, unbefugter Handlungen oder anderer Verstöße gegen dieser CP/CPS und Bezugsvertrag/Nutzungsbedingungen der daraus abgeleiteten Verfahren zu ahnden und entsprechende

Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen und können Maßnahmen bis einschließlich der Kündigung beinhalten.

5.3.6.2 Mitarbeiter der DTAG die Authentifizierungen, bzw. Identifizierungen von Personen vornehmen

Die Ahndung etwaige Verstöße obliegt der Verantwortung des Auftraggebers.

Bei deliktischem Handeln oder Straffällen wird die verantwortliche Person zur Verantwortung gezogen. Dies kann Disziplinarmaßnahmen als auch strafrechtliche Konsequenzen zur Folge haben.

5.3.7 Anforderungen an unabhängige Auftragnehmer

T-Systems behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter von T-Systems 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 T-Systems nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.3.8 Dokumentation für das Personal

5.3.8.1 Mitarbeiter der T-Systems

Um die beruflichen Pflichten angemessen erfüllen zu können, stellt T-Systems seinen Mitarbeitern alle dafür erforderliche Dokumente (Schulungsunterlagen, Verfahrensanweisungen) und Hilfsmittel zur Verfügung.

5.3.8.2 Mitarbeiter der DTAG die Authentifizierungen, bzw. Identifizierungen von Personen vornehmen

T-Systems stellt entsprechende Schulungsunterlagen zur Verfügung, aus der die Funktionen, Prozesse und begleitende Dokumentation in Bezug auf die Tätigkeit zur Authentifizierung, bzw. Identifizierung von Personen ersichtlich sind.

5.4 Protokollereignisse

Es ist im Loggingkonzept sowie im Installationshandbuch festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden und wie sie vor Verlust und unbefugtem Zugriff geschützt werden. Es werden dabei die Anforderungen aus [ETSI EN TSP] Kap. 7.10 umgesetzt.

5.4.1 Art der aufgezeichneten Ereignisse

5.4.1.1 CA-Schlüsselpaare und CA-Systeme

Für das Lifecycle–Management für CA-Schlüsselpaare bzw. von CA-Systemen protokolliert das T-Systems Trust Center für cPKI mindestens die folgenden Ereignisse:

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

5.4.1.2 EE- und CA-Zertifikate

Für das Lifecycle-Management von EE- als auch CA-Zertifikaten und deren Validierung protokolliert das T-Systems Trust Center für die cPKI mindestens die folgenden Ereignisse:

- Auftrag 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 wird im Ticketsystem SM9 der DTAG dokumentiert.
- Annahme oder Ablehnung von Zertifikatsaufträgen
- Ausstellung eines Zertifikates
- Erzeugung von Sperrlisten (CRL) und OCSP-Einträgen

5.4.1.3 Sonstige sicherheitsrelevante Ereignisse

Zusätzlich werden vom T-Systems Trust Center für den Betrieb der Infrastruktur der cPKI 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
- Ergebnisse von Netzwerkprüfungen (Schwachstellenüberprüfungen)

5.4.2 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/History-Daten/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft T-Systems ihre Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen der cPKI.

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 gemäß Kapitel 5.5.2 archiviert.

5.4.4 Schutz der Audit-Protokolle

Audit-Protokolle/History-Daten/Logging-Dateien werden mit Betriebssystemmechanismen gegen unbefugten Zugriff geschützt.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Eine inkrementelle Sicherung von Audit-Protokolle/History-Daten/Logging-Dateien wird täglich durchgeführt.

5.4.6 Audit-Erfassungssystem

Audit-Protokolle/History-Daten/Logging-Dateien von Anwendungs-, Netzwerk- und Betriebssystemebene werden automatisch erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von T-Systems-Mitarbeitern aufgezeichnet.

5.4.7 Benachrichtigung des ereignisauslösenden Subjekts

Ereignisse, die das Audit-Monitoringsystem erfasst, werden bewertet und 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 Schwachstellenbewertung

Nach jeder signifikanten System- oder Netzwerkänderung oder einer Aufforderung vom CA/Browserforum erfolgt innerhalb einer Woche, mindestens jedoch alle 3 Monate eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan). Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen festgelegt und in einem definierten Plan umgesetzt. Die Schwachstellenüberprüfungen, ihre Ergebnisse und Aktionen (Behebungen, Austausch) werden dokumentiert.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen, die dem TSP mitgeteilt wurden, werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Im Falle, dass eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

5.5 Datenarchivierung

5.5.1 Art der archivierten Datensätze

T-Systems archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener Form (z.B. Angebote, Aufträge),
- Informationen in Zertifikatsanträgen und zum Zertifikatslebenszyklus (z.B. Sperr- und Erneuerungsanträge),
- Soft-PSE,
- alle Audit-Daten/Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden,
- Zentrale Schlüsselsicherung (Key-Back-Up) von Soft-PSE.

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, werden sieben (7) Jahre nach Ablauf der Zertifikatsgültigkeit vorgehalten,
- Audit- und Event Logging Daten werden entsprechend der gesetzlichen Bestimmungen archiviert.

5.5.3 Schutz von Archiven

T-Systems 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 Vollsicherung Sicherung der elektronischen Daten wird täglich durchgeführt.

T-Systems bewahrt die Datenträger auf, die die Archivdaten und die zur Verarbeitung der Archivdaten erforderliche Anwendungen enthalten, um die Archivdaten für den in dieser CP/CPS festgelegten Archivierungszeitraum zu gewährleisten.

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 Archivierungssystem (intern / extern)

T-Systems 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

Zertifikate verlieren ihre Gültigkeit nach Überschreitung des Gültigkeitszeitraums.

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.

Ein Schlüsselwechsel von Endteilnehmer-Zertifikaten liegt in der Verantwortung des Auftraggebers. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3).

Die Generierung neuer CA- und Root-CA-Schlüssel als auch OCSP-Responder-Zertifikate wird dokumentiert und gemäß den Regelungen des Schlüsselgenerierungsverfahren (Key Generation Ceremony) überwacht. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3).

T-Systems informiert unverzüglich den DTAG internen Auftraggeber vor Integration der neuen CA- und Root-CA-Zertifikate in die entsprechenden Dienste, damit ein reibungsloser Übergang von altem auf ein neues Schlüsselpaar möglich wird.

Abgelaufene oder gesperrte CA- und Root-CA-Zertifikate stehen weiterhin zur Validierung auf einer Webseite zur Verfügung, bis das letzte Endteilnehmer-Zertifikat abgelaufen ist und nach der gesetzlich vorgeschriebenen Archivierungszeit gelöscht wurde.

5.7 Kompromittierung und Wiederherstellung (Desaster Recovery)

5.7.1 Umgang mit Störungen und Kompromittierungen

T-Systems hat ein IT-Servicemanagement gemäß ITIL sowie ISMS Prozesse etabliert, über die Störungen und Sicherheitsvorfälle nach definierten Standard-Prozessen bearbeitet werden.

Durch die Festlegung aller erforderlichen Ansprechpartner und entsprechend eingerichteter Gruppen in den IT-Servicemanagement-System sowie der Etablierung einer Rufbereitschaft und des MoD (Manager on Duty) ist sichergestellt, dass die Bearbeitung von Störungen und Sicherheitsvorfälle kurzfristig beginnt, damit der Schaden möglichst gering bleibt und schnell beseitigt werden kann.

Die cPKI verfügt über ein Service Level Agreement (SLA), indem der Störungsprozess und die Servicekette ausführlich beschrieben ist.

Störungen werden vom Endteilnehmer über die im Service Level Agreement (SLA) definierten Kontakte eingereicht und im Rahmen des Service Managements bearbeitet.

Das Personal des Service Desk bewertet zunächst die Störung auf Basis der im Service Level Agreement (SLA) definierten Störungsklassen, bevor die Störung in die Störungsbearbeitungsanwendung der T-Systems eingegeben, priorisiert und an den/die Fachbereich(e) zwecks Störungsbeseitigung weitergeleitet wird. In der EDV-Anwendung werden transparent alle Informationen revisionssicher gespeichert, um jederzeit den Bearbeitungsstand der Störung bis zur Beseitigung nachvollziehen zu können.

Das Service Desk wird, entsprechend der Störungsklasse, von dem Fachbereich über den Bearbeitungszustand in Kenntnis gesetzt, um entsprechende Informationen bereitstellen zu können.

Der Auftraggeber wird, sofern erforderlich, schnellstmöglich informiert und in den Prozess eingebunden.

5.7.2 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 Sicherheitsabteilung der DTAG/T-Systems 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).

Jegliche Hard- und Software die zur Bereitstellung der cPKI erforderlich ist, wird als Vermögensgegenstand (Asset) und Anwendung im Konfigurationsmanagement der T-Systems geführt.

Diese Anwendung bildet auch die Basis für ein Problem-Management.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme einer Kompromittierung des privaten Schlüssels einer CA oder Root-CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet. Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechende Zertifizierungsstellen-Sperrliste (CARL) zu generieren und zu veröffentlichen. Die Generierung neuer Schlüssel und Zertifikate ist gemäß den Arbeitsanweisungen zu dokumentieren und gemäß den Auflagen des jeweiligen Sicherheitskonzepts zu überwachen. Neue Zertifikate und ihre Fingerprints sind zu veröffentlichen (siehe hierzu Kapitel 2.2).

5.7.4 Geschäftskontinuität nach einem Notfall

T-Systems hat für den Rechenzentrumsbetrieb einen Notfallplan entwickelt, implementiert und getestet, um die Auswirkungen von Katastrophen (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 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),

- Ausweichverfahren,
- Wiederanlauf Verfahren,
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung,
- Sensibilisierungsmaßnahmen,
- 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 cPKI 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, mit der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden,
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur cPKI 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 Kapitel 8) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

Schlüsselmaterial des Endteilnehmers, dass auf MyCards (Smartcards) ausgestellt wurde, ist nicht im Rahmen dieses Notfallplans abgedeckt.

5.8 Betriebsbeendigung einer Zertifizierungs- oder Registrierungsstelle

Eine Betriebsbeendigung der Zertifizierungsstelle (Kapitel 1.3.1 ff) oder automatischen sowie der manuellen Registrierungsstelle der T-Systems (Kapitel 1.3.2) kann nur durch T-Systems ausgesprochen werden.

Im Falle der Einstellung des Zertifizierungsdienstes geht die Zertifizierungsstelle entsprechend den Vorgaben aus [ETSI EN TSP] Kap. 7.12 vor und hat dafür einen Beendigungsplan erstellt, der folgende Maßnahmen beschreibt:

- Benachrichtigung des DTAG internen Auftraggebers, Endteilnehmer und vertrauende Dritte über die geplante Einstellung des Dienstes,
- Fortführung der Sperrfunktionalitäten einschließlich der regelmäßigen Erstellung von Sperrlisten, Abruf der Zertifikatsstatusinformationen und Service-Desk-Funktionen,
- Sperrung von ausgegebenen CA-Zertifikaten,
- eventuell erforderliche Übergangsregelungen auf eine Nachfolge-CA,
- Aufbewahrung der Unterlagen und Archive der Zertifizierungsinstanz (CA).

Vor der Einstellung des Dienstes werden alle möglichen Maßnahmen getroffen, um den potentiellen Schaden für alle Beteiligten möglichst gering zu halten. Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen, betroffene nachgeordnete Stellen (Endteilnehmer, vertrauende Dritte, des DTAG internen Auftraggebers und T-Systems) so früh als möglich vorab über diese Betriebsbeendigung zu informieren.

Anschließend sind alle noch gültigen Zertifikate zu sperren. Anschließend werden alle Rechte der Mitarbeiter der Zertifizierungsstelle und der Registrierungsstellen entzogen, die privaten Schlüssel der CA werden vernichtet.

Alle elektronisch erfassten Daten mit Ausnahme der Zertifikate und Sperrlisten werden gelöscht. Die Zertifikate und Sperrlisten sowie Papierdokumente werden archiviert, um ggf. zur Beweissicherung in Gerichtsprozessen darauf zugreifen zu können

6 TECHNISCHE SICHERHEITSKONTROLLEN

Die technischen Sicherheitsmaßnahmen sind in einem Sicherheitsrahmenkonzept des Trust Centers [SRK TC] und Sicherheitskonzept der cPKI [Siko cPKI] festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen. Es werden die Vorgaben aus [ETSI EN TSP] Kap. 7.5 umgesetzt.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren (CA)

Alle Schlüsselpaare für CA-Zertifikate werden von geschultem und vertrauenswürdigem Fachpersonal in einem abstrahlarmen Raum auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140-2/ Level 3 evaluiert) in der sogenannten “Key Ceremony” (Schlüsselgenerierungsverfahren) erzeugt und abgelegt.

Im Fall von CA- und Root-CA-Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem evaluierten HSM (FIPS 140-1/ Level 3) erzeugt und abgelegt.

Alle Aktivitäten während der “Key Ceremony“ werden dokumentiert und von allen beteiligten Personen unterzeichnet. Diese Aufzeichnungen werden zu Audit- und Nachverfolgungszwecken für einen von T-Systems als angemessen erachteten Zeitraum aufbewahrt.

Die Generierung des Schlüsselpaars für ein Zertifikat für eine öffentliche Stammzertifizierungsstelle (Public Root) und dem zugehörigen Zertifikat für eine Zwischenzertifizierungsstelle (Sub-CA) erfolgt auf einer Offline-CA und dem zugeordneten kryptografischen Hardware-Moduls (HSM) unter Aufsicht eines unabhängigen und qualifizierten Auditor.

Die Generierung des Schlüsselpaars für eine Zwischenzertifizierungsstelle (Sub-CA) erfolgt auf dem für die cPKI zugeordneten kryptografischen Hardware-Moduls (HSM) im Online-Betrieb. Das zugehörigen Zertifikat der Zwischenzertifizierungsstelle wird auf der Offline-CA generiert.

Alle Schlüsselgenerierungen und Zertifikatsausstellungen an der Offline-CA werden mittels Prüfprotokoll und Video-Aufzeichnung protokolliert und revisionssicher dokumentiert.

Die Systeme der Offline-CA, bestehend aus Zertifizierungsinstanz, kryptografischen Hardware-Moduls (HSM) (inkl. Back-Up-Token) und Browser, werden „offline“, d.h. ohne Anbindung an irgendeine eine Netzstruktur, betrieben. Die Systeme der Offline-CA sind in einem verschließbaren Computer-Rack untergebracht und gehen Öffnung und Austausch versiegelt. Die Unversehrtheit der Versiegelung wird bei jeder Nutzung der Offline-CA geprüft und dokumentiert.

Schlüsselpaare für ausgegebene Signatur- und Authentifizierungszertifikate von Endteilnehmern basieren auf der MyCard als Trägermedium. Sie werden durch den Hersteller der MyCard in einer speziellen, abgeschirmten Umgebung erzeugt, durch das TCOS Chipkarten-Betriebssystem gesichert auf der Karte abgelegt und mit einer speziellen Transportversiegelung ausgeliefert.

Schlüsselpaare für Verschlüsselungszertifikate von Endteilnehmern werden durch die cPKI zentral in einer speziell geschützten Umgebung unter Verwendung von Hardware Security Modulen (HSM) erzeugt und während der Personalisierung gesichert auf der MyCard abgelegt.

6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Im Falle der Nutzung einer MyCard werden für Signatur und Authentifizierung die bei der Produktion auf die Karte aufgebrachten Schlüssel verwendet. Es findet keine Übermittlung dieser privaten Schlüssel außerhalb einer MyCard statt. Verschlüsselungsschlüssel werden serverseitig generiert und nach vorheriger Authentisierung des Endteilnehmers durch die angebotenen Anmeldeverfahren sowie Eingabe eines individuellen One Time Password über einen TLS-verschlüsselte Verbindung sicher auf die Smartcard übertragen.

Im Falle von Soft-PSE wird zum Schutz des privaten Schlüssels die Soft-PSE mit einem sicheren Passwort versehen. Dies gilt auch für Schlüsselmaterial (Soft-PSE), das im Rahmen einer Schlüsselsicherung (Key-Back-Up) erzeugt wurde.

Der Abruf von Schlüssel und Zertifikat, die im Rahmen einer „Zentralen Schlüsselsicherung“ erstellt wurden, kann:

- durch die manuelle Registrierungsstelle des Trust Centers und unter Einhaltung des in Kapitel 4.1.2.2 Prozzeses das Schlüsselmaterial und Zertifikate suchen und über eine verschlüsselte TLS/SSL-Verbindung auf eine Smartcard (MyCard) heruntergeladen werden.
- über die automatische Registrierungsstelle als KeyBackup bei der Erstellung einer neuen Smartcard Erstellung über eine verschlüsselte TLS/SSL-Verbindung auf eine Smartcard (MyCard) installiert werden.
- im Rahmen der Bereitstellung von Schlüsselmaterial für Mobile Devices über die automatische Registrierungsstelle über eine verschlüsselte TLS/SSL-Verbindung an das durch die DTAG betriebene Enterprise Mobile Device Management (EMM) übertragen werden. Die Speicherung, Sicherung sowie der Versand- und Installationsart der Schlüssel im EMM und auf den mobilen Endgeräten obliegt der Verantwortung des Auftraggebers.

Im Falle, dass der Endteilnehmer selbst Schlüsselpaare über das Betriebssystem oder Applikation generiert, oder ein anderes Schlüsselmedium (vorbeschlüsselte Smartcard) nutzt, entfällt die Zustellung von privaten Schlüsseln an den Endteilnehmer.

6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller

Alle Endteilnehmer und Registratoren reichen, nach erfolgreicher Authentifizierung, den zu zertifizierenden öffentlichen Schlüssel in elektronischer Form (PKCS#10-Request) über eine durch TLS/SSL gesicherten Verbindung bei der Zertifizierungsinstanz der cPKI ein.

6.1.4 Zustellung öffentlicher Zertifizierungsstellenschlüssel an vertrauende Dritte, Publikation öffentlicher Schlüssel der Zertifizierungsstelle

Das Stammzertifikat „Deutsche Telekom Root CA 2“ und „T-TeleSec GlobalRoot Class 2“, dass für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich ist, wird für alle Endteilnehmer und vertrauende Dritte durch die Einbettung in die gängigen Zertifikatsspeicher der Betriebssysteme und Anwendungen zur Verfügung gestellt.

Das Stammzertifikat „Deutsche Telekom Internal Root CA 1“ und „Deutsche Telekom Internal Root CA 2“, dass für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich ist, muss in den Zertifikatsspeicher von Arbeitsplatzsystemen nachinstalliert werden. Dies erfolgt bei gemanagten Arbeitsplatzsystemen der DTAG mittels GPO oder per automatisierter Softwareverteilung.

Das dem jeweiligen Stammzertifikat untergeordnete Sub-CA-Zertifikat wird im Rahmen einer Signatur durch die Applikation zur Zertifikatsvalidierung vom Absender (Quelle) mit versandt oder ist vorab in den jeweiligen Zertifikatsspeicher nachträglich zu installieren.

Alle Stammzertifikate und Sub-CA-Zertifikate stehen auf der öffentlichen Webseite https://corporate-pki.telekom.de/ und auf dem Verzeichnisdienst der cPKI zum Herunterladen bereit.

6.1.5 Schlüssellängen

Um nicht mit Hilfe der Kryptoanalyse private Schlüssel ermitteln zu können, müssen die Schlüssellängen innerhalb des definierten Verwendungszeitraums über eine ausreichende Länge verfügen.

Alle Zertifikate (Zwischenzertifizierungsstelle, Endteilnehmer), die von einer öffentlichen Stamm-zertifizierungsstelle ausgestellt werden, als auch dieses Zertifikat selbst, erfüllten die Anforderungen der Baseline Requirements [CAB-BR] in der aktuellen Fassung zum Zeitpunkt der Freigabe und Veröffentlichung.

Alle Zertifikate (Stamm- und Zwischenzertifizierungsstellen, Endteilnehmer), verfügen über eine RSA-Schlüssellängen von mindestens 2.048 Bit.

6.1.6 Generierung der Parameter von öffentlichen Schlüssel und Qualitätskontrolle

Der, während der Beauftragung, mit dem Zertifikatsrequest eingereichte öffentliche Schlüssel wird auf die folgenden Qualitätsparameter geprüft:

- für die Erzeugung wurde das Kryptoverfahren RSA verwendet
- die Mindestschlüssellänge für RSA-Schlüssel beträgt 2.048 Bit
- der Exponent des öffentlichen Schlüssels ist e >1 und ungerade
- als Hash-Algorithmus zulässig ist SHA-256,

Schlägt eine der Parameterüberprüfungen fehl, wird der entsprechende Zertifikatsauftrag mit einem Hinweistext abgelehnt.

6.1.7 Schlüsselverwendungen (gemäß X.509v3-Erweiterung „key usage“)

- key usage siehe Kapitel 7.1.2.1.
- extended key usage siehe Kapitel 7.1.2.5

6.2 Schutz privater Schlüssel und technische Kontrollen kryptographischer Module

Das Trust Center der T-Systems hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA- und Root-CA-Schlüsseln gewährleisten zu können. Dies bezieht sich auch auf das Schlüsselmaterial, das im Rahmen der „zentralen Schlüsselarchivierung“ für den Kunden vorgehalten wird.

Die Verwendung privater Schlüssel ist grundsätzlich immer durch Besitz (PSE, Token) und Wissen (PIN), der für die Nutzung autorisierten Rollenträger, geschützt.

Im Falle von privaten Schlüsseln für Zertifizierungsstellen werden im Trust Center auf einem HSM gesichert abgelegt und gegen nicht autorisierte Verwendung geschützt.

Endteilnehmer verpflichtet alle erforderlichen Vorkehrungen zu treffen, um Verlust, Offenlegung und unberechtigte Nutzung von ihren privaten Schlüsseln zu verhindern.

6.2.1 Standards und Kontrollen für kryptographische Module

Die privaten Schlüssel der CAs werden auf einem FIPS 140-2/ Level 3 evaluiertem Hardware Security Modul (HSM) abgelegt. Die Sicherung der Schlüssel wird unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken (siehe auch Kapitel 6.2.2) durchgeführt.

Zum Schutz der kryptographischen Geräte während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet, die während der FIPS- und CC-Zertifizierungen geprüft wurden. Die Geräte werden hierbei getrennt von den zum Betrieb und zur Nutzung benötigten PED-Keys aufbewahrt, so dass die Kompromittierung einer einzelnen Lokation nicht ausreicht, um die Geräte missbräuchlich zu verwenden

6.2.2 Mehrpersonenkontrolle (m von n) bei privaten Schlüsseln

T-Systems hat technische, organisatorische und prozessuale Mechanismen implementiert, die die Teilnahme mehrerer vertrauenswürdiger und geschulter Personen des T-Systems Trust Centers erfordern, um vertrauliche kryptographische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentification mit Key) geschützt, der nur hierfür zuständigen Personen bekannt ist. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung von privaten Schlüsseln (CA- und Root-CA-Schlüssel) bei Treuhändern außerhalb von T-Systems wird nicht durchgeführt.

Die Hinterlegung von Schlüsseln von Endteilnehmern ist in Kapitel 4.12 ff beschrieben.

6.2.4 Sicherung von privaten Schlüsseln

Das T-Systems Trust Center behält für Wiederherstellungs- und Notfallzwecke Sicherungskopien (Back-Up) des Schlüsselmaterials jedes CA-Zertifikates im erzeugenden HSM. Diese Schlüssel werden in verschlüsselter Form innerhalb des kryptografischen Hardware-Moduls (HSM) und zugehörigen Schlüsselspeichergeräten im Trust Center der T-Systems gespeichert.

Weiterhin gibt es Sicherungen der privaten CA-Schlüssel der jeweiligen Sub-CAs der cPKI in gesicherter Umgebung. Der Zugriff auf diese Schlüssel ist nur vertrauenswürdigen Personen des Trust Centers (Trusted Role) gestattet.

Der jeweilige private Schlüssel wird dabei in verschlüsselter Form auf speziellen Security-Tokens gespeichert.

Zur Wiederherstellung eines privaten Schlüssels einer CA, d.h. Installieren des Schlüssels in die CA-Software, werden ebenfalls mehrere vertrauenswürdige Personen des Trust Centers (Trusted Role) benötigt. Eine Wiederherstellung darf nur innerhalb der Hoch-Sicherheitszone des T-Systems Trust Centers erfolgen.

Im Rahmen der bestehenden Beauftrag und der vereinbarten Leistungen erfolgt durch das Trust Center der T-Systems eine Archivierung des privaten Schlüssels. Informationen zur Sicherung von privaten Endteilnehmerschlüsseln sind in den Kapiteln 4.12 ff und 6.2.3 beschrieben.

Die Wiederherstellung des Schlüsselmaterials von Endteilnehmern ist erlaubt,

- sofern der Endteilnehmer bzw. Schlüsselverantwortliche der Wiederherstellung zustimmt.
- soweit es sich um eine automatische Schlüsselwiederherstellung im Rahmen der Ausstellung einer neuen Smartcard (myCard) oder
- es sich um die Bereitstellung des Schlüsselmaterials für das Enterprise Mobility Managements (EMM) handelt

Liegt diese Erlaubnis nicht vor, darf der Auftraggeber dennoch die Wiederherstellung durchführen lassen, wenn rechtliche Gründe vorliegen wie

- Anforderungen in einem gerichtlichen oder behördlichen Verfahren,
- im Rahmen polizeilicher Ermittlungen,
- gesetzliche oder staatliche Vorschriften,
- Organisationsrichtlinien der DTAG
- durch eine autorisierte Stelle der DTAG unter Beachtung gesetzlicher Auflagen des Datenschutzes (DSGVO) und der Rahmenbedingungen des Betriebsverfassungsgesetzes (BetrVG) angefordert wurde.

6.2.4.1 Sicherung und Wiederherstellung des Verschlüsselungsschlüssels durch Enrollment-Software

Die PSE zum aktuellen Verschlüsselungszertifikat sowie vorhandener Key-Historien-Zertifikate wird bei der Personalisierung der MyCard durch Verwendung geeigneter Enrollment-Software gesichert auf die MyCard übertragen.

6.2.4.2 Sicherung und Wiederherstellung von Soft-PSE über das Betriebssystem

Die Schlüssel sind nicht exportierbar.

Die Soft-PSE ist mit einem Sitzungsschlüssel verschlüsselt gespeichert und per Passwort gesichert. Zur Nutzung der Soft-PSE bedarf es der Eingabe des Passworts.

6.2.4.3 Sicherung und Wiederherstellung von Soft-PSE durch das Trust Center

Bei der zentralen Schlüsselsicherung durch das T-Systems Trust Center sind die passwortgeschützte Soft-PSE und die korrespondierende Passwortdatei (enthält das Passwort der Soft-PSE) getrennt verschlüsselt gespeichert. Zur Wiederherstellung werden zwei getrennte Rollen benötigt.

6.2.5 Archivierung privater Schlüssel

Im Falle der Überschreitung des Gültigkeitszeitraums der Zertifikate der Zwischenzertifizierungsstelle (Sub-CA) oder des OCSP-Service wird das Schlüsselmaterial des jeweiligen Zertifikates vernichtet. Eine Archivierung findet nicht statt.

Das Trust Center der T-Systems archiviert Kopien von privaten Schlüsseln von Endteilnehmern,

- die im Rahmen einer Smartcard-Personalisierung von Triple-Key-Zertifikaten als Verschlüsselungsschlüssel durch das CA-System generiert wurden und in Verbindung mit der zentralen Schlüsselsicherung (Key-Back-Up) zu einem späteren Zeitpunkt abrufbar sein sollen,

6.2.6 Übertragung privater Schlüssel in oder von einem kryptographischen Modul

Das Schlüsselmaterial für ein Zertifikat einer Zwischenzertifizierungsstelle (Sub-CA) wird auf einem kryptografischen Hardware-Modul (HSM) im Online-Betrieb generiert. Der zu zertifizierende öffentliche Schlüssel, mit den Daten des Subject-DN, wird in elektronischer Form (PKCS#10-Request) auf sicherem Wege auf die Offline-CA übertragen, die das Sub-CA-Zertifikat generiert. Anschließend wird das Sub-CA-Zertifikat auf sicherem Wege auf das Hardware-Modul (HSM) übertragen und dem privaten Schlüssel zugeordnet. Die Übertragung des Schlüsselmaterials und dem zugehörigem Sub-CA-Zertifikat zwischen den Hardware-Modulen (HSM) im Online-Betrieb erfolgt in verschlüsselter Form.

Bei einer Erneuerung eines Zertifikats einer Zwischenzertifizierungsstelle (Sub-CA) wird das Schlüsselpaar beibehalten, bei betrieblichen oder sicherheitsrelevanten Erfordernissen kann jedoch auf dem angebundenen HSM ein neues Schlüsselpaar generiert und dort sicher gespeichert werden. Der zu zertifizierende öffentliche Schlüssel, mit den Daten des Subject-DN, wird in elektronischer Form (PKCS#10-Request) auf sicherem Wege auf die Offline-CA übertragen, die das Sub-CA-Zertifikat generiert. Anschließend wird das Sub-CA-Zertifikat auf sicherem Wege auf das Hardware-Modul (HSM) übertragen und dem privaten Schlüssel zugeordnet.

Smartcards, auf denen bereits Schlüssel aufgebracht sind oder die selbst Schlüssel generieren, ist ein Export privater Schlüssel nicht möglich. Im Rahmen einer Schlüsselsicherung kann lediglich das Schlüsselmaterial des Verschlüsselungszertifikats in die Karte importiert werden.

6.2.7 Speicherung privater Schlüssel auf kryptographischen Modulen

Das T-Systems Trust Center speichert CA-Schlüssel in sicherer Form auf kryptografischen Hardware-Modulen (HSM), welche nach FIPS 140-2/Level 3 evaluiert sind.

Smartcards (MyCards) speichern extern erzeugte Schlüssel oder selbst generierte Schlüssel in sicherer Form.

6.2.8 Methode zur Aktivierung privater Schlüssel

Alle Endteilnehmer (inkl. Registratoren) und Schlüsselverantwortliche müssen die Aktivierungsdaten (z.B. PIN, Importpasswort) für ihren bzw. anvertrauten privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß der vorliegenden CP/CPS schützen.

Der private Schlüssel des Zertifikats einer Zwischenzertifizierungsstelle (Sub-CA) bleibt aktiv bis der Gültigkeitszeitraum überschritten wurde oder ein Sperrgrund vorliegt, der die Zertifikatssperrung auslöst.

6.2.8.1 Private Schlüssel von Endteilnehmer

Der Endteilnehmer hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer ähnlichen Sicherheitsmaßnahme, um den Endteilnehmer vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann auch z.B. ein Passwort zum Betrieb des privaten Schlüssels, beinhalten. Die vorherige Bestimmung gilt nicht für Geräte-Zertifikate.
- Es werden wirtschaftlich angemessene Maßnahmen zum physikalischen Schutz des PC-Arbeitsplatzes oder Geräts ergriffen, um die Nutzung dieses Platzes/Geräts in Verbindung mit der Nutzung des zugehörigen privaten Schlüssels ohne Genehmigung des Endteilnehmers oder einer autorisierten Person zuverlässig zu verhindern.

Wenn Endteilnehmer-Zertifikate mit ihren zugehörigen privaten Schlüsseln deaktivieret (abgelaufen, gesperrt) sind, dürfen sie nur in verschlüsselter Form und/oder mit Passwort- bzw. PIN-Schutz aufbewahrt werden.

6.2.8.2 Private Schlüssel von -Registratoren

Nicht anwendbar, da für Registratoren kein gesondertes Schlüsselmaterial ausgestellt wird, es erfolgt die Nutzung der für Endteilnehmer ausgestellten Schlüssel und Zertifikate. Die Zuordnung der Rollen findet im LifeCycle Management der cPKI statt.

6.2.8.3 Private Schlüssel von Stamm- und Zwischenzertifizierungsstellen

Schlüsselmaterial für CA- und Root-CA-Zertifikate wird entsprechend durch die autorisierten Personen aktiviert und auf kryptographischen Hardware-Modulen (HSM) aufgebracht (Kapitel 6.2.2 und 6.4.1).

Der zum CA-Zertifikat gehörende private Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt (Kapitel 4.9.3).

Der zum Root-CA-Zertifikat gehörende private Schlüssel wird nur zur Erzeugung von weiteren CA-Zertifikaten aktiviert. Nach Ablauf des Root-CA-Zertifikats wird der private Schlüssel nicht mehr genutzt

Wenn Zertifikate mit ihren zugehörigen privaten Schlüsseln deaktiviert (gesperrt, abgelaufen) werden, dürfen sie nur in verschlüsselter Form und/oder mit Passwort- bzw. PIN-Schutz aufbewahrt werden.

6.2.8.4 Private Schlüssel von Trust-Center-Administratoren und -Operatoren

Nicht anwendbar, da für Trust-Center-Administratoren und -Operatoren kein gesondertes Schlüsselmaterial ausgestellt wird, es erfolgt die Nutzung der für Endteilnehmer ausgestellten Schlüssel und Zertifikate.

Der Trust-Center-Administrator oder -Operator hat zum Schutz des privaten Schlüssels Ergreifung geeigneter Maßnahmen zum physischem Schutz des Administrator- oder Operator-Arbeitsplatzes vor unberechtigtem Zugriff.

6.2.9 Methode zur Deaktivierung privater Schlüssel

Die Deaktivierung von CA- und Root-CA-Schlüsseln erfolgt ereignisbezogen und obliegt dem Personal des Trust Centers der T-Systems.

Die Deaktivierung von privaten Endteilnehmer Schlüsseln obliegt dem Endteilnehmer.

Eine Deaktivierung von privaten Schlüsseln, die im Rahmen einer zentralen Schlüsselsicherung (Key-Back-Up) erstellt wurden, bedarf einer einzelvertraglichen Regelung.

6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von CA-Schlüsseln erfordert die Teilnahme mehrerer vertrauenswürdiger Personen (Trusted Roles) des Trust Centers. Dabei ist sicherzustellen, dass nach Vernichtung keine Fragmente des Schlüssels übrigbleiben, die zu einer Rekonstruktion des Schlüssels führen könnte.

T-Systems verwendet zur sicheren Schlüsselvernichtung eine integrierte Löschfunktion des HSM.

Die Vernichtung von privaten Schlüsseln der Endteilnehmer obliegt diesen bzw. dem Endteilnehmer selbst.

6.2.11 Bewertung kryptographischer Module

Siehe 6.2.1

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Im Rahmen der regelmäßigen Sicherungs- und Archivierungsmaßnahmen von T-Systems werden die Zertifikate CA-, Root-CA-, Endteilnehmer-Zertifikate) gesichert und archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Zertifikatsgültigkeit beginnt mit der Generierung des Zertifikats und endet mit Ablauf des Gültigkeitszeitraums oder durch Sperrung. Die Gültigkeitsdauer von Schlüsselpaaren entspricht der Gültigkeitsdauer des zugehörigen Zertifikats. Die Zertifikate können jedoch weiterhin zur Entschlüsselung und Signaturvalidierung verwendet werden, sofern der dazu passende private Schlüssel vorliegt.

In Tabelle 16 sind die maximalen Gültigkeitszeiträume der in der Hierarchie beteiligten Zertifikate dargestellt, die zum Zeitpunkt des Inkrafttretens dieser CP/CPS ausgestellt wurden.

T-Systems stellt sicher, dass die CA- und Root-CA-Zertifikate vor Ablauf ausgewechselt werden, um die entsprechende Zertifikatsgültigkeit von Endteilnehmer-Zertifikaten gewährleisten zu können.

Zertifikatstyp	Gültigkeitsdauer
T-TeleSec GlobalRoot Class 2 (öffentliche Root-CA)	25 Jahre
Deutsche Telekom AG Issuing CA 01	8 Jahre
Deutsche Telekom AG secure email CA	10 Jahre
Deutsche Telekom Internal Root CA 1 (interne Root-CA)	20 Jahre
Deutsche Telekom Internal Root CA 2 (interne Root-CA)	20 Jahre
Deutsche Telekom AG Issuing CA 01	8 Jahre
Deutsche Telekom AG Issuing CA 02	8 Jahre
Deutsche Telekom AG Issuing CA 03	16 Jahre
Deutsche Telekom AG mobile device CA	10 Jahre
Endteilnehmer-Zertifikate:	standardmäßig 12 oder 36 Monate (bzw. 1 oder 3 Jahre)
Deutsche Telekom AG Employee Encryption	3 Jahre
Deutsche Telekom AG Employee Signature	3 Jahre
Deutsche Telekom AG Employee Authentication	3 Jahre
Deutsche Telekom AG External Workforce Encryption	1 Jahre
Deutsche Telekom AG External Workforce Signature	1 Jahre
Deutsche Telekom AG External Workforce Authentication	1 Jahre
Geräte-Zertifikate:	Standardmäßig 24, 36 oder 72 Monate (bzw. 2, 3 oder 6 Jahre), nach Vereinbarung kann eine abweichende Laufzeit administriert werden
CodeSigning-Zertifikate	3 Jahre
OCSP-Signing-Zertifikate	6 Monate

Tabelle 16: Gültigkeitszeiträume von Zertifikaten

6.4 Aktivierungsdaten

Zertifikate von Zertifikatsinhabern (Endteilnehmern)

Die Aktivierung von Zertifikaten ist grundsätzlich verknüpft mit Wissen (One Time Secret und/oder PIN) und dem Besitz eines Schlüsselträgermediums (Smartcard oder Software-PSE).

6.4.1 Generierung und Installation von Aktivierungsdaten

6.4.1.1 T-Systems

Um die auf dem HSM hinterlegten privaten Schlüssel der CA- und Root-CA-Zertifikate schützen zu können, werden Aktivierungsdaten (Geheimnisanteile) nach dem in Kapitel 6.2.2 dieser CP/CPS beschriebenen Anforderungen und dem Dokument „Key Ceremony“ generiert. Die Erstellung und Verteilung von Geheimnisanteilen wird protokolliert.

6.4.1.2 Endteilnehmer

Bei Zertifikaten von Zertifikatsinhabern (Endteilnehmer) werden One Time Secrets von der PKI generiert und dem Teilnehmer an seine im Zertifikatsantrag hinterlegte Emailadresse gesendet.

Die Vergabe einer PIN (MyCard oder Software-PSE) erfolgt bei der Aktivierung durch die jeweiligen Zertifikatsinhaber.

Abhängig von den Eingabemedien (z.B. PC-Tastatur, Tastatur eines Smartcard-Lesers) empfiehlt T-Systems zum Export von Soft-PSE oder Aktivierung/Nutzung des privaten Schlüssels die Vergabe von sicheren Passwörtern oder Kennphrasen, die folgender Syntax entsprechen:

- Zeichenlänge von mindestens 8 alphanumerischen Ziffern und Zeichen inkl. Sonderzeichen wie !, ?; /, usw.
- Groß- und Kleinschreibung,
- keine gängigen Bezeichnungen die in Lexika zu finden sind,
- keine Benutzernamen.

Für die Vergabe der Smartcard (MyCard) PIN ist folgende PIN Policy hinterlegt, ein abweichen davon wird durch die cPKI technisch verhindert.

- PIN Länge: 6
- Erlaubte Zeichen: 0-9
- Maximale Anzahl wiederholter Zeichen = 2
  Mit dieser Einstellung wird verhindert, dass PINs mit benachbarten, sich wiederholenden Zeichen verwendet werden.
  Beispiel: 111222 als PIN wird verhindert
- Maximale Anzahl sortierter Zeichen: = 3
  Mit dieser Einstellung wird verhindert, dass PINs mit benachbarten aufeinanderfolgenden oder sequentiellen/aufeinander folgenden Zeichen 1234567890 verhindert werden

6.4.2 Schutz der Aktivierungsdaten

6.4.2.1 T-Systems

Die Trust Center Administratoren bzw. von T-Systems autorisierte Personen verpflichten sich, die Geheimnisanteile für die Aktivierung der privaten Schlüssel der CA- und OCSP-Zertifikate zu schützen.

6.4.2.2 Endteilnehmer

Der Endteilnehmer verpflichtet sich die die Geheimnisanteile (OTP, PIN, Passwörter) für die Aktivierung der privaten Endteilnehmer Schlüssels zu schützen.

Zur Erhöhung der Sicherheit empfiehlt T-Systems eine regelmäßige Änderung der PIN für Endteilnehmer-Zertifikate.

Die Durchsetzung des Schutzes obliegt der Verantwortung des Auftraggebers.

6.4.3 Weitere Aspekte der Aktivierungsdaten

6.4.3.1 Übertragung von Aktivierungsdaten

Sofern Aktivierungsdaten für private Schlüssel, unabhängig vom Übertragungsmedium, übertragen werden, müssen die Trust-Center-Administratoren die Übertragung mithilfe von Methoden zum Schutz gegen Verlust, Diebstahl, Änderung, unbefugter Offenlegung oder Nutzung dieser privaten Schlüssel schützen.

Bei der Verwendung der Kombination von Benutzername und Passwort zur Anmeldung an Netzwerken als Aktivierungsdaten für einen Endteilnehmer, müssen die in einem Netzwerk zu übertragenen Kennwörter ebenfalls gegen den Zugriff durch unbefugte Benutzer geschützt werden.

6.4.3.2 Vernichtung von Aktivierungsdaten

Nach dem Löschen der privaten Schlüssel (Kapitel 6.2.10) sind die Aktivierungsdaten nicht mehr schützenswert.

6.5 Computer-Sicherheitskontrollen

T-Systems führt alle PKI-Funktionen mit Hilfe vertrauenswürdiger und geeigneter Systeme durch. Die Systeme werden von Monitoring-Systemen fortlaufend auf Funktion und Kapazität geprüft, so dass im Bedarfsfall zeitnah eine Erweiterung von Ressourcen durchgeführt werden kann. Die Sicherheitsmaßnahmen für Computer der Zertifizierungsstelle (z.B. Netzwerksicherheit, Zugriffskontrolle, Überwachung etc.) sind im Sicherheitsrahmenkonzept [SRK TC] beschrieben. Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.4 umgesetzt.

Die Systeme für Entwicklung, Test (cPKI CAST1 und CAST 2) und Produktion (cPKI-PROD) sind vollkommen getrennt voneinander aufgebaut, sie befinden sich auf unterschiedlicher Hardware in verschiedenen Netzsegmenten, so dass eine gegenseitige Beeinflussung ausgeschlossen ist.

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

T-Systems stellt sicher, dass die Verwaltung der CA-Systeme vor unbefugtem Zugriff Dritter gesichert ist. Die CA-Komponenten sind logisch von anderen Systemen getrennt und sind nur von autorisiertem Personal zugängig. Es werden aktuelle Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, Multifaktor Authentifizierung) eingesetzt, um die CA-Funktionalitäten, Verzeichnisdienste und OCSP-Responder vor internen und externen Eindringligen zu schützen. Die CA verwendet auf Netzwerksebene implementierte Intrusion Detection Systeme (IDS) und Intrusion-Prevention-Systeme (IPS), die unnormale oder unautorisierte Zugriffsversuche erkennen und alarmieren. Der direkte Zugriff auf CA-Datenbanken, die die CA-Funktionalitäten unterstützen, ist auf geeignetes, geschultes und vertrauenswürdiges Betriebspersonal beschränkt.

Die Sicherheitsmaßnamen umfassen

- Physikalische Sicherheit und Sicherung der Umgebung,
- Die CA-Systeme sind so konfiguriert, dass nicht benötigte Ports, Accounts, Anwendungen, Services und Protokolle entweder deaktiviert oder entfernt wurden,
- Maßnahmen zum Schutz der Systemintegrität, die mindestens aus Konfigurationsmanagement, Schutz von Sicherheitsanwendungen und Malware-Erkennung und -verhinderung bestehen,

- Netzwerksicherheit und Firewall Management, inklusive Portsperren und IP Adressfilterung, als auch Intrusion Detection System (IDS) und Intrusion-Prevention-Systeme (IPS),
- Benutzerverwaltung, Berechtigungsmatrix, Aufklärung, Sensibilisierung und Schulung/Ausbildung sowie
- Verfahrenskontrollen, Aktivitätsprotokollierung und Abschaltung bei Timeouts.

Auf den Systemen des Trust Centers werden Betriebssysteme eingesetzt, die die Durchsetzung von Sicherheitseinstellungen unterstützen. Keines der Systeme kann ohne Benutzeranmeldung verwendet werden.

Sicherheitskritische Einstellungen werden nur im 4-Augen-Prinzip verändert. Die Durchsetzung der Zugangsbeschränkungen an den Systemen wird durch die umgesetzte restriktive Password Policy unterstützt.

Besonders sicherheitskritische Applikationen (beispielweise die Zertifikatsgenerierung) erfordern zusätzliche Authentisierungen des Bedieners im Trust Center.

PC-Arbeitsplätze, an denen die Ausstellung von Zertifikaten autorisiert wird, werden durch Multi-Faktor-Authentisierung abgesichert.

Der TSP lässt einen Penetrationstest (PEN-Test) an den TSP-Systemen durchführen

- bei der Einrichtung,
- umfangreichen Upgrades oder Änderungen der Infrastruktur oder der Anwendungen,
- mindestens aber ein Mal pro Jahr,

die der TSP als wesentlich erachtet.

Der TSP erbringt den Nachweis, dass jeder Penetrationstest von einer Person oder Organisation durchgeführt wurde, die über die erforderlichen Fähigkeiten, Werkzeuge, Kenntnisse, ethischen Grundsätze und Unabhängigkeit verfügt, um einen zuverlässigen Bericht erstellen zu können.

6.5.2 Bewertung der Computersicherheit

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

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Systementwicklungskontrollen

T-Systems hat Mechanismen und Kontrollen implementiert, um eingekaufte, entwickelte oder veränderte Software auf Schadelemente oder bösartigen Code (z.B. Trojaner, Viren) überwachen und schützen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Neue Software-Versionen der Software (geplante Updates) oder Fehlerbeseitigungen (kurzfristige Bugfixes) werden zunächst auf einem Entwicklungssystem des Herstellers/Entwicklers bereitgestellt und getestet.

Nach erfolgreicher Prüfung der Software in der Entwicklungsumgebung wird eine Software-Package des Herstellers erzeugt, das auf einem Testsystem (Test-Umgebung, Test Unit) im Netz bzw. Lokation der T-Systems befindet (cPKI CAST1 oder cPKI CAST2).

Erst nach erfolgreichen Tests und Abnahme auf dem Testsystem erfolgt die Installation auf dem Wirksystem (cPKI-PROD) der T-Systems im georedundanten Rechenzentrum der T-Systems.

Das bei der T-Systems etablierte Change- und Release-Management findet Anwendung.

Die Verwaltung der PKI-Systeme (CA, HSM, Web-Server, ...) durch die Trust-Center-Administratoren (Systemadministratoren) erfolgt über ein getrenntes Netz das ausschließlich diesen Rolleninhabern zur Verfügung steht [Siko cPKI]. Die Verwaltung anderer IT-Systeme (nicht PKI-Systems) über dieses Netz ist unzulässig.

6.6.2 Sicherheitsverwaltungskontrollen

T-Systems hat Mechanismen und/oder Richtlinien implementiert, um die Konfiguration der PKI-Systeme im Trust Center kontrollieren und überwachen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Die Systemkonten (System Accounts) der Trust-Center-Administratoren werden spätestens nach 90 Kalendertagen überprüft. Nicht mehr benötigte Accounts werden deaktiviert.

6.6.3 Sicherheitskontrollen des Lebenszyklus

T-Systems hat Mechanismen und Kontrollen implementiert, dass Sicherheitspatchs innerhalb einer angemessenen Zeit, nachdem sie verfügbar sind, installiert werden. Die Integrität des Sicherheitspatchs wird vor der Installation manuell verifiziert.

Ein Sicherheitspatch wird nicht installiert, wenn zusätzliche Sicherheitslücken oder Instabilitäten entstehen, die die Vorteile der Anwendung des Sicherheitspatchs überwiegen. Der Grund für die Nichtanwendung von Sicherheitspatchs wird dokumentiert.

6.7 Netzwerk-Sicherheitskontrollen

Folgende Netzwerk-Sicherheitsmaßnahmen wurden implementiert:

- Die Netzwerke des Zertifizierungsdienstes sind durch Firewalls abgesichert und in verschiedene Sicherheitszonen eingestuft.
- Sicherheitskritische Komponenten und Systeme, die vom Internet aus erreichbar sind (z.B. Verzeichnisdienst, OCSP-Responder) werden durch Firewalls von Internet und den internen Netzen getrennt. Alle anderen sicherheitskritischen Komponenten und Systeme (z.B. CA, DB, Signer) befinden sich in einem separaten Netzen oder, im Falle der Offline-CA, ohne jegliche Netzanbindung.
- Die internen Netzwerke des Zertifizierungsdienstes sind nach dem Schutzbedarf der Systeme und Komponenten aufgeteilt und untereinander durch Firewalls getrennt.
- Ein Zugriff aus dem Internet erfolgt nur auf die Verzeichnisdienste, OCSP-Responder, CRL, des Weiteren sind auf einer separaten Webseite Informationen zur cPKI und das CP/CPS hinterlegt und aus dem Internet erreichbar. Zugriffe aus dem Internet auf CAs, dem Zertifikatsmanagement oder den Registration Authoritys ist nicht möglich.
- In regelmäßigen Abständen werden Schwachstellenüberprüfungen durchgeführt. Weitere Details sind in Kapitel 5.4.8 beschrieben.
- Alle berechtigten Nutzer müssen sich gegenüber den Systemen mit festgelegten Mechanismen authentifizieren, nicht mehr benötigte Accounts werden umgehend gelöscht oder deaktiviert.
  - Das Management von Benutzerzugriffsrechten erfolgt für alle Nutzer über ein Rollen und Rechte Konzept.
  - Für die Endteilnehmer wird mittels des ersten Auftrages über den automatischen Registrierungsplatz ein Account in Zertifikats LifeCycle Management der cPKI angelegt, Endteilnehmer müssen sich an diesem Account mittels ihres Active Directory Acoounts, mittels zwei Faktor Authentifizierung am Web-Portal der cPKI authentifizieren
  - Eine Ausstellung von Zertifikaten ist nur möglich, wenn vorher ein Auftrag über die RA für den Endteilnehmer eingestellt und als gültig verifiziert wurde.
  - Administratoren und Support Mitarbeiter müssen sich immer mittels 2 Faktor-Authentifizierung (Smartcard mit gültigem Authentifizierungszertifikat) anmelden und bekommen je nach Ihrer Rolle Ihre Rechte zugewiesen.
  - Service Accounts werden in einem Passwort Safe hinterlegt und sind nur Administratoren mit den entsprechenden Rollen mittels Smartcard Authentifizierung zugänglich.

- Es finden regelmäßige Prüfungen statt, ob Administrative oder Service Accounts noch benötigt werden. Werden Accounts identifiziert, die nicht mehr benötigt werden, werden diese umgehend gelöscht, deaktiviert oder den Benutzern die Rechte entzogen.

- Das Trust Center ist georedundant über getrennte Zuführungen sowohl mit der cPKI-Infrastruktur als auch mit dem Intranet verbunden. Ein Übergang von der cPKI-Infrastruktur ins Internet oder umgekehrt wird durch mehrere Firewallsysteme verhindert. Gleiches gilt für Übergänge ins Internet zur Bereitstellung der Verzeichnisdienste und Repositories

Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.8 umgesetzt.

6.8 Zeitstempel

Zertifikate, Sperrlisten, Online-Statusprüfungen und andere wichtige Informationen enthalten Datums- und Zeitinformationen, die aus einer zuverlässigen Zeitquelle abgeleitet werden (siehe Kapitel 5.5.5). Ein kryptografischer Zeitstempel wird nicht verwendet.

7 ZERTIFIKATS-, SPERRLISTEN-, UND OCSP PROFILE

7.1 Zertifikatsprofile

Die Zertifikatsbeantragung (siehe Kapitel 4.1 ff) erfolgt, abhängig vom Registrierungsmodell (Kapitel 4.2), in elektronischer Form über technische Schnittstellen.

Bedingt durch das Beantragungsverfahren bzw. die Schnittstelle wird ein Zertifikatsantrag bereits einem entsprechenden Zertifikatsprofil (z.B. Benutzer, Extern, Intern, Server) zugeordnet. In Tabelle 17 sind die von cPKI angebotenen Zertifikatstypen den jeweiligen Zertifikats-Templates zugeordnet.

Zertifikatstypen:	Zertifikats-Template:	Verwendung:
Benutzer	Single Key (nur Mobile Devices)	Sig
	Triple Key	Sig
		Enc
		LogOn
Gruppen-, Funktions-, Rollenzertifikate	Single Key	Sig/Enc
Server	Single Key	Sig/Enc
Router/Gateway	Single Key	Sig/Enc
Mail-Gateway	Single Key	Sig/Enc
Domain-Controller	Single Key	Sig/Enc
Computer Zertifikate 802.1x	Single Key	Client Authentication
Mobile Device Client Auth.	Single Key	Client Authentication
Code Signing	Single Key	Code Sig
OCSP	Single Key	Sig/Enc

Tabelle 17: Zuordnung Zertifikatsprofile und Templates

Ein Zertifikatsantrag (Request), der aus einem Gerät oder einer Anwendung stammt, wird auf definierte Inhalte des Subject-DN (siehe Kapitel 3.1.1 ff) und Verwendung unerlaubter Zeichen überprüft. Es gilt die Ausprägung des jeweiligen Zertifikatsprofils wie in Kapitel 7.1 ff beschrieben. Die Verwendung von unerlaubten Zeichen wird mit der Überprüfung wird bei der manuellen Registration angezeigt oder dem Antragsteller mitgeteilt. Bei Zertifikatsanträge über die automatische Registrierungsstelle, werden die Aufträge mit einer Fehlermeldung (Notifikation) zurückgewiesen.

Die von T-Systems ausgestellten Zertifikate entsprechen folgenden Anforderungen:

- [RFC 5280]
- [X.509]
- [CAB-BR]
- [ETSI 319411-1 Policy LCP]

Die ausgestellten X.509.v3-Zertifikate weisen mindestens die in Tabelle 18 aufgeführten Inhalte auf.

Feld	Wert oder Wertbeschränkung:
Version:	Zertifikatsversion (Kapitel 7.1.1)
Zertifikats-Seriennummer:	Eindeutiger Wert zur Identifikation des Zertifikats

Feld	Wert oder Wertbeschränkung:
Signaturalgorithmus:	RSA – SHA-256[3]
Aussteller:	Zertifizierungsstelle (Kapitel 1.3.1.2.1 und 1.3.1.2.2
Gültig ab:	Zeitbasis koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Gültig bis:	Zeitbasis koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Antragsteller:	Eindeutiger Name (Kapitel7.1.4); Benutzer-Zertifikate: 3.1.1.1.16
Öffentlicher Schlüssel:	Gemäß RFC 5280 kodiert
Erweiterungen:	
Schlüsselverwendung:	Kapitel 7.1.2.1
Zertifizierungsrichtlinie:	Kapitel 7.1.2.2
Alternativer Antragstellername	Kapitel 7.1.2.3
Basiseinschränkungen	Kapitel 7.1.2.4
Erweiterte Schlüsselverwendung:	Kapitel 7.1.2.5
Sperrlistenverteilungspunkt	Kapitel 7.1.2.6
Schlüsselkennung des Antragstellers:	Kapitel 7.1.2.7
Stellenschlüsselkennung:	Kapitel 7.1.2.8
Zugriff auf Stelleninformation	Kapitel 7.1.2.9
Zertifikatsvorlagename	Kapitel 7.1.2.10

Tabelle 18: Zertifikatsattribute nach X509.v3

Zusätzliche Erweiterungen und Eigenschaften werden in den folgenden Kapiteln ausführlicher erklärt.

7.1.1 Versionsnummern

Die von der cPKI der DTAG ausgestellten X.509-Zertifikate für Endteilnehmer entsprechen der z. Zt aktuellen Version 3. Die zusätzlichen Erweiterungen und Eigenschaften werden in den folgenden Kapiteln ausführlicher beschrieben.

Die CA- und Root-CA-Zertifikate sind ebenfalls vom Typ X.509v3.

7.1.2 Zertifikatserweiterungen

Um dem Standard X.509v3 zu erfüllen, ergänzt T-Systems das Zertifikatsprofil um entsprechende Erweiterungen, die in den Kapiteln 7.1.2.1 bis 7.1.2.10 beschrieben sind.

7.1.2.1 Schlüsselverwendung (KeyUsage)

Die Schlüsselverwendung richtet sich nach den Regeln des RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” und ist darin beschrieben.

In Tabelle 19 bis Tabelle 21 ist die Erweiterung „Schlüsselverwendung“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Geräte Zertifikate							
	Zertifikatsprofil:	**Server**	**Router / Gateway**	**Mail-Gateway**	**Domain-Controller**	**Mobile Devices**	**Computer**

[3] Alternativ RSA - SHA-1

Geräte Zertifikate

	Risikowert (Criticality)	critical	critical	critical	critical	critical	critical
Bit	Bezeichnung	Sig/Enc	Sig/Enc	Sig/Enc	Sig/Enc	Client Auth.	Client Auth.
0	digitalSignature	✓	✓	✓	✓	✓	✓
1	nonRepudiation	×	×	×	×	×	×
2	keyEncipherment	✓	✓	✓	✓	✓	✓
3	dataEncipherment	×	×	×	✓	×	×
4	keyAgreement	×	×	×	×	×	×
5	keyCertSign	×	×	×	×	×	×
6	CRLSign	×	×	×	×	×	×
7	encipherOnly	×	×	×	×	×	×
8	decipherOnly	×	×	×	×	×	×
	Wert (Hex)	A0	A0	A0	B0	A0	A0

Tabelle 19: Zuordnung der Erweiterung „Schlüsselverwendung“ (Key Usage), Teil 1

Benutzer-Zertifikate:

		Single-Key FMB/GRP	**Single-Key Mobile Device**	**Triple-Key**		
	Risikowert (Criticality)	critical	critical	critical	critical	critical
Bit	Bezeichnung	Sig/Enc	Sig	Sig	Enc	LogOn
0	digitalSignature	✓	✓	✓	×	✓
1	nonRepudiation	×	×	×	×	×
2	keyEncipherment	✓	×	×	✓	×
3	dataEncipherment	✓	×	×	✓	×
4	keyAgreement	×	×	×	×	×
5	keyCertSign	×	×	×	×	×
6	CRLSign	×	×	×	×	×
7	encipherOnly	×	×	×	×	×
8	decipherOnly	×	×	×	×	×
	Wert (Hex)	B0	80	80	30	80

Tabelle 20: Zuordnung der Erweiterung „Schlüsselverwendung“ (Key Usage), Teil 2

CA-Zertifikate

	Zertifikatsprofil:	Sub-CA	Root-CA
	Risikowert (Criticality)	critical	critical
Bit	Bezeichnung	Cert/CRL	Cert/CRL
0	digitalSignature	✓	×
1	nonRepudiation	×	×
2	keyEncipherment	×	×
3	dataEncipherment	×	×
4	keyAgreement	×	×
5	keyCertSign	✓	✓
6	CRLSign	✓	✓
7	encipherOnly	×	×
8	decipherOnly	×	×
	Wert (Hex)	86	06

Tabelle 21: Zuordnung der Erweiterung „Schlüsselverwendung“ (Key Usage), Teil 3

Auf Kundenwunsch kann das Zertifikatsprofil (außer für CA-Zertifikate) mit der Erweiterung „Schlüsselverwendung“ um weitere Werte aus og. Tabelle ergänzt werden.

Im Falle, dass die Schlüsselverwendung als „unkritisch“ deklariert ist, besteht eine erweiterte Schlüsselverwendung (Extended Key Usage), die „kritisch“ markiert ist.

Obwohl das nonRepudiation-Bit in der Erweiterung „Schlüsselverwendung“ nicht gesetzt ist, unterstützt T-Systems dennoch die Nichtabstreitbarkeit für diese „fortgeschrittenen“ Signatur-Zertifikate. Es ist z. Zt. nicht unbedingt erforderlich, das nonRepudiation-Bit in diesem Zertifikatstyp zu setzen, da die PKI-Industrie noch keinen Konsens darüber erzielt hat, welche Bedeutung das nonRepudiation-Bit tatsächlich hat. Bis ein solcher Konsens erzielt wird, hat das nonRepudiation-Bit für potenzielle vertrauende Dritte keine Bedeutung.

Darüber hinaus werten die gängigsten Anwendungen (z.B. E-Mail) das nonRepudiation-Bit nicht. Aus diesem Grunde ist eine Definition des Bits für vertrauende Dritte bei der Entscheidung über die Vertrauenswürdigkeit nicht hilfreich.

7.1.2.2 Erweiterung „Zertifizierungsrichtlinien (Certificate Policies)”

Die Erweiterung „Zertifizierungsrichtlinie“ besteht aus Objekt-Kennungen (Object Identifier, OID, siehe auch Kapitel 7.1.6) und einer URL, hinter der diese CP/CPS abrufbar ist. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.3 Erweiterung „alternativer Antragstellername (subjectAltName)”

In Tabelle 22 ist die Erweiterung „alternativer Antragstellernamen“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Zertifikatsprofile

	Benutzer-Zertifikat:		Server-Zertifikat:	Router / Gateway-Zertifikat:	Mail-Gateway-Zertifikat:	Domain-Controller-Zertifikat:	Computer Zertifikat
Erweiterung:	SK FMB	TK					
RFC822-Name	✓	✓	×	✓	✓	✓	×
Principalname	✓	✓	×	×	×	×	×

Zertifikatsprofile							
DNS-Name	×	×	✓	×	×	✓	✓
IP-Address	×	×	×	✓	×	×	×
Other Name (DS-Objekt-Guid)	×	×	×	×	×	✓	×

Tabelle 22: Zuordnung der Erweiterung „alternativer Antragstellername (subjectAltName)“

Für Mobile Device Benutzer Signatur und Mobile Device Client Auth. werden keine alternativen Antragstellernamen benutzt.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.4 Erweiterung „Basiseinschränkungen (BasicConstraints)”

Die Erweiterung „Basiseinschränkung“ definiert folgende Inhalte

- Benutzertyp (subjectTyp) und
- Beschränkung des Zertifizierungspfades (pathLenConstraint)

Der Benutzertyp gibt an, ob das ausgestellt Zertifikat für einen Endteilnehmer (CA = false) oder Zertifizierungsstellen (CA) bestimmt ist.

Die Einschränkung des Zertifizierungspfads gibt an, wie viele Zertifizierungsstellen in der Zertifikatshierarchie höchstens vorkommen dürfen.

In Tabelle 23 sind die von der cPKI genutzten Root- und Sub-CA-Zertifikate dargestellt. Die cPKI stellt kein weiteres Sub-CA-Zertifikat aus, das hierarchisch einer der dargestellten Sub-CAs untersteht.

Basic Constraints Root- und Sub-CA-Zertifikate			
Name/Typ	**Risikowert (Critically)**	**Benutzertyp**	**Beschränkung des Zertifizierungstyps**
T-TeleSec GlobalRoot Class 2	critical	Zertifizierungsstelle	keine
Deutsche Telekom Root CA 2	non critical	Zertifizierungsstelle	5
Deutsche Telekom Internal Root CA 1	critical	Zertifizierungsstelle	1
Deutsche Telekom Internal Root CA 2	critical	Zertifizierungsstelle	keine
Deutsche Telekom AG secure email CA	critical	Zertifizierungsstelle	0
Deutsche Telekom AG Issuing CA 01	critical	Zertifizierungsstelle	0
Deutsche Telekom AG Issuing CA 02	critical	Zertifizierungsstelle	0
Deutsche Telekom AG Issuing CA 03	critical	Zertifizierungsstelle	0
Deutsche Telekom AG mobile device CA	critical	Zertifizierungsstelle	0
Endteilnehmer	non critical	Endeinheit	keine

Tabelle 23: Zuordnung der Erweiterung „Basiseinschränkungen“ (Basic Constraints)

7.1.2.5 Erweiterung „Erweiterte Schlüsselverwendung (ExtendedKeyUsage)”

In der nachfolgenden Tabelle ist die „Erweiterte Schlüsselverwendung“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Extended KeyUsage Benutzer-Zertifikate:

	Single-Key FMB/GRP	Single-Key Mobile Device	Single-Key Code Signing	Triple-Key		
Risikowert (Criticality)	**non critical**	**non critical**	**non critical**	**non critical**	**non critical**	**critical**
Bezeichnung	Sig/Enc	Sig	Sig	Sig	Enc	LogOn
Secure E-Mail (1.3.6.1.5.5.7.3.4)	✓	✓	×	✓	✓	×
Code Signing (1.3.6.1.5.5.7.3.3)	×	×	✓	×	×	×
Server authentication (1.3.6.1.5.5.7.3.1)	×	×	×	×	×	×
Timestamping (1.3.6.1.5.5.7.3.8)	×	×	×	×	×	×
Client authentication (1.3.6.1.5.5.7.3.2)	×	×	×	×	×	✓
OCSPSigning (1.3.6.1.5.5.7.3.9)	×	×	×	×	×	×
MS SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	×	×	×	×	×	✓

Tabelle 24: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung“ (Extended Key Usage) für Benutzer-Zertifikate

Extended KeyUsage Benutzer-Zertifikate:

	Server Authentication	Client Authentication	Code Signing	Secure E-Mail	Smartcard Logon
OID	1.3.6.1.5.5.7.3.1	1.3.6.1.5.5.7.3.2	1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4	1.3.6.1.4.1.311.20.2.2
DTAG Employee Encryption	×	×	×	✓	×
DTAG Employee Signature	×	×	×	✓	×
DTAG Employee Authentication	×	✓	×	×	✓
DTAG External Workforce Encryption	×	×	×	✓	×
DTAG External Workforce Signature	×	×	×	✓	×
DTAG External Workforce Authentication	×	✓	×	×	✓
DTAG Encryption für Pseudonyme	×	×	×	✓	×
DTAG Signature für Pseudonyme	×	×	×	✓	×
DTAG Authentication für Pseudonyme	×	✓	×	×	✓
DTAG Encryption für Gruppen und Funktionsaccounts	×	×	×	✓	×

Extended KeyUsage Benutzer-Zertifikate:

DTAG Signature für Gruppen und Funktionsaccounts	×	×	×	✓	×
DTAG Employee Signature Mobile Devices	×	×	×	✓	×
DTAG Code Signing	×	×	✓	×	×

Tabelle 25: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung" (Extended Key Usage) für Benutzer-Zertifikate,

Extended Key Usage Geräte-Zertifikate

Zertifikatsprofil:	**Server**	**Router / Gateway**	**Mail-Gateway**	**Domain-Controller**	**Mobile Device Client Auth.**	**Computer**
Risikowert (Criticality)	n.v.	n.v.	critical	critical	critical	critical
Secure E-Mail (1.3.6.1.5.5.7.3.4)	×	×	✓	×	×	×
Code Signing (1.3.6.1.5.5.7.3.3)	×	×	×	×	×	×
Server authentication (1.3.6.1.5.5.7.3.1)	✓	×	×	✓	×	✓
Timestamping (1.3.6.1.5.5.7.3.8)	×	×	×	×	×	×
Client authentication (1.3.6.1.5.5.7.3.2)	✓	×	×	✓	✓	✓
OCSPSigning (1.3.6.1.5.5.7.3.9)	×	×	×	×	×	×
MS SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	×	×	×	×	×	×

Tabelle 26: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung" (Extended Key Usage) für Geräte-Zertifikate

Extended Key Usage Geräte-Zertifikate

	Risikowert (Criticality)	Server Authentication	Client Authentication	Code Signing	Secure E-Mail	Smartcard Logon
OID		1.3.6.1.5.5.7.3.1	1.3.6.1.5.5.7.3.2	1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4	1.3.6.1.4.1.311.20.2.2
Server-Zertifikat	**n.v.**	✓	×	×	×	×
Router / Gateway-Zertifikat	**n.v.**	✓	×	×	×	×
Mail-Gateway-Zertifikat:	**critical**	×	×	×	✓	×

Extended Key Usage Geräte-Zertifikate						
Domain-Controller-Zertifikat:	**critical**	✓	✓	×	×	✓
Mobile Device Client Auth.	**critical**	×	✓	×	×	×
Computer Zertifikat	**critical**	✓	✓	×	×	×

Tabelle 27: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung“ (Extended Key Usage) für Geräte-Zertifikate

7.1.2.6 Erweiterung „Sperrlistenverteilungspunkt (CRLDistributionPoints)”

Alle Endteilnehmer-Zertifikate verfügen über einen Sperrlistenverteilungspunkt, über dessen URL (HTTP und LDAP) die aktuelle Zertifikatssperrliste (CRL) auf dem Verzeichnisdienst abrufbar ist. Vertrauende Dritte benötigen diese URL zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Das CA-Zertifikat verfügt ebenfalls über einen Sperrlistenverteilungspunkt, über dessen URL (HTTP und LDAP) die aktuelle Sperrliste für Zertifizierungsstellen (CARL) auf dem Verzeichnisdienst abrufbar ist. Vertrauende Dritte benötigen diese zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Die Root-CA-Zertifikate enthalten keinen Sperrlistenverteilungspunkt.

7.1.2.7 Erweiterung „Schlüsselkennung des Antragstellers (subjectKeyIdentifier)”

In allen Endteilnehmer-Zertifikaten enthält die Erweiterung „Schlüsselkennung des Antragstellers“ als Attributswert SHA-1 Hashwert, der individuell aus den jeweiligen öffentlichen Schlüssel gebildet wird.

Die Erweiterung „Schlüsselkennung des Antragstellers“ des von CA-Zertifikaten enthält als Attributswert einen SHA-1 Hashwert, der aus dem öffentlichen Schlüssel der jeweiligen CA gebildet wird. Dieser Wert stimmt mathematisch mit dem Wert der Erweiterung „Stellenschlüsselkennung“ (siehe Kapitel 7.1.2.8) des jeweiligen Endteilnehmer-Zertifikats überein.

Es gelten ebenfalls die Regelungen der jeweils hierarchisch übergeordneten Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.8 Erweiterung Stellenschlüsselkennung (authorityKeyIdentifier)”

In Endteilnehmer-Zertifikaten enthält die Erweiterung „Stellenschlüsselkennung“ als Attributswert einen SHA-1-Hashwert, der mit dem Wert der Erweiterung „Schlüsselkennung des Antragstellers“ des Zertifikats der hierarchisch übergeordneten Zertifizierungsinstanz (CA) mathematisch übereinstimmt.

Es gelten ebenfalls die Regelungen der jeweils hierarchisch übergeordneten Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.9 Erweiterung Zugriff auf Stelleninformation (Authority Information Access)

7.1.2.9.1 Endteilnehmer-Zertifikate

In Endteilnehmer-Zertifikat enthält die Erweiterung „Zugriff auf Stelleninformation“ die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch HTTP-URL des jeweiligen OCSP-Responders, siehe auch Kapitel 2.2 unter „Bereitstellung von Zertifikatsstatusdaten über das OCSP-Protokoll“

Zugriff auf Stelleninformation (AIA) in Endteilnehmer-Zertifikaten
Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1

Endteilnehmer-Zertifikat ausgestellt von CA	OCSP-Pfad	Anmerkungen
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocsp	(Endteilnehmer-Zertifikate bis 08.11.2016)
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocsp	(Endteilnehmer-Zertifikate bis 08.11.2016)
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocsp	(Endteilnehmer-Zertifikate vor dem 08.11.2016)
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocspr	(Endteilnehmer-Zertifikate 08.11.2016 bis 18.04.2018)
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocsp	(Endteilnehmer-Zertifikate vor dem 08.11.2016)
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocspr	(Endteilnehmer-Zertifikate ab 08.11.2016)
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocsp	(Endteilnehmer-Zertifikate bis 08.11.2016)
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocspr	(Endteilnehmer-Zertifikate ab 08.11.2016)
Deutsche Telekom AG mobile device CA:	http://ocsp-cpki.telekom.de/ocspr	(Endteilnehmer-Zertifikate ab 18.04.2018)
Deutsche Telekom AG secure email CA:	http://ocsp-cpki.telekom.de/ocspr	(Endteilnehmer-Zertifikate ab 18.04.2018)

Tabelle 28: Erweiterung Zugriff auf Stelleninformation (Authority Information Access) Teil 1

7.1.2.9.2 Sub-CA-Zertifikate

In Zertifikaten von Zwischenzertifizierungsstellen (Sub-CA) enthält die Erweiterung „Zugriff auf Stelleninformation“ die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch HTTP-URL des jeweiligen OCSP-Responders.

Zugriff auf Stelleninformation (AIA) in Zwischenzertifizierungsstellen-Zertifikaten
Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1

CA-Zertifikat	OCSP-Pfad
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocsp
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocsp
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocsp
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG mobile device CA:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG secure email CA:	http://ocsp-cpki.telekom.de/ocspr

Tabelle 29: Erweiterung Zugriff auf Stelleninformation (Authority Information Access) Teil 2

Die CA Zertifikate enthalten zusätzlich noch die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.2 mit den HTTPS und LDAP Pfadangaben des jeweiligen Root-CA-Zertifikats.

Zugriff auf Stelleninformation (AIA) in Root CA-Zertifikaten
Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.2

CA	http-Pfad	Ldap-Pfad
Deutsche Telekom AG Issuing CA 01:	http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
Deutsche Telekom AG Issuing CA 02	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority
Deutsche Telekom AG Issuing CA 03:	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority
Deutsche Telekom AG mobile device CA:	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority
Deutsche Telekom AG secure email CA:	http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate

Tabelle 30: Erweiterung Zugriff auf Stelleninformation (Authority Information Access) Teil 3

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.10 Erweiterung Zertifikatsvorlagenname (Certificate Template Name)

Für das Zertifikatsprofil „Domain-Controller“ ist die Erweiterung „Zertifikatsvorlagenamen“ belegt mit dem Namen „DomainController“.

7.1.3 Objekt-Kennungen von Algorithmen

Innerhalb des cPKI der DTAG stehen für das Signieren von Zertifikaten folgende Signatur-Algorithmen zur Verfügung:

- sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}, -> 1.2.840.113549.1.1.11
- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}, -> 1.2.840.113549.1.1.5

Diese Signatur-Algorithmen beziehen sich auf alle Zertifikatstypen (Stammzertifizierungsstelle, Zwischenzertifizierungsstelle und Endteilnehmer).

Aus Sicherheitsgründen müssen alle Endteilnehmer-Zertifikate und Zertifikate der Zwischenzertifizierungsstelle (Sub-CA) den Signatur-Hash-Algorithmus SHA-256 verwenden.

Der Signatur-Hash-Algorithmus SHA-1 wird aus Sicherheitsgründen nicht mehr empfohlen und ist in Zertifikaten, die von einer öffentlichen Sub-CA ausgestellt werden, nicht zugelassen.
SHA-1 ist ausschließlich nur aus Interoperabilitätsgründen in Zertifikaten erlaubt, die von einer internen Sub-CA ausgestellt werden.

7.1.4 Namensformen

Die Endteilnehmer-Zertifikate der „cPKI“ enthalten einen, eindeutigen Ausstellernamen (Issuer-DN) der jeweiligen Zertifizierungsstelle (Kapitel 1.3.1.2).

Die Inhalte des Subject-DN (Antragsteller) sind abhängig vom Zertifikatstyp (z.B. Benutzer, Server, Router/Gateway) und setzen sich wahlweise aus den Feldern wie in dem Kapitel 3.1.1.1 beschrieben zusammen. Die Felder enthalten Pflichtangaben (mandatory), optionale oder automatisch erzeugte Angaben.

Pflichtangaben bei Zertifikate für Personen,

- die aus dem Vertrauenswürdigen Verzeichnis (cIAM) übernommen werden enthalten folgende Felder:
  - Common Name (CN) = <Vorname Name>,
  - E-Mail-Address (E) = <primäre eMail aus dem AD>,
  - Given Name (G) = <Vorname>
  - Surname (SN) = <Nachname>
  - Organizational Unit Name (OU) = <Corporate ID (CID)>
  - Organizational Unit Name (OU) = Employee oder External Workforce
- die vom System automatisch erzeugt werden beinhalten folgende Felder:
  - Country Name (C)=DE
  - Organization Name (O) = DTAG oder Deutsche Telekom AG
  - Organizational Unit Name (OU) = Person

Pflichtangaben bei Zertifikate für Pseudonyme,

- die aus dem vertrauenswürdigen Verzeichnis (cIAM) übernommen werden enthalten folgende Felder:
  - Common Name (CN) = PN-<Vorname Name>,
  - E-Mail-Address (E) = <primäre eMail aus dem AD>,
  - Pseudonym (PN) = <Name des Pseudoyms>
  - Organizational Unit Name (OU) = <Corporate ID (CID)>

  - Organizational Unit Name (OU) = External Workforce
- die vom System automatisch erzeugt werden beinhalten folgende Felder:
  - Organization Name (O) = DTAG oder Deutsche Telekom AG
  - Organizational Unit Name (OU) = Person
  - Country Name (C) = (DE)

Pflichtangaben bei Zertifikate für Funktionsgruppen (FMB),

- die aus dem Active Directory (AD) der DTAG übernommen werden enthalten folgende Felder:
  - Common Name (CN) = <FMB-Bezeichnung>.<SAM Account Name>,
  - Organizational Unit Name OU = <Funktionsgruppe (FMB oder GRP)>
  - Organizational Unit Name OU = < Country Name (DE)>
  - Domain Controller DC = emea1
  - Domain Controller DC = cds
  - Domain Controller DC = t-internal
  - Domain Controller DC = com
  - Organizational Unit Name OU = Internal
  - Organizational Unit Name OU = Users
- die vom System automatisch erzeugt werden beinhalten folgende Felder:
  - Organization Name (O) = Deutsche Telekom AG
  - Country Name (C) = DE

Pflichtangaben bei Zertifikate für juristische Personen,

  - Common Name (CN) = <Name der juristischen Person>
  - E-Mail-Address (E) = <primäre eMail aus dem AD>,
  - organizationIdentifier = WEEE-Reg.-Nr. <Nummer>
- die vom System automatisch erzeugt werden beinhalten folgende Felder:
  - Organization Name (O) = Deutsche Telekom AG
  - Organizational Unit Name (OU) = Person
  - Country Name (C) = (DE)

Pflichtangaben bei Zertifikate für Geräte

- Computerzertifikat 802.1x
  - Common Name (CN) = Fully Qualified Domain Name, FQDN
- Server
  - Common Name (CN) = Fully Qualified Domain Name, FQDN
  - localityName (L) = <Stadt/Ort>
  - stateOrProvinceName (S) = <Bundesland/State/Province>
  - Organization Name (O) = <Firma/Organisation>
  - Country Name (C) = <Land>

Folgende Felder sind optional:

- Organizational Unit Name 3 (OU3)
- User Principal Name (UPN)
- Weitere E-Mail-Adressen und Server-Namen (Fully Qualified Domain Name, FQDN)

Die E-Mail-Adresse muss nicht zwingend Inhalt des Subject-DN sein, wenn sich diese in der Erweiterung „alternativer Antragstellername (subjectAltName) wiederfindet.

Sofern nicht alle Zertifikatsantragsdaten in den Subject-DN aufgenommen werden können, weil technische oder Interoperabilitätsbeschränkungen (z.B. Dateigröße des Zertifikats, nur ein OU-Eintrag) in Zertifikaten die Verwendung unmöglich machen, sind Abweichungen zu den vorangehenden Bestimmungen zulässig.

Die Inhalte des alternativeren Antragstellernamens (subjectAltName) sind ebenfalls abhängig vom Zertifikatstyp (z.B. Benutzer, Server, Router/Gateway) und setzen sich wahlweise wie folgt zusammen:

- User Principal Name (UPN)
- RFC822
- DNS-Name

Die ausgestellten Zertifikate enthalten in jedem Fall die Felder „Issuer Distinguished Name“ und „Subject Distinguished Name“:

Zertifikat	Issuer DN	Subject DN
Deutsche Telekom AG Employee Encryption	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>, CN =<Vorname Name> OU = <CID> OU = Employee OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG Employee Signature	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD> CN =<Vorname Name> OU = <CID> OU = Employee, OU = Person O = DTAG oder Deutsche Telkom AG C = DE

Zertifikat	Issuer DN	Subject DN
Deutsche Telekom AG Employee Authentication	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD> C CN =<Vorname Name> OU = <CID> OU = Employee OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG External Workforce Encryption	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>, CN =<Vorname Name> OU = <CID> OU = External Workforce, OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG External Workforce Signature	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>, CN =<Vorname Name> OU = <CID> OU = External Workforce, OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG External Workforce Authentication	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>, CN =<Vorname Name> OU = <CID> OU = External Workforce, OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG Encryption für Pseudonyme	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>, CN = PN-<Vorname Name>, OU = <CID> OU = External Workforce, OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG Signature für Pseudonyme	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>,, CN = PN-<Vorname Name>, OU = <CID> OU = External Workforce, OU = Person O = DTAG oder Deutsche Telkom AG C = DE
Deutsche Telekom AG Authentication für Pseudonyme	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>,, CN = PN-<Vorname Name>, OU = <CID> OU = External Workforce, OU = Person O = DTAG oder Deutsche Telkom AG C = DE

Zertifikat	Issuer DN	Subject DN
Deutsche Telekom AG Signatur und Encryption für Gruppen und Funktionsaccounts	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	CN = FMB-<Postfachname>.<SAM Account Name > OU = FMB OU = Internal OU = Users OU = DE DC = emea1 DC = cds DC = t-internal DC = com O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Signatur für Benutzer auf Mobile Devices	CN=<Zertifizierungsstelle>, OU = <Organistationseinheit>, O =<Organisation> C = <Land>	E = <primäre eMail aus AD>, CN =<Vorname Name>, OU = <CID> OU = Employee, OU = Mobile O = DTAG oder Deutsche Telekom AG C = DE

Tabelle 31: Issuer DN und Subject DN

Zusätzlich werden noch bei einigen Zertifikaten Einträge im „Subject Alternative Name“ vorgenommen:

Zertifikat	Other Name	Principal Name	RFC822 Name
Deutsche Telekom AG Employee Encryption	none	UPN	E-Mail-Adresse
Deutsche Telekom AG Employee Signature	none	UPN	E-Mail-Adresse
Deutsche Telekom AG Employee Authentication	none	UPN	E-Mail-Adresse
Deutsche Telekom AG External Workforce Encryption	none	UPN	E-Mail-Adresse
Deutsche Telekom AG External Workforce Signature	none	UPN	E-Mail-Adresse
Deutsche Telekom AG External Workforce Authentication	none	UPN	E-Mail-Adresse
Deutsche Telekom AG Signatur und Encryption für Gruppen und Funktionsaccounts	none	UPN	E-Mail-Adresse
Deutsche Telekom AG Signatur für Benutzer auf Mobile Devices	none	none	none
Deutsche Telekom AG Mobile Devices	none	none	none

Zertifikat	Other Name	Principal Name	RFC822 Name
Deutsche Telekom AG Telekom Computer	DNS	none	none
Deutsche Telekom AG Domain Controller	DNS	none	none

Tabelle 32: Einträge im Subject Alternative Name

7.1.5 Namensbeschränkungen

Es sind nur Namen/Domains zugelassen die von der DTAG verwaltet werden.

Dazu sind im Zertifikat der Deutsche Telekom AG secure email CA die zugelassenen Namen/Domains definiert und auf diese Namen/Domains beschränkt.

7.1.6 Objekt-Kennungen (OIDs) für Zertifizierungsrichtlinien

7.1.6.1 Objekt-Identifikatoren für Zertifizierungsrichtlinien der cPKI

Alle Endteilnehmer- und CA-Zertifikate enthalten eine Erweiterung „Zertifizierungsrichtlinie (certificate policies)“. Neben der HTTP-URL findet sich folgende Objekt-Kennung für die CP/CPS:

policy OBJECT IDENTIFIER ::= {iso(1) iso identified organization(3) us department of defence(6) oid assignments(1) private(4) iana registrated private enterprises(1) T-TeleSec(7879) policy identifier(13) cPKI(26)} -> 1.3.6.1.4.1.7879.13.26

7.1.6.2 Objekt-Identifikatoren für Zertifizierungsrichtlinien der Baseline Requirements

Vom CA/Browser Forum wurden in den Baseline Requirements [CAB-BR] folgende Policy-OIDs definiert:

- 2.23.140.1.2.1 (domain validated (DV)) und
- 2.23.140.1.2.2 (organizational validated (OV))
- 2.23.140.1.2.3 (individual validated (IV))

Für die durch das CA/Browser-Forum in den [CAB-BR] definierten Policy-OIDs gelten die folgenden Anforderungen, welche von den CAs der cPKI unter einer öffentlichen Root eingehalten werden.

Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.2 verwendet, müssen in SSL Zertifikate zwingend folgende Felder des Subject DN ausgefüllt sein:

- organizationName (Kapitel 3.1.1.1.2)
- localityName (Kapitel 3.1.1.1.12)
- stateOrProvinceName (Kapitel 3.1.1.1.13)
- countryName (Kapitel 3.1.1.1.1)

Aus der cPKI werden keine Server Zertifikate unter der öffentlichen CA mit der Policy-OID 2.23.140.1.2.2 ausgestellt.

Die Policy-OIDs 2.23.140.1.2.1 und 2.23.140.1.2.3 werden von der cPKI nicht verwendet, da keine DV- und IV-Zertifikate durch die CA unter der öffentlichen Root ausgestellt werden.

7.1.7 Verwendung der Erweiterung von Richtlinienbeschränkungen (Policy Constraints)

Nicht anwendbar.

7.1.8 Syntax und Semantik von Richtlinienkennungen

Die Zertifikate enthalten einen Eintrag “Policy Qualifier” sowie einen Verweis (URI) auf die zum Zeitpunkt der Ausstellung gültigen CP/CPS.

Es ist jeweils die aktuelle CP/CPS hinterlegt. Ältere Versionen werden in entsprechender Ablage (Repository) abgelegt. Siehe Kapitel 7.1.2.2 und Kapitel 7.1.6

7.1.9 Verarbeitungssemantik der kritischen Erweiterung „Zertifikats-Richtlinien (critical Certificate Policies)“

Nicht anwendbar.

7.1.10 Subject-DN Serial Number (SN)

Nicht anwendbar.

7.1.11 Objekt-Identifikatoren für „Certificate Transparency (CT)“

Nicht anwendbar.

7.2 Sperrlisten-Profil

Die von T-Systems 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,

Zertifikatssperrlisten müssen mindestens die in Tabelle 33 aufgeführten Inhalte aufweisen:

Felder	Wert
Version	Sperrlistenversion (Kapitel 7.2.1)
Aussteller (Issuer)	Enthält die Instanz, die die Sperrliste ausgegeben und signiert hat. Zertifizierungsstelle (Kapitel 1.3.1)
Gültig ab:	Zeitbasis: Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Nächste Aktualisierung:	Datum und Uhrzeit der nächsten geplanten Veröffentlichung. .
Signaturalgorithmus:	RSA – SHA-256[4]
Gesperrte Zertifikate:	Liste der gesperrten Zertifikate inkl. Seriennummer mit Sperrdatum- und zeitpunkt des gesperrten Zertifikats.
Erweiterungen:	
Stellenschlüsselkennung:	Es gelten die Regelungengemäß Kapitel 7.2.2.1).
Sperrlistennummer:	Eindeutiger Wert (Kapitel 7.2.2.2)
Sperrgrund:	Kodierung des Sperrgrunds nach RFC 5280 (Kapitel 7.2.2.3).

Tabelle 33: CRL Profil (hier: Basiswerte)

[4] Alternativ RSA - SHA-1

7.2.1 Versionsnummer

Die von der cPKI ausgestellten X.509-Zertifikatssperrlisten entsprechen der Version 2.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Ausgegebene CRLs enthalten die folgenden “Extension”-Einträge:

Felder	Wert
Authority Key Identifier	Dieser Eintrag enthält den Key-Hash der ausgebenden Instanz.
CRL Number	Eindeutige, aufsteigende Nummer der Sperrliste
CA Version	Startwert: 0.0
Next CRL Publish	Datum und Zeit der nächsten Sperrlistenveröffentlichung

Tabelle 34: CRL Profil: Extension-Einträge

7.2.2.1 Erweiterung „Stellenschlüsselkennung (authorityKeyIdentifier)”

Die Sperrlisten enthalten die Erweiterung „Stellenschlüsselkennung“ wie in Kapitel 7.1.2.8 beschrieben.
Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.2.2.2 Erweiterung „Sperrlistennummer“

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

7.2.2.3 Erweiterung „Sperrgrund” (Reason Code)

Bei der Sperrung von Zertifikaten muss zwingend ein Sperrgrund angegeben werden. Gemäß nachfolgender Tabelle 35 sind folgende Sperrgründe implementiert:

Ereignis	Sperrgründe nach RFC 5280	Wert des Sperrgrundes nach RFC 5280
Nicht spezifiziert	Nicht angegeben (unspecified)	0
Schlüssel kompromittiert	Schlüsselkompromittierung (keyCompromise)	1
Angaben im Zertifikat nicht mehr aktuell	Zuordnung geändert (affiliationChanged)	3
Zertifikat nach Erneuerung gesperrt	Abgelöst (superseded)	4
Temporäre Sperrung	Temporäre Sperrung (certificateHold)	6

Tabelle 35: Erweiterung Sperrgrund

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.3 OCSP Profil

OCSP (Online Certificate Status Protocol) stellt auf gleichnamigen Protokoll einen Validierungsdienst zur Verfügung, mit dessen Hilfe dem vertrauende Dritten eine zeitgerechte Information zum Sperrstatus von Endteilnehmer-Zertifikaten übermittelt wird.

Der eingesetzte OCSP-Responder erfüllt die Anforderungen des RFC 6960.

7.3.1 Versionsnummer

Es wird die Version 1 gemäß der OCSP-Spezifikation nach RFC 6960 unterstützt.

7.3.2 OCSP Erweiterungen

Das OCSP-Zertifikat, ausgestellt von der Zwischenzertifizierungsstelle (Sub-CA) (Übersicht siehe Abbildung 1, Abbildung 2, Abbildung 3), enthält das Attribut „Erweiterter Schlüsselverwendung“ mit der OID „1.3.6.1.5.5.7.3.9“ (OCSP noCheck, id-pkix-ocsp-nocheck), d.h. das OCSP-Zertifikat wird nicht validiert.

8 COMPLIANCE-AUDITS UND ANDERE PRÜFUNGEN

Die Stellen, die einem Audit, einer Überprüfung oder einer Untersuchung unterzogen werden, müssen T-Systems und/oder einen beauftragten Dritten unterstützen.

Weiterhin ist T-Systems berechtigt, die Durchführung dieser Audits, Überprüfungen und Untersuchungen auf Dritte (Kapitel 8.2) zu übertragen.

Die T-Systems-Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI 319411-1 Policy LCP) unterzogen. Zertifizierungsgegenstand sind alle Prozesse, die zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (Kapitel 1.3.1.1.1 und 1.3.1.2.1) dienen.
T-Systems führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durch (Kapitel 8.1).

8.1 Intervall oder Gründe von Prüfungen

Compliance-Audits finden in der Regel jährlich oder nach Bedarf statt und werden auf Kosten der überprüften Stelle durchgeführt. Der Beginn dieser Maßnahme ist mindestens eine Woche vorher schriftlich anzukündigen. Audits werden über einer ununterbrochenen Folge von Auditperioden durchgeführt, deren Zeitraum die Dauer von einem Jahr nicht überschreitet.

Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits), die die Servicequalität sicherstellen, finden regelmäßig und bei Bedarf (z.B. Sicherheitsvorfall) statt. Es werden mindestens 3 (drei) Prozent der in diesem Zeitraum relevanten ausgestellten Zertifikate, aber in jedem Fall 1 ausgestelltes Zertifikat betrachtet, wobei die Auswahl zufällig erfolgt. Es wird immer der Zeitraum, der auf die Periode des vorangegangenen Selbstaufsichtsmaßnahme folgt, für die Auswahl herangezogen.

8.2 Identität und Qualifikation von Prüfern

Die Trust-Center-spezifischen Compliance-Audits werden von qualifizierten Mitarbeitern der T-Systems oder einem Dritten (z.B. qualifiziertes Unternehmen wie TÜV IT) durchgeführt, die Erfahrung in den Bereichen Public-Key-Infrastructure-Technologie, Sicherheits-Auditing und Verfahren und Hilfsmittel der Informationssicherheit vorweisen können.

Für Auditoren, welche im T-Systems Trust Center ein Audit auf Anforderung eines oder mehrerer Anwendungssoftwareanbieter durchführen, gelten besondere Anforderungen. Für cPKI beauftragt das Trust Center einen für die ETSI-Zertifizierung akkreditierten Auditor. Dadurch ist die Einhaltung der besonderen Anforderungen (z.B. Qualifikation, Unabhängigkeit) an den Auditor gewährleistet.

Die Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) werden durch einen qualifizierten T-Systems Mitarbeiter mit entsprechender Fachkunde in den Bereichen PKI, IAM sowie ETSI-Anforderungen durchgeführt.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die ETSI-Zertifizierungen handelt es sich um einen unabhängigen und qualifizierten Auditor (z.B. Wirtschaftsprüfer, Gutachter).

Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) werden von dafür qualifizierten T-Systems Mitarbeitern durchgeführt.

8.4 Abgedeckte Bereiche der Prüfung

Zielsetzung der Überprüfung ist die Umsetzung dieses Dokuments. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Ausstellung von Zertifikaten
- Datenquelle / vertrauenswürdige Datenbasis auf deren die Endteilnehmer registriert werden
- Zertifikatsbeantragungsverfahren
- Bearbeitung von Zertifikatsanträgen
- Verteilung von Schlüsseln und Geheimnissen (Passwort, OTP, PIN)
- Zertifikatsannahmen
- Zertifikatserneuerung (Re-Zertifizierung)
- Schlüsselerneuerung (Re-Key)
- Zertifikatssperrungen
- Zutrittsschutz
- Schlüsselsicherung und -archivierung
- Berechtigungs- und Rollenkonzept
- Einbruchshemmende Maßnahmen
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen der folgenden Audit-Kriterien geprüft:

- ETSI 319411-1 Policy LCP

Risikobewertung und Sicherheitsplan

Das T-Systems Trust Center führt in der Regel jährlich oder nach Bedarf eine Risikobewertung durch, welches u.a. auch den PKI-Dienst cPKI abdeckt.

Die Überprüfung beinhaltet zumindest die folgenden Punkte:

1. Identifikation vorhersehbarer externer, als auch interner Gefährdungen (d.h. insbesondere die zu Grunde liegenden Schwachstellen), welche
   a. zu unbefugten Zugriffen auf relevante Daten oder Systeme,
   b. zur Weitergabe oder einem Missbrauch von relevanten Daten,
   c. zu Veränderungen oder Zerstörung von relevanten Daten,
   d. zur Beeinträchtigung, Störung oder Ausfall von Teilen oder des gesamten Zertifikatsverwaltungsprozesses

führen können.

2. Beurteilung der Eintrittswahrscheinlichkeit und der daraus resultierenden potenziellen Schäden (d.h. Schadenshöhe) durch das Ausnutzten einer Schwachstelle. Dabei ist der besondere Schutzbedarf der Zertifikatsdaten und des Zertifikatsverwaltungsprozesses zu berücksichtigen.
3. Beurteilung der Wirksamkeit und Angemessenheit der getroffenen Gegenmaßnahmen (z.B. Richtlinien, Verfahren, eingesetzte Sicherheits-Systeme, Technologien, Versicherungen) welche die Gefährdung beseitigen oder das Risiko minimieren.

Basierend auf der Risikobewertung hat das T-Systems Trust Center einen Sicherheitsplan entwickelt, der regelmäßig überprüft und bei Bedarf angepasst wird. Der Sicherheitsplan besteht aus Verfahren, Maßnahmen und Produkten, um die Bewertung und das Management der während der Risikobewertung identifizierten Risiken zu unterstützen. Der

Sicherheitsplan enthält entsprechend der Sensibilität der Daten und des Zertifikatsverwaltungsprozesses administrative, organisatorische, technische und physische Sicherheitsmaßnahmen.

8.5 Maßnahmen zur Mängelbeseitigung

Werden bei einem Compliance Audit von T-Systems Mängel oder Fehler festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durch zu führen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheiden der Leiter Trust Center über den Zeitrahmen der Behebung.

8.6 Mitteilung der Ergebnisse

Die Ergebnisse der Prüfung werden in einem vom Prüfer erstellten Bericht dokumentiert und T-Systems übergeben.

T-Systems behält sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, z.B. wenn Missbrauch stattfand oder bei möglicher Schädigung des Ansehens der T-Systems.

Auditberichte, die auf Anforderung eines oder mehrerer Anwendungssoftwareanbieter abgelegt werden, und welche sich auf ein Stammzertifizierungsstellenzertifikat der T-Systems beziehen, müssen spätestens drei Monate nach Ablauf der jeweiligen Auditperiode veröffentlicht werden.

Für die cPKI werden die geforderten Audits nach dem ETSI 319411-1 Policy LCP Kriterien abgelegt. Die zugehörigen Berichte werden auf der Internetseite https://corporate-pki.telekom.de/ veröffentlicht.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

Die Entgelte für PKI Services werden in den jeweiligen vertraglichen Vereinbarungen mit dem Auftraggeber festgelegt; eine Publikation dieser Entgeltvereinbarungen erfolgt nicht.

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

T-Systems ist berechtigt, für das Ausstellen, Erneuern und Verwalten von Endteilnehmer-Zertifikaten Entgelte zu berechnen. Dies gilt insbesondere für die Bereitstellung und Überlassung des cPKI Dienstes.

9.1.2 Entgelte für den Zugriff auf Zertifikate

T-Systems berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst der cPKI keine Entgelte.

Dritten ist es nur nach vorheriger, ausdrücklicher schriftlicher Genehmigung gestattet, die von T-Systems öffentlich zur Verfügung gestellten Zertifikate selbst zu vermarkten oder zur Vermarktung anzubieten.

9.1.3 Entgelte für Sperrung oder Statusabfragen

T-Systems berechnet für den Zugriff auf Sperrungs- oder Statusinformationen für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile keine Entgelte.

Dritten ist es nur nach vorheriger, ausdrücklicher schriftlicher Genehmigung gestattet, die von T-Systems öffentlich zur Verfügung gestellten Sperr- und Statusinformationen selbst zu vermarkten oder zur Vermarktung anzubieten.

9.1.4 Entgelte für andere Leistungen

T-Systems berechnet keine Entgelte auf den Abruf und der damit verbundenen Betrachtung dieses Dokuments „Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS))“. Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1), die das Urheberrecht des Dokuments (Kapitel 9.5.2) besitzt.

Ebenfalls ist die Nutzung dieser CP/CPS entgeltfrei, sofern Sie als mit geltende Vertragsunterlage für die Vertragsbeziehung zwischen Auftraggeber und T-Systems dient.

9.1.5 Entgelterstattung

Die Erstattung von Entgelten durch T-Systems erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts.

9.2 Finanzielle Verantwortlichkeiten

Es gelten die Regelungen des Einzelvertrages.

9.2.1 Versicherungsschutz

Dem Auftraggeber obliegt die Pflicht sich im Rahmen seiner Betriebshaftpflichtversicherung bei einem Versicherungsträger oder mittels einer eigenen Deckungsvorsorge für einen wirtschaftlich angemessenen Versicherungsschutz abzusichern.

T-Systems verfügt über einen entsprechenden Betriebs- und Vermögenshaftpflichtversicherungsschutz.

9.2.2 Sonstige finanzielle Mittel

Dem Auftraggeber wird empfohlen, selbst über ausreichend finanzielle Mittel zu verfügen, um damit die Aufrechterhaltung ihres PKI-Betriebes als auch zur Erfüllung seiner aus diesem Dokument beschriebenen und abgeleiteten Pflichten nachkommen zu können. Darüber hinaus muss der Auftraggeber in der Lage sein, das Haftungsrisiko gegenüber den Endteilnehmern zu tragen, sofern dieses Risiko nicht übertragen werden kann.

T-Systems wird nicht grundsätzlich den Nachweis über finanzielle Mittel fordern. Eine Ausnahme bilden jedoch Compliance-Audits wie in Kapitel 8 beschrieben.

9.2.3 Versicherung oder Garantie für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

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) der cPKI 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 der cPKI eingestuft, die in ausgegebenen Zertifikaten (z.B. E-Mail-Adresse, Organisation, Vor- und Nachname), Sperrlisten, Statusinformationen enthalten sind oder davon abgeleitet werden können.

9.3.3 Verantwortung zum Schutz von vertraulichen Informationen

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

Der Auftraggeber hat die einschlägigen gesetzlichen Bestimmungen sowie ggf. weiteren Regelungen zum Datenschutz zu beachten.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

9.4.1 Datenschutzkonzept

Innerhalb der cPKI muss T-Systems zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten.

Die T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß Art. 32 DSGVO sowie nach nationales Recht § 64 BDSG sicher.

Entsprechend den Konzernvorgaben der DTAG wurde für die cPKI ein Datenschutzkonzept im Rahmen eines obligatorisch durchzuführenden Verfahrens (sogenanntes PSA-Verfahren) erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte für die cPKI zusammen.

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 zum Schutz personenbezogener Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.3.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsantragsteller stimmt der Nutzung von personenbezogenen Daten durch eine cPKI zu, soweit dies zur Leistungserbringung erforderlich ist.

Für Mitarbeiter der DTAG, ihrer Töchter und Beteiligungen, sowie für Auftragnehmer, die im Rahmen ihres Beschäftigungs- oder Auftragsverhältnisses die cPKI nutzen, ist die Rechtsgrundlage der innerhalb der cPKI verarbeiteten personenbezogener Daten durch die DSGVO Art. 6 Abs. 1 lit.b sowie durch nationales Recht nach § 26 BDSG „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“ gegeben. Die Nutzung der cPKI und die hierfür erforderliche Verarbeitung von personenbezogenen Daten ist des Weiteren in einer Betriebsvereinbarung innerhalb der DTAG geregelt.

Ferner dürfen alle Informationen veröffentlicht werden, die nach Kapitel 9.4.3 als nicht vertraulich behandelt werden und deren Veröffentlichung durch den Auftraggeber nicht widersprochen wurde.

Die cPKI veröffentlicht eine Datenschutzinformation, diese steht allen Endteilnehmern im Intranet der DTAG zur Verfügung.

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 einer Offenlegung

Keine Bestimmungen.

9.5 Rechte des geistigen Eigentums (Urheberrechte)

Die nachfolgenden Kapitel 9.5.1 bis 9.5.4 gelten für geistige Eigentumsrechte von Endteilnehmern und vertrauenden Dritten.

9.5.1 Eigentumsrechte an Zertifikaten und Sperrungsinformationen

T-Systems behält sich jede geistigen Eigentumsrechte an Zertifikaten, Sperr- oder Statusinformationen, öffentlich zugängliche Verzeichnisdiensten und Datenbanken mit den ihnen enthaltenen Informationen vor, die die cPKI ausstellt bzw. verwaltet.

Sofern Zertifikate und deren Inhalte die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt T-Systems die Zustimmung, Zertifikate auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren.

Unter Voraussetzung, dass die Nutzung von Sperrungs- oder Statusinformationen und deren Inhalte, die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt T-Systems ihre Zustimmung, Sperrlisten und Statusinformationen auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren, insbesondere an vertrauende Dritte.

9.5.2 Eigentumsrechte dieser CP/CPS

Dieses Dokument „Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS))“ ist urheberrechtlich geschützt, alle geistigen Eigentumsrechte obliegen der T-Systems. Jegliche andere Nutzung (z.B. Vervielfältigung, Verwendung von Texten und Bildern, Änderung oder Erzeugung eines vergleichbaren oder abgeleiteten Dokuments, Weitergabe an Personen ohne Interesse an dem in diesem Dokument beschriebenen Dienst), auch auszugsweise, bedarf der vorherigen ausdrücklichen schriftlichen Genehmigung des Herausgebers dieses Dokuments (siehe Kapitel 1.5.1).

9.5.3 Eigentumsrechte an Namen

Der Endteilnehmer behält, sofern zutreffend, alle Rechte an Namen oder Marken, die im Zertifikat enthalten sind, sofern das Zertifikat einen eindeutigen Namen beinhaltet.

9.5.4 Eigentumsrechte an Schlüsseln und Schlüsselmaterial

Die geistigen Eigentumsrechte von Schlüsselmaterial der CA- und Root-CA verbleiben bei T-Systems, ungeachtet des Mediums, auf denen sie gespeichert sind. Kopien von CA- und Root-CA-Zertifikaten dürfen vervielfältigt werden um diese in vertrauenswürdige Hardware- und Software-Komponenten zu integrieren.

Schlüsselmaterial, das der Auftraggeber bzw. dessen Endteilnehmer selbst erzeugte, verbleibt sein Eigentumsrecht. Dies gilt auch für Schlüsselmaterial auf MyCards, das er erworben hat.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle

Die Zertifizierungsstelle „cPKI“ der DTAG übernimmt die Verantwortung für alle Aspekte der Bereitstellung des Zertifizierungsdienstes, als auch für die Tätigkeiten, die an Unterauftragnehmer ausgelagert werden. Die Zertifizierungsinstanz hat die Verantwortlichkeiten klar geregelt.

Ebenfalls gelten die entsprechenden Regelungen „Delegierung von Tätigkeiten“ der [CAB-BR].

Die Zertifizierungsinstanz verfügt über eine dokumentierte Vereinbarung und ein aktuelles Vertragsverhältnis, die die Bereitstellung des PKI-Dienstes hinsichtlich Zulieferung oder andere Vereinbarungen mit Dritten unterstützt. Der Betrieb der CA erfolgt durch die T-Systems, eine Ausgliederung von Betriebsfunktionen (Outsourcing) erfolgt nicht.

T-Systems verpflichtet sich:

- keine unrichtigen Angaben in Zertifikaten aufzunehmen, die der Zertifizierungsstelle oder den Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass 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,
- dass alle Zertifikate den wesentlichen Anforderungen dieser CP/CPS genügen und
- dass die Sperrfunktionalitäten und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP Responder) allen wesentlichen Anforderungen der geltenden CP/CPS erfüllen.

Weiterhin sichert das T-Systems Trust Center zu, dass zum Zeitpunkt der Ausstellung eines [CAB-BR] konformen Zertifikates:

1. eine definierte Prozedur existiert um sicherzustellen, dass der Antragsteller das Recht hat, die im Zertifikat benannten Domains/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 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 diesem CP/CPS detailliert spezifiziert wird
7. eine definierte Prozedur befolgt wird, um zu prüfen, dass 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 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 detailliert spezifiziert wird.

Das T-Systems Trust Center sichert weiterhin zu, dass

13. falls der Zertifikatsnehmer einem verbundenen Unternehmen (Affilate) angehört oder in dessen Namen für dieses auftritt, der Repräsentant des Antragstellers vor der Ausstellung eines Zertifikates die "Nutzungsbedingung" akzeptieren muss.
14. falls der Zertifikatsnehmer einer Beauftragten Drittpartei angehört oder in deren Namen für dieses auftritt, der Antragsteller mit der T-Systems die "Bezugsvertrag" in einer rechtlich durchsetzbaren Form vereinbart.
15. es ein öffentlich zugängliches Verzeichnis betreibt, welches Status Informationen zu allen nicht abgelaufenen Zertifikaten (gültig oder gesperrt) enthält. Dieses Verzeichnis ist 7x24h verfügbar.
16. die ausgestellten Zertifikate aus allen in den [CAB-BR] aufgeführten Gründen sperren wird.
17. bei einer Kenntnisnahme der Zertifizierungsstelle über eine Kompromittierung die betroffenen Zertifikate sperren wird.

T-Systems behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Auftraggeber für den Betrieb der cPKI abzuschließen.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle

Registrierungsstellen verpflichten sich:

- das Zertifikat der Registrierungsstelle (und deren Derivate, Kapitel 1.3.2) nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- ihren privaten Schlüssel geheim zu halten vor unberechtigtem Zugriff durch Dritte zu schützen,
- bei Verlust oder Verdacht der Kompromittierung des privaten Schlüssels eine Sperrung des entsprechenden Authentifizierungs-Zertifikats (und deren Derivate) zu veranlassen,
- keine wesentlich unrichtigen Angaben im Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- dass das von ihnen eingesetzte Zertifikat ausschließlich für autorisierte und legale Zwecke verwendet wird, die der Auftraggeber vorgibt, und nicht den Regelungen dieser CP/CPS widersprechen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der vorliegenden Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) beschriebenen Pflichten entstehen,
- auf Anforderung eines Endteilnehmers oder autorisierten Vertreters bei Verlust oder Verdacht der Kompromittierung des geheimen Schlüssels eine Sperrung durchzuführen,
- dass alle Zertifikate den wesentlichen Anforderungen dieser CP/CPS genügen, und
- dass die Sperrfunktionalitäten und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) in allen wesentlichen Anforderungen der vorliegenden Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) erfüllen.

T-Systems behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Auftraggeber für den Betrieb der cPKI abzuschließen.

9.6.3 Zusicherungen und Gewährleistungen der vertrauenswürdigen Datenbank

Vertrauenswürdigen Datenbank verpflichten sich,

- einen Nachweis zur Sicherstellung der Authentizität von Daten im Endteilnehmer-Zertifikatsantrag für Benutzer zu erbringen,
- zur regelmäßigen Durchführung von Audits mit dem Internal Control System (ICS IT) durch Externe Wirtschaftsprüfer,
- zur Durchführung und Freigabe in einem PRIVACY & SECURITY ASSESSMENT (PSA) Verfahren
- zur Durchführung von Penetrationstests durch Sicherheitsexperten der Telekom Security
- zur Zertifizierung nach ISO 27001

9.6.4 Zusicherungen und Gewährleistungen des Endteilnehmers

Endteilnehmer verpflichten sich,

- das Endteilnehmer-Zertifikat nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- ihren privaten Schlüssel vor unberechtigtem Zugriff durch Dritte zu schützen. Im Falle von privaten Schlüsseln von juristischen Personen oder Geräten erfolgt der Schutz durch autorisierte Personen,

- dass jede digitale Signatur mit dem privaten Schlüssel erstellt wird, die zum im Zertifikat zugehörigen öffentlichen Schlüssel passt und dem Endteilnehmer eindeutig zugeordnet werden kann,
- dass jede digitale Signatur mit dem Schlüsselmaterial eines gültigen und nicht gesperrten Zertifikats erfolgt,
- dass die in seinem Endteilnehmer-Zertifikat aufgenommenen Zertifikatsinhalte des Subject-DN der Wahrheit entsprechen. Im Falle von juristischen Personen oder Geräten erfolgt die Prüfung der Zertifikatsinhalte durch autorisierte Personen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung des vorliegenden CP/CPS beschriebenen Pflichten entstehen,
- dafür Sorge zu tragen, dass ihre Geräte bei der Zertifikatsbeantragung und –ausstellung als auch Zertifikats-Validierung keine technischen Schnittstellen der cPKI beeinträchtigen (rollenspezifische Webseiten, LDAP, SCEP, Mail, OCSP, CRL),
- bei Verlust oder Verdacht der Kompromittierung des geheimen Schlüssels, wesentliche Änderungen der Zertifikatsangaben oder Missbrauchsvermutung eine Sperrung des entsprechenden Endteilnehmer-Zertifikat zu veranlassen bzw. selbst durchzuführen,
- bei Kompromittierung des privaten Schlüssels ist die Verwendung des privaten Schlüssels des Zertifikatsinhabers unmittelbar und dauerhaft einzustellen,
- dass das von ihnen eingesetzte Zertifikat ausschließlich für autorisierte und legale Zwecke die, diesem CP/CPS entsprechen, verwendet wird und nicht den Regelungen dieser Erklärung widersprechen, und
- dass der Endteilnehmer tatsächlich ein Endteilnehmer ist und mit seinem privaten Schlüssel, dem der im Zertifikat enthaltene öffentliche Schlüssel zugeordnet ist, keine CA-Funktionalitäten durchführt wie z.B. Signatur von Zertifikaten oder Sperrlisten.

Die T-Systems behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Endteilnehmers abzuschließen.

9.6.5 Zusicherungen und Gewährleistungen der Schlüsselverantwortlichen von Funktions- und Gruppenzertifikate

Der Schlüsselverantwortliche verpflichtet sich,

- zur Identifizierung und Authentisierung der Gruppenmitglieder,
- gegenüber dem Trust Center nachzuweisen, dass er Besitzer des Funktions- oder Gruppenpostfachs und damit Schlüsselverantwortlicher ist.
- dass bei Übergabe seiner Verantwortung an einen neuen Schlüsselverantwortlichen die Vorgaben für das Verwalten des Schlüssels und der Zertifikate beachtet werden. Wie z.B. das Ausscheiden eines Gruppenmitglieds.
- alle erforderlichen Stellen innerhalb der Organisation sowie das Trust Center über den Wechsel zu informiert, bzw. sicherzustellen, dass in den am Trust Center angebunden elektronischen Systemen der Wechsel dokumentiert und der aktuelle Schlüsselverantwortliche abrufbar ist,
- alle weiteren Schlüsselinhaber (Gruppenmitglieder) über die Pflicht zur Einhaltung der Sonderregelungen für Gruppenzertifikate zu informieren,
- im Falle automatisierter IT-Prozesse für die sichere Anwendung der Gruppenzertifikate auf der Grundlage diesen CPS, den Compliance-, Datenschutz und Sicherheitsvorgaben der DTAG sowie ggf. eines Sicherheitskonzepts sorge zutragen,
- die Sperrung der Gruppen-Zertifikate in Übereinstimmung mit der Policy der ausstellenden CA und den Vorgaben für Gruppen-Zertifikate zu verantworten und ggf. durchzuführen,
- nach Ausscheiden eines Gruppenmitglieds zu prüfen, welche Risiken durch einen unberechtigten Zugriff auf den geheimen Schlüssel bestehen. Er stellt sicher, dass ein Missbrauch des geheimen Schlüssels und des Zertifikats

durch das ausgeschiedene Gruppenmitglied verhindert wird. Da der entsprechende geheime Schlüssel und das Zertifikat für den Gruppen- Funktionsaccount auf die jeweiligen persönlichen Smartcards der Gruppenmitglieder geschrieben werden, ist durch den Schlüsselverantwortlichen der Entzug (Löschung) des entsprechenden geheimen Schlüssels und Zertifikats auf der Smartcard des ausscheidenden Gruppenmitglieds durch den Schlüsselverantwortlichen sicherzustellen. Sollte ein Löschen des geheimen Schlüssels und des Zertifikats nicht möglich, bzw. nicht erfolgreich sein, ist durch den Schlüsselverantwortlichen zu überprüfen, ob der Entzug des Zugriffs auf die Anwendung/Postfachs oder den gesicherten Daten hinreichend ist oder ein Schlüsselwechsel erforderlich ist. Bei Bedarf veranlasst der Schlüsselverantwortliche dann die Sperrung, bzw. Erneuerung des Funktions- oder Gruppenzertifikats. Ggf. kann auch durch Einziehen der persönlichen Smartcard (MyCard) durch den Vorgesetzten ein Missbrauch verhindert werden.

- falls ein Missbrauch des Schlüssels befürchtet wird, bzw. bei Verdacht auf Kompromittierung des Schlüsselmaterials, die sofortige Sperrung des Zertifikats durchzuführen und informiert umgehend die Unternehmenssicherheit der DTAG sowie das Trust Center der T-Systems über diesen Vorfall.
- zu berücksichtigen, dass bei einem Schlüsselwechsel verschlüsselt archivierte Dokumente der ganzen Gruppe betroffen sind und stellt die Verfügbarkeit dieser Dokumente sicher.

9.6.6 Zusicherungen und Gewährleistungen von vertrauenden Dritten

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

Der vertrauende Dritte muss sein Gerät so konfigurieren, dass bei der Zertifikats-Validierung keine technischen Schnittstellen der cPKI beeinträchtigt werden (rollenspezifische Webseiten, LDAP, SCEP, Mail, OCSP, CRL).

9.6.7 Zusicherungen und Gewährleistungen anderer Teilnehmer

Nicht anwendbar.

9.7 Haftungsausschluss

Die T-Systems haftet gegenüber dem Kunden stets

a. für die von ihr sowie ihren gesetzlichen Vertretern oder Erfüllungsgehilfen vorsätzlich oder grob fahrlässig verursachten Schäden,

b. nach dem Produkthaftungsgesetz und

c. für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die der Anbieter, seine gesetzlichen Vertreter oder Erfüllungsgehilfen zu vertreten haben.

Die T-Systems haftet bei leichter Fahrlässigkeit nicht, außer soweit sie eine wesentliche Vertragspflicht verletzt hat, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Kunde regelmäßig vertrauen darf. Schäden (inkl. Imageschäden), die durch missbräuchlichen oder Zertifikatsinhalt (Kapitel 4.5.1, 5.8) oder missbräuchliche Nutzung von Warenzeichen, Markenrechte (Kapitel 3.1.6) entstehen, gehen zu Lasten des Auftraggebers.

9.8 Haftungsbeschränkungen

9.8.1 Haftung des Anbieters (T-Systems)

Diese Haftung ist bei Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden beschränkt. Dies gilt auch für entgangenen Gewinn und ausgebliebene Einsparungen. Die Haftung für sonstige entfernte Folgeschäden ist ausgeschlossen.

Bei Vereinbarung einer Einmal-Vergütung ist die Haftung bei Sach- und Vermögensschäden auf 10 % des Netto-Auftragsvolumens pro Schadensereignis und für alle Schäden innerhalb eines Vertragsjahres auf 25 % des Netto-Auftragsvolumens begrenzt. Bei Vereinbarung einer wiederkehrenden Vergütung ist die Haftung bei Sach- und sonstigen Schäden auf 10 % des Netto-Jahresentgelts pro Schadensereignis und für alle Schäden innerhalb eines Vertragsjahres auf 25 % des Netto-Jahresentgelts begrenzt. Die Parteien können bei Vertragsabschluss eine weitergehende Haftung gegen gesonderte Vergütung vereinbaren. Vorrangig ist eine gesondert vereinbarte Haftungssumme. Die Haftung gemäß Kapitel 9.7 bleibt von diesem Absatz unberührt.

Ergänzend und vorrangig ist die Haftung der T-Systems wegen leichter Fahrlässigkeit - unabhängig vom Rechtsgrund - insgesamt begrenzt auf 2,5 Mio. EUR. Die Haftung gemäß Kapitel 9.7 Buchstabe b) bleibt von diesem Absatz unberührt.

Aus einer Garantieerklärung haftet die T-Systems nur auf Schadensersatz, wenn dies in der Garantie ausdrücklich übernommen wurde. Diese Haftung unterliegt bei leichter Fahrlässigkeit den Beschränkungen gemäß Kapitel 9.8.1.

Bei Verlust von Daten haftet die T-Systems nur für denjenigen Aufwand, der für die Wiederherstellung der Daten bei ordnungsgemäßer Datensicherung durch den Kunden erforderlich ist. Bei leichter Fahrlässigkeit der T-Systems tritt diese Haftung nur ein, wenn der Kunde unmittelbar vor der zum Datenverlust führenden Maßnahme eine ordnungsgemäße Datensicherung durchgeführt.

Für Aufwendungsersatzansprüche und sonstige Haftungsansprüche des Kunden gegen die T-Systems gelten die Kapitel 9.7 und 9.8 ff entsprechend.

9.8.2 Haftung des Zertifikatsinhabers

Der Zertifikatsinhaber (Zertifikatsnehmer) haftet gegenüber dem Anbieter (T-Systems) und den beteiligten Parteien für Schäden, die aus Missbrauch, vorsätzlichem Fehlverhalten, Nichteinhaltung von aufsichtsrechtlichen Verpflichtungen oder Nichteinhaltung anderer Bestimmungen zur Nutzung des Zertifikats resultieren.

9.9 Schadenersatz

Für etwaige Schadensersatzansprüche gelten die Regelungen in Kapitel 9.7 und 9.8 ff.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Die Erstveröffentlichung dieses Dokuments „CP/CPS“ als auch dessen Änderungen treten mit der Veröffentlichung auf öffentlichen Webseiten der T-Systems (siehe Kapitel 2.3) in Kraft.

9.10.2 Beendigung

Diese CP/CPS 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 cPKI Dienstes bleiben der Auftraggeber als auch die Benutzer der daraus erzeugten Endteilnehmer-Zertifikaten an die in der CP/CPS enthaltenen Regelungen gebunden, bis das letzte ausgegebene Zertifikat ungültig oder gesperrt wird.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

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

9.12 Änderungen

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

9.12.1 Verfahren für Änderungen

Änderungen dieser CP/CPS können nur vom T-Systems 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 dieses Dokuments setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet T-Systems über weitere Vorgehensweise.

Innerhalb bestehender Verträge sind Änderungen dieser CP/CPS mindestens sechs Wochen vor Wirksamwerden schriftlich dem Auftraggeber für den Betrieb der cPKI mitzuteilen. Bei Änderungen zu Ungunsten des Auftraggebers sind diese Einvernehmlich mit dem Auftragnehmer zu regeln, Ausnahmen stellen hier Änderungen dar, die nicht durch das Trust Center zu verantworten sind (z.B. Änderungen von Vorgaben der CAB BR oder Gesetzliche Vorgaben) . Erfolgt seitens des Auftraggebers für den Betrieb der cPKI innerhalb von sechs Wochen nach Zugang der Änderungsmitteilung kein schriftlicher Einspruch, werden die Änderungen zum Zeitpunkt des Wirksamwerdens Vertragsbestandteil.

9.12.2 Benachrichtigungsverfahren und -zeitraum

Die im Zusammenhang mit einzelvertraglichen Regelungen benannten Ansprechpartner werden über Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch einzulegen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion nach Ablauf der Frist in Kraft. Darüberhinausgehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Falls T-Systems der Ansicht ist, dass z.B. gravierende 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, unter denen die Objekt-Kennung (Objekt – ID) geändert werden muss

T-Systems Advisory Board entscheidet darüber, ob Änderungen der Objekt-ID der CP/CPS notwendig werden. Andernfalls erfordern Änderungen keine Änderungen der Objekt-ID der Zertifikatsrichtlinie

9.13 Bestimmungen zur Beilegung von Streitigkeiten

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

9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Frankfurt am Main, 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 CP/CPS 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 CP/CPS unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser CP/CPS 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

Es gelten die einzelvertraglichen Regelungen, welche mit dem Auftraggeber vereinbart wurden.

Innerhalb des gesetzlich zulässigen Rahmens müssen Verträge mit Auftraggebern, vertrauende Dritten oder Endteilnehmern Schutzklauseln über höhere Gewalt enthalten, um T-Systems schützen zu können.

Mit dieser Regelung soll sichergestellt werden, dass T-Systems mit seinen Auftraggebern, vertrauende Dritten oder Endteilnehmern vereinbart, dass T-Systems nicht in Verzug gerät, wenn sich die Leistung infolge höherer Gewalt verzögert oder unmöglich wird.

9.17 Sonstige Bestimmungen

9.17.1 Barrierefreiheit

Der Zugang zu den TC-Services der Corporate PKI der DTAG erfolgt im Wesentlichen browserbasiert. Betriebssysteme bieten hier eine Vielzahl unterschiedlicher Barrierefreiheitsfeatures, um behinderten Personen den Zugriff auf die Web-Portale der Trust Center Services zu erleichtern. Diese kompensieren insbesondere Einschränkungen des Seh- und Hörvermögens, physischen Einschränkungen sowie Wahrnehmungsstörungen (z.B. „Informationen zur Barrierefreiheit für IT-Experten“).

Für die durch die Corporate PKI eingesetzte Software und Webportal liegt vom 04.03.2014 ein Barrierefreiheitstestat der T-Systems Multimedia GmbH vor, in dem die Barrierefreiheit bestätigt wird.

Das unabhängige und akkreditierte Test and Integration Center (TIC) der Multimedia GmbH hat eine Accessibility-Prüfung mit dem Ziel der Beurteilung hinsichtlich der Barrierefreiheit durchgeführt. Die Anwendung dient der Einrichtung bzw. Verwaltung der Zertifikate und Daten unter Corporate PKI der DTAG.

Um die Zugänglichkeit zu den Inhalten der Anwendung für Personen mit physischen oder motorischen

Einschränkungen zu überprüfen, wurden zunächst die von diesen Benutzergruppen verwendeten assistiven Technologien und Werkzeuge empirisch auf Kompatibilität mit der Anwendung untersucht (Assistive Technologien). Anschließend erfolgte eine Prüfung auf Konformität mit aktuell anerkannten Normen sowie geltenden gesetzlichen

Richtlinien. Nicht erfüllte Prüfkriterien wurden dabei nach Schwere und Relevanz als Zugänglichkeitsblockaden, Zugänglichkeitshürden oder leichte Zugänglichkeitseinschränkungen gewichtet.

Betrachtete Benutzergruppen:

- Sehbehinderte Benutzer (S)
- Blinde Benutzer (B)
- Motorisch eingeschränkte Benutzer (M)
- Gehörlose Benutzer (G)

Die bei der Accessibility-Prüfung verwendeten Anforderungen basieren auf der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BGG).

Diese Barrierefreie-Informationstechnik-Verordnung (BITV 2.0) enthält verschiedene Anforderungen an eine Anwendung, die erfüllt sein müssen, damit die Barrierefreiheit für Personen mit Behinderungen gewährleistet ist. Diese Anforderungen sind in zwei Prioritätsstufen unterteilt und basieren im Wesentlichen auf den Web Content Accessibility Guidelines (WCAG 2.0).

Bei der Beurteilung von Desktopanwendungen wurden ergänzend die Leitlinien für die Zugänglichkeit von Software (DIN ISO 9241-171) herangezogen.

Des Weiteren erfolgen Analysen mit den SW-Entwicklungspartnern des Trust Centers, ob es ergänzend zu den Standardboardmitteln weitere sinnvolle, betriebssystemunabhängige Möglichkeiten zur Gestaltung der Barrierefreiheit gibt.

Sollten vorgenannte Maßnahmen nicht ausreichen, bietet T-Systems darüber hinaus behinderten Menschen zur Unterstützung bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten kostenlosen telefonischen Support.

A Ergänzende Literatur

A.1 Basis-Dokumentation

- Leistungsbeschreibung (LB)
- Service Level Agreement (SLA)
- Rahmen-SLA für Trust Center Services
- Begriffsdefinitionen-Akronyme
- Personelle, Infrastrukturelle und Technische Rahmenbedingungen

A.2 Rollenspezifische Handbücher

- Benutzer-Handbuch
- Betriebs-Handbuch

B Legende

✓ Leistungsmerkmal vorhanden
✖ Leistungsmerkmal nicht vorhanden

C Akronyme und Begriffsdefinition

C.1 Akronyme

AIA	Authority Information Access
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BR	Baseline Requirements
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Country
CA	Certification Authority
CAA	Certification Authority Authorization
CAB	CA/Browser Forum
CARL	Certification Authority Revocation List
cc	Country Coded
CN	Common Name
CP	Certificate Policy
cPKI	Corporate Public Key Infrastructure der DTAG
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
CT	Certificate Transparency
DIN	Deutsche Industrie Norm
DK	Dual Key
DN	Distinguished Name
DNS	Domain Name Systems
DSGVO	Datenschutz-Grundverordnung
DTAG	Deutsche Telekom AG
DV	Domain Validation
ECC	Elliptic Curve Cryptography
EDV	Elektronische Datenverarbeitung
eIDAS	electronic Identification and Signature
ERP	Enterprise-Resource-Planning
ETSI	European Telecommunications Standards Institute (deutsch: Europäisches Institut für Telekommunikationsnormen)
FIPS	Federal Information Processing Standard

FQDN	Fully Qualified Domain Name
GRP	Kennzeichner für Gruppen, Funktions-, Rollenzertifikat
GUID	Globally Unique Identifier
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
ISP	Internet Service Providers
ITIL	Information Technology Infrastructure Library
IV	Individual Validation
L	Locality
LB	Leistungsbeschreibung
LDAP	Lightweight Directory Access Protocol
MTO	Maximum Tolerable Outage
NCP	"Normalized" Certificate Policy
NIC	Network Information Center
n.v.	nicht vorhanden
O	Organisation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
OU	Organisation Unit Name
OV	Organizational Validated
OVCP	Organizational Validation" Certificate Policy
PED	PIN Entry Device
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudonym
PSE	Personal Security Environment
PROD	Productive Unit (Wirkumgebung)

PTC	Publicly-trusted certificate
RA	Registration Authority
REST	REpresentational State Transfer, API für Application Programming Interface
RFC	Requests for Comments
RSA	Rivest Shamir Adleman
RTO	Recovery Time Objective
S	State or Province Name
SAN	Subject Alternative Name
SBCA	Shared Business CA
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key
SLA	Service Level Agreement
SMS	Short Message Service
SOAP	Simple Object Access Protocol
S/MIME	Secure Multipurpose Internet Mail Extension
SCT	signed certificate timestamp
SHA	Signature Hash Algorithm
SigG	Signaturgesetz (Seit dem 29. Juli 2017 Außerkraft und durch das Vertrauensdienstegesetz (VDG) und eIDAS abgelöst)
SN	Serial Number
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TC	Trust Center
TLD	Top Level Domain
TLS	Transport Layer Security
TK	Triple Key
TSP	Trust Service Provider
CAST	Test- und Abnahme-Umgebung
UPN	User Principal Name
URL	Uniform Resource Locator
USV	Unterbrechungsfreie Stromversorgung
UTC	Universal Time Coordinated
XML	Extensible Markup Language

C.2 Begriffsdefinition

Abkürzung	Beschreibung
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 Stamm-Zertifikate (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.
Certification Authority (CA)	Siehe Zertifizierungsstelle.
Certification Authority Authorization (CAA)	Ein Verfahren, bei dem der Domain-Inhaber im DNS festlegen kann, welche Zertifizierungsstelle(n) für seine Domain(s) Zertifikate ausstellen dürfen.
Certification Authority Revocation List (CARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (außer Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der CARL überprüft werden, ob dieses noch verwendet werden darf.
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 Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
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 MyCard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.

Abkürzung	Beschreibung
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-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.
eIDAS	EU-Verordnung über elektronische Identifizierung und Vertrauensdienste. Die eIDAS-Verordnung enthält verbindliche europaweit geltende Regelungen in den Bereichen "Elektronische Identifizierung" und "Elektronische Vertrauensdienste". Mit der Verordnung werden einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste geschaffen. Als EU-Verordnung ist diese unmittelbar geltendes Recht in allen EU-Mitgliedstaaten sowie im Europäischen Wirtschaftsraum.
Endteilnehmer	Siehe auch Zertifikatnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Endteilnehmer-Zertifikat	Ein Zertifikat, welches nicht die Basiseinschränkung (basis constraints) „Zertifizierungstelle“ verwendet, daher selber keine Zertifikate signieren kann.
Erklärung zum Zertifizierungsbetrieb (CPS)	Eines von mehreren Dokumenten, die allgemeine und spezifische Rahmenbedingungen vorgibt. Dieses beninhaltet insbesondere eine Beschreibung der Verfahrensweise, wie die Zertifizierungsstelle (CA) Zertifikate ausstellt, verwaltet, sperrt und erneuert.
Erlaubte Internet-Domänen	Ein Domänenname, der aus der Top-Level-Domain und weiteren Sub-Domains besteht, und nach erfolgreicher Prüfung durch die interne Registrierungsstelle als „erlaubte Internet-Domäne“ in die PKI-Konfiguration des Mandanten (Master-Domäne) aufgenommen wird.
ETSI-Zertifizierung	Überprüfung und Bestätigung für Zertifizierungsstellen durch einen unabhängigen Gutachter, dass die PKI nach den ETSI-Kriterien „ETSI EN 319 411-1“ betrieben werden. Ziel der ETSI-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken. Für die cPKI gilt die Zertifizierung nach Policy LCP
EU-DSGVO	Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden. Die Verordnung ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Abkürzung	Beschreibung
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 E-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.
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-History	Mechanismus zur Schlüsselsicherung, um nach Wechsel der MyCard oder Neuausstellung von Zertifikaten auf bereits vorhandene verschlüsselte elektronische Dokumente oder E-Mails weiterhin zugreifen zu können.
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.

Abkürzung	Beschreibung
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-E-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.
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.
MyCard	Siehe Smartcard
Nicht registrierter Domain-Name	Ein Domain-Name, der kein registrierter Domain-Name ist.
Nutzungsbedingungen (Terms of Use)	Bestimmungen bezüglich der Verwahrung und zugelassenen Verwendungszwecke eines ausgestellten Zertifikats in Übereinstimmung mit den gegebenen Anforderungen, wenn der Antragsteller/Zertifikatnehmer beispielsweise ein verbundenes Unternehmen der Zertifizierungsstelle (CA) ist.
Object Identifier (OID)	Ein eindeutiger alphanumerischer oder numerischer Bezeichner, der unter dem jeweiligen Standard für ein bestimmtes Objekt oder eine Objektklasse der Internationalen Organisation für Normung (ISO) registriert ist.
Online Certificate Status Protocol (OCSP) [BR]	Ein Protokoll zur Online-Zertifikatsvalidierung, mit dessen Hilfe die Anwendungssoftware der vertrauenden Seite den Status eines identifizierten Zertifikats bestimmen kann. Siehe auch OCSP-Responder.
OCSP-Responder	Ein Online-Server, der der Zertifizierungsstelle (CA) untersteht und mit deren zentrale Datenablage (Repository) zur Bearbeitung von Zertifikatsstatusanfragen verbunden ist. Siehe auch Online Certificate Status Protocol (OCSP).

Abkürzung	Beschreibung
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.
One Time Passwort (OTP)	Einmalgültiges Passwort
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 MyCard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Phishing	Angriffsmethode im Internet, um an (geheime) Daten (z.B. PINs, TANs, Passwörter) eines Internetnutzers zu gelangen. Meist werden die Opfer dazu auf gefälschte Webseiten gelockt und zur Eingabe der Daten aufgefordert. Da die Seite auf den ersten Blick offiziellen Charakter hat, ist der Nutzer oft bereit, diese Daten preiszugeben.
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 Infrastruktur (PKI)	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.
Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
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 MyCard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Pseudonym-Account	Ein Pseudonym-Account hat die Eigenschaft, dass aus seinem in SAP HR gepflegten Namen nicht hervorgeht, wer mit dem Account bzw. dem dahinterliegenden Zertifikat arbeitet. Dies kann in der Organisation vorkommen z. B. für Trainingsaccounts oder Funktionsaccounts. Eine Anforderung ist, dass solche Accounts einer bestimmten Nomenklatur folgen müssen, um identifizierbar zu sein und der verantwortliche Nutzer (Schlüsselverantwortlicher) hinter diesem Account leicht ermittelbar ist.
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.

Abkürzung	Beschreibung
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.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das 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 den Kunden 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. Kann ihn vielen Fällen statt dem komplexeren IPsec verwendet werden.
Service Desk	Der Service Desk ist eine organisatorische Einheit innerhalb eines Unternehmens, das für den Kunden 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. Siehe auch MyCard.
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.

Abkürzung	Beschreibung
Stammzertifizierungsstelle (Root-CA)	Die oberste Zertifizierungsstelle, deren Stammzertifikat von Anwendungssoftwareanbietern verteilt wird und die untergeordnete CA-Zertifikate (Sub-Zertifikate) ausstellt.
Statement of Auditing Standards 70 (SAS 70)	Statement of Auditing Standards (SAS) Nr.70 mit dem Titel „Service Organizations“, ist ein international anerkannter Standard, der vom AICPA ins Leben gerufen wurde.
Subject Alternative Name	Zusätzliche Felder in einem Zertifikat. Die Felder können zusätzliche Namen des Zertifikatinhabers enthalten und ist eine Standarderweiterung des X509 Standards.
Subject-Distinguished-Name (Subject-DN)	Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Subject-DN bezeichnet eindeutig die Person oder Gerät.
Subjekt	Die natürliche Person, das Gerät, System, die Einheit oder juristische Person, die in einem Zertifikat als Subjekt benannt wird. Das Subjekt ist entweder der Zertifikatnehmer oder ein Gerät, das der Kontrolle des Zertifikatnehmers untersteht oder von diesem betrieben wird.
Subjektidentitätsdaten	Daten, die das Zertifikatssubjekt identifizieren. Subjektidentitätsdaten beinhalten keinen Domain-Namen, der in der Erweiterung subjectAltName oder im Feld Subject commonName aufgeführt ist.
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 MyCard-LogOn getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt drei entsprechende Zertifikate.
T-Systems Advisory Board	Gremium innerhalb der T-Systems das über PKI-Funktionalitäten entscheidet.
Untergeordnete Zertifizierungsstelle (Sub-CA)	Eine Zertifizierungsstelle, deren Zertifikat von der Stammzertifizierungsstelle (Root-CA) oder einer anderen Zwischenzertifizierungsstelle (Sub-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).

Abkürzung	Beschreibung
Validierungsspezialist	Jemand, der die Datenüberprüfungsaufgaben gemäß den jeweiligen Anforderungen wahrnimmt. Im Kontext der cPKI ist dies der Rolleninhaber: Trust-Center-Operator
Verbundenes Unternehmen (Affiliate)	Beispielsweise ein Unternehmen, eine Partnerschaft, ein Joint Venture, Körperschaft, (Kapital) Gesellschaft, Verband, Stiftung oder eine andere Organisation (juristische Person), welche eine andere Organisation (juristische Person), Einrichtung, Abteilung, Gebietskörperschaft oder eine Einheit, die einer Regierungsbehörde direkt unterstellt ist, beaufsichtigt, von dieser beaufsichtigt wird oder mit dieser einer gemeinsamen Kontrolle untersteht.
Vertrauende Dritte (Relying Parties)	Eine natürliche oder juristische Person, die sich auf ein gültiges Zertifikat verlässt. Ein Anbieter von Anwendungssoftware gilt nicht als vertrauender Dritter, wenn die von diesem Anbieter vertriebene Software lediglich Informationen zu einem Zertifikat anzeigt.
Vertrauenswürdiges Zertifikat	Ein Zertifikat, dem aufgrund der Tatsache vertraut wird, dass sein entsprechendes Stammzertifikat als Vertrauensanker in weit verbreiteter Anwendungssoftware verteilt ist
Vertreter des Antragstellers	Falls abweichend vom Antragsteller, eine natürliche Person oder Kostenträger, ein Beschäftigter des Antragstellers oder ein Handlungsbevollmächtigter ist, der die ausdrückliche Befugnis besitzt, den Antragsteller zu vertreten: (i) die im Namen des Antragstellers einen Antrag auf ein Zertifikat unterzeichnet, einreicht oder genehmigt, und/oder (ii) die im Namen des Antragstellers eine Bezugsvertrag (Subscriber Agreement) unterzeichnet und einreicht, und/oder (iii) die im Namen des Antragstellers die Nutzungsbestimmungen des Zertifikats anerkennt und ihnen zustimmt, wenn der Antragsteller eine verbundene Unternehmen (Affiliate) der Zertifizierungsstelle (CA) ist.
Verzeichnisdienst	Datenspeicher zum Abruf von Zertifikaten und Zertifikats-Validierungsinformationen (Sperrlisten).
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).
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. Im Kontext mit der cPKI wird dieses Merkmal nicht unterstützt.
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. Zertifikatsrichtlinien, Erklärung zum Zertifizierungsbetrieb, CA-Zertifikate) sowie Zertifikatsstatusinformationen, entweder in Form einer CRL- oder OCSP-Antwort, enthält.
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) ausgestellter Sub-Zertifikate unterstützen.

Abkürzung	Beschreibung
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 (CARL) ist ein Spezialfall der Zertifikatssperrliste (CRL), da sie nur Sub-CA-Zertifikate enthält
Zertifikatsverwaltungsprozess	Prozesse, Praktiken und Verfahren im Zusammenhang mit der Verwendung von Schlüsseln, Software und Hardware, mit deren Hilfe die Zertifizierungsstelle (CA) Zertifikatsdaten prüft, Zertifikate ausstellt, eine zentrale Datenablage (Repository) unterhält und Zertifikate widerruft/sperrt.
Zertifizierungsrichtlinie (CP)	Ein Regelwerk, das die Verwendungsmöglichkeit eines genannten Zertifikats auf eine bestimmte Gemeinschaft (PKI-Beteiligte) und/oder eine PKI-Implementierung mit gängigen Sicherheitsanforderungen, vorgibt.
Zertifizierungsstelle (CA)	Eine Organisation, die für die Generierung, Ausstellung, die Sperrung und die Verwaltung von Zertifikaten zuständig ist. Die Bezeichnung bezieht sich sowohl auf Stammzertifizierungsstellen (Root-CA) als auch auf untergeordnete Zertifizierungsstellen (Sub-CA).
Zuständigkeitsbereich	Hierarchisch untergeordneter Teilbereich der Master-Domäne, der von einem Sub-Registrator verwaltet wird.
Zuverlässige öffentliche Datenquelle	Ein Authentifizierungsdokument oder eine Datenquelle (z.B. Identitätsdatenbank, Handelsregister), anhand der Subjektidentitätsdaten überprüft werden und die im Allgemeinen von kommerziellen Unternehmen und Behörde (öffentliche Verwaltung) als zuverlässig anerkannt wird und die von einer dritten Partei für einen anderen Zweck als der Zertifikatsausstellung durch den Antragsteller erstellt wurde.

C.3 Quellenverzeichnis

[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“

[CP/CPS Class2] CP bzw. CPS der T-TeleSec GlobalRoot Class 2

[CP/CPS DTIRCA1] CP bzw. CPS der Deutschen Telekom Internal Root CA 1

[CP/CPS DTRCA2] CP bzw. CPS der Deutschen Telekom Root CA 2

[ETSI LCP] ETSI EN 319 411-1 V1.1.1 (2016-02), European Telecommunications Standards Institute, „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, policy LCP http://www.cabforum.org/documents.html

[ETSI EN TSP] ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

[EU-DSGVO] Europäische Datenschutz-Grundverordnung 2016/679, in Kraft getreten am 25.05.2018

[ISAE 3402] ISAE3402-Report, International Standards for Assurance Engagements, http://isae3402.com/ISAE3402_reports.html

[PITR cPKI] Personelle, Infrastrukturelle und Technische Rahmenbedingungen der Corporate PKI der DTAG (cPKI)

[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)

[RFC 2560] X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP

[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003

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

[RFC6844] DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013

[RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013

[Siko cPKI] Sicherheitskonzept cPKI

[SRK TC] Sicherheitsrahmenkonzept des Trust-Center-Informationsverbunds

[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), http://www.itu.int/rec/T-REC-X.509/en