OS Corporate PKI
Certificate Policy (CP) & Certification Practice Statement (CPS)

T-Systems International GmbH

Version	1.1
Stand	12.05.2014
Status	freigegeben
Autor	J. Portaro

Geheimhaltungsvermerk: öffentlich

Impressum

Herausgeber
T-Systems International GmbH
CSS, GCU MPHS, PSS
Untere Industriestraße 20, 57250 Netphen

Dateiname	**Dokumentennummer**	**Dokumentenbezeichnung**
CP-CPS_cPKI_v1 0_DRAFT	Dokumentnummer: Datei > Eigenschaften	CP_CPS_CorpPKI NG_V1.1
Version	**Stand**	**Status**
1.1	12.05.2014	freigegeben
Autor	**Inhaltlich geprüft von**	**Freigegeben von**
J. Portaro	Karl-Heinz Rödel Netphen im März 2014	Klaus Jungbluth Netphen im März 2014
Ansprechpartner	**Telefon / Fax**	**E-Mail**
Oliver Stegemann	+49 6151 58 35020	oliver.stegemann@t-systems.com

Kurzinfo

In dem vorliegenden Dokument sind CP und CPS für die Corporate PKI Next Generation (cPKI) beschrieben . Es beschreibt das für den Betrieb der cPKI erforderliche Sicherheitsniveau und beinhaltet Sicherheitsvorgaben sowie Erklärungen hinsichtlich technischer, organisatorischer und rechtlicher Aspekte.

Das Dokument orientiert sich an den dem internationalen Standard für Zertifizierungsrichtlinien RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework der Internet Society.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Certification Practice Statement (CPS) beschreibt konform zu den dokumentierten Prozessen und Funktionen der cPKI Next Generation die wesentlichen Tätigkeiten des T-Systems Trust Center in der Funktion als Zertifizierungs- und Registrierungsstelle. Es ermöglicht die qualitative Beurteilung der angebotenen Dienstleistung und dient als Entscheidungsgrundlage für eine Anerkennung der ausgestellten Zertifikate.

Das vorliegende Dokument orientiert sich an dem internationalen Standard für Zertifizierungsrichtlinien und Erklärungen zum Zertifizierungsbetrieb, dem „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ [RFC3647] der Internet Society (ISOC).

Das vorliegende CPS stellt die Zertifizierungsrichtlinie (engl. Certificate Policy kurz CP) und die Erklärung zum Zertifizierungsbetrieb (engl. Certification Practice Statement, kurz CPS) der cPKI Next Generation dar und beinhaltet Sicherheitsvorgaben sowie Beschreibungen technischer, organisatorischer und rechtlicher Aspekte.

Im Einzelnen behandelt diese CPS die folgenden Regelungen:

- Veröffentlichungen und Verzeichnisdienst,
- Authentifizierung von PKI Teilnehmern,
- Ausstellung von Zertifikaten,
- Erneuerung von Zertifikaten (Re-Zertifizierung),
- Sperrung und Suspendierung von Zertifikaten,
- bauliche und organisatorische Sicherheitsmaßnahmen,
- technische Sicherheitsmaßnahmen,
- Zertifikatsprofile,
- Auditierung,
- verschiedene Rahmenbedingungen.

1.1 Überblick

Im Rahmen von Office Standardization ist mit der CPKi Next generation (cPKI) eine Public Key Infrastructure realisiert, welche sich konform der Internet-Standards (RFC zu LDAP v2 und LDAP v3) verhält. Diese PKI erstellt und verwaltet Zertifikate, welche als elektronische Identitätsnachweise für Mitarbeiter des Konzerns Deutsche Telekom verwendet werden können. Jeder Mitarbeiter des Konzerns Deutsche Telekom erhält durch Verwendung der durch die PKI bereitgestellten Funktionen, die Möglichkeit sich an elektronischen Services zu verlässlich zu identifizieren 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 (siehe auch Anlage 1 Prozessbeschreibung).

Die nachfolgende Tabelle zeigt eine Übersicht der wesentlichen benutzerbezogenen Leistungsmerkmale:

Leistungsmerkmal	**vorhanden**
Signaturzertifikat	X
Verschlüsselungszertifikat	X
Authentifizierungszertifikat	X
Management Zertifikatslebenszyklus	X
Backup und Historie für Verschlüsselungszertifikate und -schlüssel	X
Self-Service Portal für Benutzer	X
Recovery von Verschlüsselungszertifikaten	X

Eine Bereitstellung von Domain-Controller, Server-, Gateway-, Code Signing Zertifikatendurch die cPKI ist derzeit nicht im Leistungsumfang enthalten, jedoch bereits für spätere Ausbaustufen im OS Future Mode of Operation in Planung.

Das vorliegende CPS Dokument bezieht sich dementsprechend auf Personenzertifikate und die hierfür benötigten PKI-Workflow-Prozesse.

Personenzertifikate für interne und externe Mitarbeiter werden grundsätzlich unter Verwendung einer Smart Card (MyCard) als Schlüsselträgermedium ausgegeben. Eine Ausnahme ergibt sich bei Verwendung von Mobile Devices für Verschlüsselungszertifikate von MyCard Nutzern und in diesem Zusammenhang benötigte Zertifikate für eine Authentifizierung an Zielanwendungen, da das Deployment und die Nutzung dieser Zertifikate softwarebasierend (sogenannte Software-PSE) erfolgt.

1.2 Einhaltung der Baseline Requirements des CA/Browser-Forums

Das Trust Center der T-Systems stellt sicher, dass die Sub-CAs Deutsche Telekom Issuing CA 01 die Anforderungen und Regelungen der jeweils aktuellen veröffentlichten Version der [CAB-BR] (http://www.cabforum.org/documents.html) erfüllen und einhalten. Im Falle eines Widerspruchs zwischen dem vorliegendem Dokument und den [CAB-BR], haben die Regelungen aus den [CAB-BR] Vorrang.

1.3 Dokumentenname und Identifikation

Name:	**CP & CPS cPKI**
Version:	1.1
Datum	12.05.2014
Objektbezeich-nung (Object Identifier)	1.3.6.1.4.1.7879.13.26

1.4 PKI Beteiligte

1.4.1 Zertifizierungsstellen

Die Struktur der involvierten Zertifizierungsstellen der cPKI wird in den folgenden Abschnittn vorgestellt.

Das T-Systems Trust Center betreibt die „Deutsche Telekom Root CA 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 genannte Root-CA Instanz zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen. Im Falle der cPKI ist dies die „Deutsche Telekom AG Issuing CA 01“.

Zur Ausstellung von Zertifikaten, für die eine Validierung außerhalb des Telekom Intranets nicht obligatorisch ist, wird im T-Systems Trust Center außerdem die „Deutsche Telekom Internal Root CA 1“ betrieben. Diese zusätzliche Root-CA Instanz zertifiziert die beiden nachgeordneten Instanzen „Deutsche Telekom AG Issuing CA 02“ und „Deutsche Telekom AG Issuing CA 03“.

Zertifizierungshierarchie

Die Struktur der CA-Hierarchie der cPKI ist in der folgenden Abbildung schematisch dargestellt:

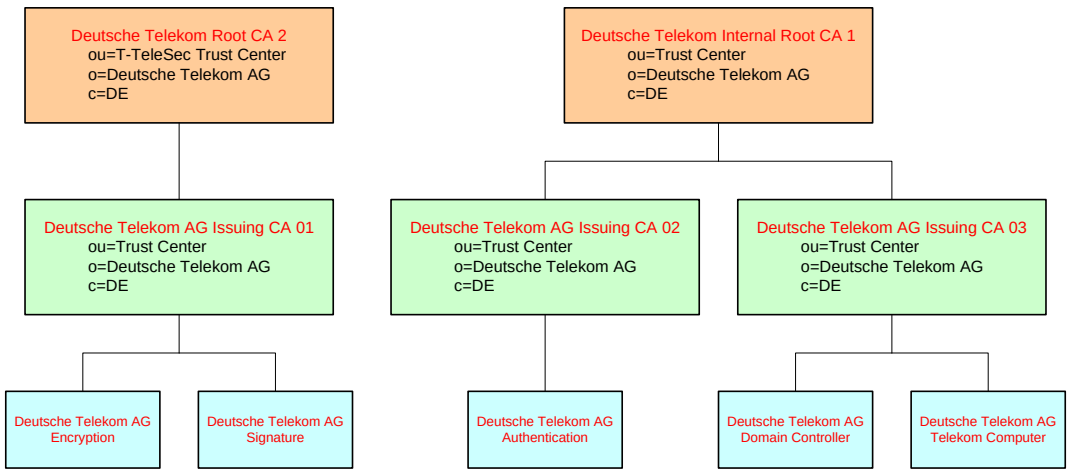

Abbildung 1: CA-Hierachie der cPKI

In der nachfolgenden Tabelle sind die vollständigen Distinguished Names, gemäß den Namensformen nach Abschnitt 3.1.1ff, der genannten Zertifizierungsstellen dargestellt.

Country Name (C)	DE	DE	DE
Organization Name (O)	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
Common Name (CN)	Deutsche Telekom Issuing CA 01	Deutsche Telekom Issuing CA 02	Deutsche Telekom Issuing CA 03
Fingerabdruck-algorithmus	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	a4 65 65 16 29 36 52 fc b2 74 d0 50 88 e1 d4 40 9f ea 5d 70	97 92 1a 0a e2 47 94 52 13 16 40 75 e1 28 1f 38 26 2d 11 82

Relevant für die weitere Betrachtung betreffend der Einhaltung der Baseline Requirements des CA/Browser Forums ist lediglich die Deutsche Telekom Issuing CA 01, da nur diese von einer Web-Trust zertifizierten Stammzertifizierungsstelle, der „Deutschen Telekom Root CA 2“, ausgestellt wurde.

1.4.2 Registrierungsstellen

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. Die Zertifizierungsstellen Deutsche Telekom Issuing CA 01, die Deutsche Telekom Issuing CA 02 und die Deutsche Telekom CA 03 verfügen über eine automatisierte Registrierungsstelle mit einer Schnittstelle zum Provisionierungssystem TAdmin2, sowie zum Verzeichnisdienst Corporate Active Directory.

Zusätzlich hierzu verfügt die Telekom Issuing CA 01 über eine manuell betriebene Registrierungsstelle, welche aufgrund unternehmensrechtlicher Gegebenheiten (Unternehmenssicherheit, gesetzliche Anforderungen) Kopien von Verschlüsselungszertifikaten und -schlüsseln von Zertifikatsinhabern für autorisierte Stellen (vertretende Personen) bereitstellt.

Die Registrierungsstellen erfüllen 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, und

Generierung einer neuen und damit aktuellen Zertifikatssperrliste (CRL).Grundsätzlich muss jede Registrierungsstelle gewährleisten, dass kein unberechtigter Endteilnehmer in den Besitz von privatem Schlüsselmaterial zu Zertifikaten der PKI gelangt.

1.4.3 Endteilnehmer (End Entity)

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

- natürliche Personen (Benutzer, Registratoren, Rolleninhaber, Pseudonym),
- Personen- und Funktionsgruppen,
- Geräte (z.B. Server, Router, Gateways, Mail-Gateways, Domain-Controller, Firewalls oder andere Geräte).

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

Zertifikatstyp	**Endteilnehmer**
Benutzer	natürliche Personen, Personen- und Funktionsgruppen, Rolleninhaber
Funktionspostfächer	Personen- und Funktionsgruppen, Rolleninhaber
Domän Controller	Geräte, juristische Personen
Computer	Geräte, juristische Personen

In den folgenden Abschnittn wird weitestgehend der Namen des Zertifikatstyp als Synonym für den jeweiligen Endteilnehmer verwendet. D.h. unter Benutzer-Zertifikat werden die Zertifikate für natürliche Personen, Personen- und Funktionsgruppen, Rolleninhaber subsummiert, unter Geräte-Zertifikate werden alle Computer- und Domain-Controller-Zertifikate verstanden!

Im Gegensatz zu natürlichen Personen stimmt im Falle von juristischen Personen und Geräten das Subjekt (Zertifikatantragssteller) nicht mit dem Endteilnehmer überein, auf das sich das Zertifikat bezieht. Das Subjekt ist entweder der Zertifikatnehmer oder ein Gerät, das der Kontrolle des Zertifikatnehmers untersteht oder von diesem betrieben wird. Der Endteilnehmer ist Inhaber des privaten und öffentlichen Schlüssels und trägt die

letztendliche Verantwortung für den Gebrauch des Zertifikats. Im Falle von natürlichen Personen stellt der Endteilnehmer gleichzeitig auch das Subjekt dar.

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

1.4.4 Vertrauender Dritter (Relying Parties)

Ein vertrauender Dritter (Relying Parties) ist eine natürliche Person oder Subjekt, die/das sich auf die Vertrauenswürdigkeit des von der cPKI ausgestellten Zertifikats 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.

1.4.5 Weitere Teilnehmer

Eine Personen- und Funktionsgruppe, juristische Person als auch Gerät wird durch eine autorisierte Person repräsentiert, die vom Mandanten bevollmächtigt ist. Die autorisierte Person wird wie eine natürliche Personen identifiziert und registriert und ist verantwortlich für die sichere Verteilung, Nutzung und ggf. Sperrung des Zertifikats. Im Falle, dass die autorisierte Person nicht für die Verteilung oder Sperrung verantwortlich sein soll, wird diese Funktion auf den Rolleninhaber „Schlüsselverantwortlichen“ übertragen.

1.5 Zertifikatsverwendung

1.5.1 Zulässige Zertifikatsverwendung

Die von der Corporate PKI zur Verfügung gestellten Zertifikate werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Attribute („key usage“) zur Zertifikatsschlüsselverwendung und den Festlegungen der Zertifizierungsrichtlinie eingesetzt. 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)

Darüber hinaus dürfen Zertifikate der cPKI nur im Rahmen des geltenden gesetzlichen Rahmens insbesondere auch unter Beachtung länderspezifischer Regelungen (z.B. Ausfuhr- und Einfuhrbestimmungen) verwendet werden.

1.5.2 Unzulässige Zertifikatsnutzung

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

Ferner dürfen Zertifikate für Zertifikatsinhaber (Endteilnehmer) nicht als CA- oder Root-CA-Zertifikate verwendet werden.

1.6 Verwaltung der Richtlinie

1.6.1 Zuständigkeit für die Erklärung

Diese Zertifizierungsrichtlinie wird herausgegeben von:

T-Systems International GmbH
Trust Center Services
Untere Industriestraße 20
57250 Netphen
Deutschland

1.6.2 Kontaktinformationen

T-Systems International GmbH
Trust Center Services
Untere Industriestraße 20
57250 Netphen
Deutschland
Telefon: +49 (0) 1805-268204 1
E-Mail: telesec_support@t-systems.com
Internet: http://www.telesec.de

1.6.3 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb gemäß Zertifizierungsrichtlinie

Siehe Abschnitt 1.6.2.

1.6.4 Verfahren zur Anerkennung von Regelungen für den Zertifizierungsbetrieb (CPS)

Dieses Dokument behält seine Gültigkeit, solange sie nicht von der zuständigen Instanz widerrufen wird. Es wird bei Bedarf fortgeschrieben, die Änderungshistorie wird entsprechend aktualisiert und das Dokument erhält jeweils eine neue, aufsteigende Versionsnummer.

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

Der in Abschnitt 1.6.2 benannte Herausgeber ist für dieses Dokument (CP/CPS) und dessen Freigabe verantwortlich.

Verantwortlich für die Bewertung der Änderungsanforderung als auch Durchführung bzw. die Koordination des Reviews ist der in Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**~~1.6.1~~ benannte Bereich.

1.7 Definitionen und Abkürzungen

Siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**~~Abkürzungsverzeichnis~~ (Glossar).

2 Veröffentlichungen und Verzeichnisdienste

2.1 Verzeichnisdienste (Repositories)

T-Systems betreibt für den Dienst cPKI einen Verzeichnisdienst, eine zentrale Datenablage und ist auch 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 (OCSP-Responder) mit Statusinformationen zu versorgen.

Weiterhin werden für die Öffentlichkeit relevante Dokumente in Form einer zentrale Datenablage (Repository) zur Verfügung gestellt. Dies umfasst insbesondere die entsprechenden CP/CPS der cPKI und CP und/oder CPS-Dokumente der Stamm- und untergeordneten Zertifizierungsstellen (Root- und Sub-CAs). Dieses Verzeichnis ist 7*24 verfügbar.

Die jeweiligen Full Name CDP sind in den jeweils zu überprüfenden Zertifikaten enthalten und können durch eine Applikation aufgerufen werden, siehe auch RFC 5280 Abschnitt 4.2.2.1.

2.2 Veröffentlichung von Zertifikatsinformationen

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

In der Sperrliste für Zertifizierungsstellen (ARL) 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 standard-konformer Sperrlisten (CRL, ARL), für alle PKI-Beteiligten zur Verfügung zu stellen. Der Zugriff auf den Verzeichnisdienst erfolgt über das Protokoll LDAP (Lightweight Directory Access Protocol) und ist hinsichtlich Zugriffsschutz konfigurierbar (öffentlich oder Benutzername/Passwort-Schutz).

Ferner stellt die cPKI einen Validierungsdienst (OCSP-Responder) zur Verfügung, der über das Internetprotokoll „Online Certificate Status Protocol“ (OCSP) agiert und einem Benutzer den Status von X.509-Zertifikaten zurück liefert.

Das Root-CA-Zertifikat der „Deutsche Telekom Root CA 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. Ggf. kann das Zertifikat über den Verzeichnisdienst der cPKI oder per Internet http://www.telesec.de abgerufen werden.

Das Root-CA-Zertifikat der „Deutsche Telekom Root CA 1“ ist in gängigen Zertifikatsspeichern von Betriebssystemen und Applikationen nicht als „Vertrauensanker“ nachinstalliert

sondern wird im INTRANET der DTAG mittels Softwareverteilung auf Arbeitsplatzsystemen installiert.

Die Veröffentlichung der Zwischenzertifizierungsstellen Deutsche Telekom issuing CA 01 – 03 erfolgt deutsche den Root CA´s nachgeordneten Zertifizierungsstellen ist in den nachfolgenden Tabellen dargestellt:

Bereitstellung von Sperrlisten über die Schnittstellen, Web-Applikation, den LDAP-Server der Corporate PKI NG oder das Active Directory der jeweiligen Domäne.

	Deutsche Telekom Issuing CA 01	**Deutsche Telekom Issuing CA 02**	**Deutsche Telekom Issuing CA 03**
CRL Distribution Points (CDP)			
• **CDP [1] http**	URL=http://corporate-pki.telekom.de/cdp/Deutsche Telekom AG Issuing CA 01.crl	URL=http://corporate-pki.telekom.de/cdp/Deutsche Telekom AG Issuing CA 02.crl	URL=http://corporate-pki.telekom.de/cdp/Deutsche Telekom AG Issuing CA 03.crl
• **CDP [2] ldap**	URL=ldap://corporate-pki.telekom.de/CN=Deutsche Telekom AG Issuing CA 01,OU=Trust Center,O=Deutsche Telekom AG,C=DE?certificateRevocationList	URL=ldap://corporate-pki.telekom.de/CN=Deutsche Telekom AG Issuing CA 02,OU=Trust Center,O=Deutsche Telekom AG,C=DE?certificateRevocationList	URL=ldap://corporate-pki.telekom.de/CN=Deutsche Telekom AG Issuing CA 03,OU=Trust Center,O=Deutsche Telekom AG,C=DE?certificateRevocationList
• **CDP [3] AD**	URL=ldap:///CN=Deutsche Telekom AG Issuing CA 01,CN=HE101039,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint	URL=ldap:///CN=Deutsche Telekom AG Issuing CA 02,CN=HE101040,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint	URL=ldap:///CN=Deutsche Telekom AG Issuing CA 03,CN=HE101038,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
Deutsche Telekom AG Employee Encryption	X	-	-
Deutsche Telekom AG Employee Signature	X	-	-
Deutsche Telekom AG Employee Authentication	-	X	-
Deutsche Telekom AG External Workforce Encryption	X	-	-

Deutsche Telekom AG External Workforce Signature	X	-	-
Deutsche Telekom AG External Workforce Authentication	-	X	-
Deutsche Telekom AG Telekom Computer	-	-	X
Deutsche Telekom AG Domain Controller	-	-	X

Tabelle 1: Zuordnung der Zertifikate zu den CAs und den jeweiligen CRL Distribution Points

Bereitstellung von Zertifikatsstatusdaten über das OCSP-Protokoll

	Deutsche Telekom Issuing CA 01	**Deutsche Telekom Issuing CA 02**	**Deutsche Telekom Issuing CA 03**
Authority Information Access (AIA)			
• **AIA [1] http**	URL=http://corporate-pki.telekom.de/aia/Deutsche Telekom AG Issuing CA 01.crt	URL=http://corporate-pki.telekom.de/aia/Deutsche Telekom AG Issuing CA 02.crt	URL=http://corporate-pki.telekom.de/aia/Deutsche Telekom AG Issuing CA 03.crt
• **AIA [2] ldap**	URL=ldap://corporate-pki.telekom.de/CN=Deutsche Telekom AG Issuing CA 01,OU=Trust Center, O=Deutsche Telekom AG,C=DE?cACertificate	URL=ldap://corporate-pki.telekom.de/CN=Deutsche Telekom AG Issuing CA 02,OU=Trust Center, O=Deutsche Telekom AG,C=DE?cACertificate	URL=ldap://corporate-pki.telekom.de/CN=Deutsche Telekom AG Issuing CA 03,OU=Trust Center, O=Deutsche Telekom AG,C=DE?cACertificate
• **AIA [3] AD**	URL=ldap:///CN=Deutsche Telekom AG Issuing CA 01,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base?objectClass=certificationAuthority	URL=ldap:///CN=Deutsche Telekom AG Issuing CA 02,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base?objectClass=certificationAuthority	URL=ldap:///CN=Deutsche Telekom AG Issuing CA 03,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base?objectClass=certificationAuthority
Deutsche Telekom AG Employee Encryption	X	-	-
Deutsche Telekom AG Employee Signature	X	-	-

Deutsche Telekom AG Employee Authentica-tion	-	X	-
Deutsche Telekom AG External Workforce Encryption	X	-	-
Deutsche Telekom AG External Workforce Signature	X	-	-
Deutsche Telekom AG External Workforce Authentication	-	X	-
Deutsche Telekom AG Telekom Computer	-	-	X
Deutsche Telekom AG Domain Controller	-	-	X

Tabelle 2: Zuordnung der Zertifikate zu den CAs und den jeweiligen AIA URIs

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

Quelle	**URI**
LDAP-Server der Corporate PKI der DTAG	ldap://corporate-pki.telekom.de
X.500 Konzernverzeichnis	ldap://X500.telekom.de

Tabelle 3: Schnittstellen zur Bereitstellung der Zertifikate zum Bezug der öffentlichen Schlüssel zur Datenverschlüsselung

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

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Für die Aktualisierung der in Abschnitt *2.2* genanten Informationen gelten folgende Fristen:

- **Zertifikate:** spätestens drei Werktage nach der Ausstellung
- **CP und CPS:** spätestens eine Woche nach Erstellung einer neuen Version
- **CRLs:** siehe Abschnitt 7.2Tabelle 12.

2.4 Zugange zu Verzeichnisdiensten (Repositories)

Der lesende Zugriff auf die in Abschnitt *2.1* und *2.2* aufgeführten Informationen unterliegt für die Zertifikatsinhaber und -prüfer von Zertifikaten im DTAG INTRANET keiner Zugangskontrolle.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

Ein Distinguished Name (DN) ist ein globaler, eindeutiger Name für Verzeichnisobjekte nach dem X.500-Standard. Mit dem Distinguished Name ist eine weltweite eindeutige Unterscheidbarkeit von Personen und Systemen gegeben. Der DN 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 den Abschnittn 1.3.1 ff grafisch dargestellt. Es gelten aber die Namensformen analog zum Subject-DN.

3.1.1 Namensformen

Die Namensregeln für den „SubjectDistinguishedName“ (Subject DN) und „IssuerDistinguishedName“ (Issuer DN) müssen nach dem X.501-Standard definiert sein.

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

Für alle Zertifikatstypen müssen zumindest die folgenden Felder ausgefüllt sein:

- Country Name (C)
- Organization Name (O)

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

3.1.2 Aussagekraft von Namen

Der Name muss den Endteilnehmer bzw. Zertifikatsnehmer mit allgemein verständlicher Wortbedeutung enthalten, als auch eindeutig und nachprüfbar sein. Die Eindeutigkeit der Namensangaben ist über den gesamten Subject DN betrachtet sichergestellt (Voraussetzung: UPN oder Email-Adressen kommen im Subject-DN vor).

3.1.3 Anonymität bzw. Pseudonyme für Zertifikatsinhaber

Pseudonyme werden nicht vergeben bzw. nicht akzeptiert.

3.1.4 Regeln zur Interpretation verschiedener Namensformate

Keine Bestimmungen.Abschnitt

3.1.5 Eindeutigkeit von Namen

Für Benutzer können ein, zwei oder drei Zertifikate mit demselben eindeutigen Subject-DN ausgestellt sein, die sich jedoch in der Schlüsselverwendung bzw. erweiterten Schlüsselverwendung (z.B. Signatur, Schlüsselverschlüsselung, Client-Authentifizierung, Smartcard-Anmeldung) und der Zertifikatsseriennummer unterscheiden. Durch die Erneuerungsfunktion können zeitlich begrenzt auch mehrere Zertifikate mit dem gleichen Subject-DN erstellt sein. Zertifikate für Geräte mit gleichem Subject-DN können mehrfach vorkommen.

Siehe Abschnitt auch *3.1.2*.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Es liegt in der Verantwortung des Mandanten, dass die Namenswahl keine Warenzeichen, Markenrechte usw. oder Rechte des geistigen Eigentums verletzen. Die Zertifizierungsstelle der cPKI ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Mandanten.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes 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. In diesem Fall ist die Zuordnung zwischen öffentlichem und geheimem Schlüssel implizit gegeben.

3.2.2 Authentifizierung einer Organisation

Grundvoraussetzung für einen Neuauftrag ist die Konzernzugehörigkeit einer Organisation oder ein definiertes Vertragsverhältnis zu einer externen Organisation.

Die cPKI stellt bei der Authentifizierung von Organisationen sicher, dass verwendete Namen geprüft werden. Die cPKI führt folgende Prüfungen durch:

- Feststellung der Existenz der Organisation durch entsprechende aktuelle Organisationsdokumente der DTAG, 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.

3.2.3 Authentifizierung der identität von Endteilnehmern

Die Zertifizierungsstelle nimmt in geeigneter Weise eine zuverlässige Überprüfung derjenigen Auftragsdaten vor, die in das Zertifikat eingehen. Given name, surname und email sind in den Bezugssystemen für die PKI (TAdmin2 und Corporate AD) hinterlegt und werden durch diese der PKI bereitgestellt.

Der Ursprung dieser Daten liegt im SAP HR System, welches von den für die Personalverwaltung zuständigen Stellen innerhalb der Organisation des Konzerns Deutsche Telekom bedient wird. 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. Das CIAM System ergänzt diese Stammdatensätze im Zusammenspiel mit den Systemen Corporate AD, TAdmin2 und Corporate Exchange um weitere benötigte Datenattribute wie Corporate ID, AD-Accountdaten, Email-Adresse(n) und Attribute für Applikationsrollen (Shop, MyWorkplace, MyPortal, …). 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 dementsprechend auf einer Anwendung definierter Prozesse in der Personalverwaltung des Konzerns Deutsche Telekom sowie der Sicherheit von Systemen welche Daten für die Erzeugung und Verwaltung von X.509 Zertifikaten erzeugen, verarbeiten, ablegen und bereitstellen.

Eine Übersicht der Systeme, welche im Kontext der cPKI und der Authentifizierung von natürlichen Personen als Benutzern zu betrachten sind, zeigt die nachfolgende Grafik.

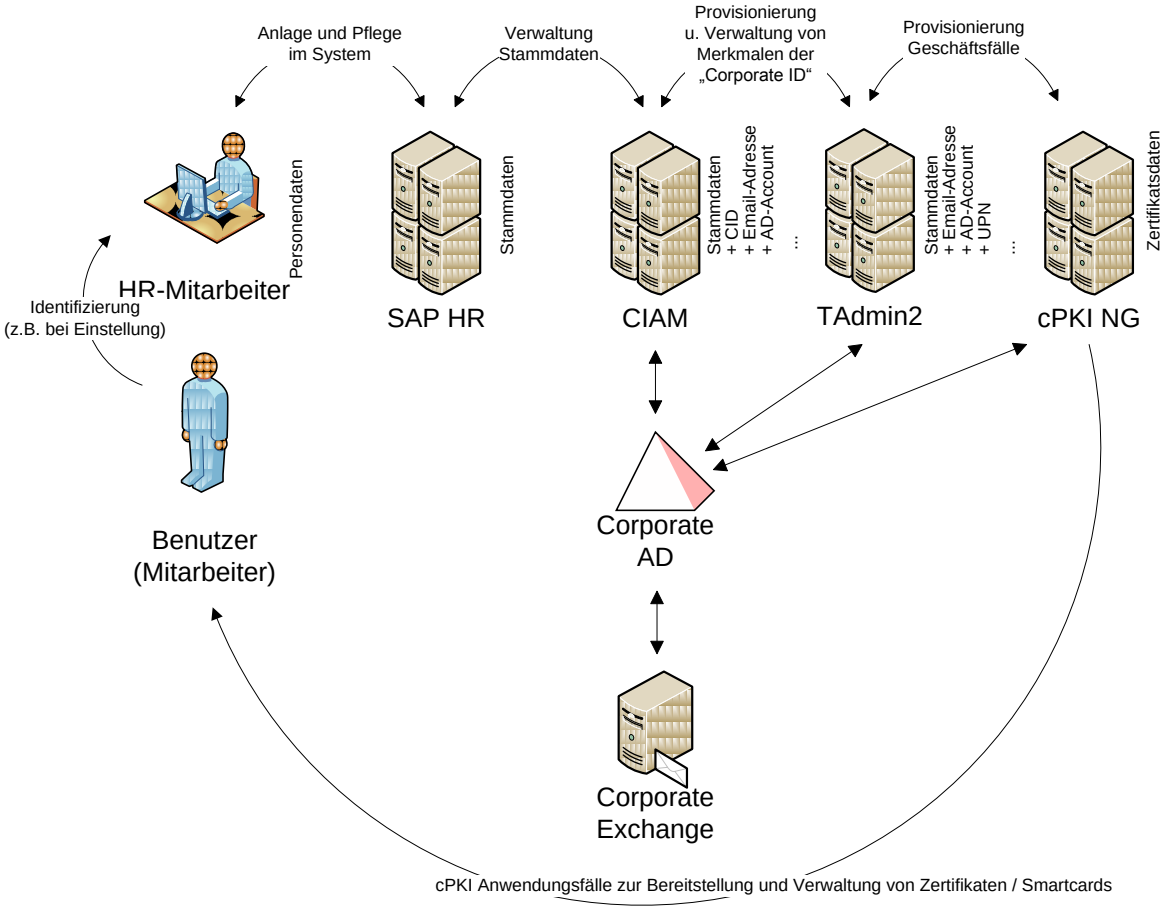

Abbildung 2: Authentifizierung einer natürlichen Person

Auf eine detailliertere Beschreibung des Registrierungsmodells wird an dieser Stelle auf das Dokument „E2E Beschreibung Registrierungsprozess“ verwiesen.

3.2.4 Nicht überprüfte Teilnehmerangaben

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

Nicht relevant, da alle Informationen, welche die cPKI erhält, aus den Backend-Systemen TAdmin2, Corporate-AD, CIAM oder SAP HR der Deutschen Telekom bereitgestellt werden.

3.2.5 Überprüfung der Berechtigung

Ein Benutzer ist zum Erhalt von Zertifikaten berechtigt, wenn er einen gültigen Arbeitsvertrag besitzt oder eine definierte Vertragsbeziehung besteht (external Workforce) und in den Backend-Systemen (SAP HR, CIAM, Corporate-AD, TAdmin2) administriert ist.

Der Kunde teilt dem Betreiber der cPKI die Domänen mit, auf die Zertifikate ausgestellt werden sollen, damit T-Systems diese nach Prüfung als „erlaubte Domänen“ in die PKI-Konfiguration der cPKI aufnehmen und pflegen kann. Änderungen dieser Domänen sind zwingend schriftlich T-Systems anzuzeigen.

Zur Erfüllung und Einhaltung der [CAB-BR] wird T-Systems spätestens nach 39 Monaten eine vollständige Whitelist aller erlaubten Domänen beim Kunden anfordern. Der Betreiber der cPKI T-Systems behält sich vor, aktuelle Identifikationsdokumente des Inhabers einer Domäne zu dessen Lasten anzufordern.

3.2.6 Interoperabilitätskriterien

Die Interoperabilität von Zertifikaten der PKI basiert auf gängigen Markt-Standards für Zertifikatsprofile (X.509v3, RFC 5280), Sperrlistenprofile (RFC 5280, Validierungsdiensten, CRL, OCSP).

Verwendet eine CA der cPKI, welche von der „Deutsche Telekom Root CA 02“ ausgestellt wurde in einem von ihr signierten Zertifikat eine Policy-OID, welche die Erfüllung und Einhaltung der [CAB-BR] repräsentiert (siehe Abschnitt 7.1.6.2), muss das jeweilige CP oder CPS der CA eine explizite Zusicherung enthalten, dass alle von dieser CA ausgestellten Zertifikate, welche diese Policy OID enthalten, in Übereinstimmung mit und Einhaltung von den [CAB-BR] ausgestellt und verwaltet werden.

Unter der „Deutsche Telekom Issuing CA 01“ werden keine weiteren Sub-CA Zertifikate ausgestellt.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

Um durchgehend 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 Schlüsselmaterial (Smartcard, Soft-PSE).

Schlüsselerneuerung für Smartcard

Bei einer Folgebeantragung kann die gleiche Smartcard mit den darauf befindlichen Schlüsselpaar verwendet werden. Andernfalls ist ein Folge-Zertifikat auf einer neuen Smartcard auszustellen. Es gelten die Regelungen der Registrierung wie in den Abschnitt 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.

3.3.1 Routinemäßige Zertifikatserneuerung

Zur Folge-Beauftragung muss die Identitätsprüfung wie bei Neuauftrag durchlaufen werden siehe 3.2.3, dabei werden für alle Verwendungszwecke neue Zertifikate ausgestellt. Darüber hinaus werden für den Verwendungszweck Verschlüsselung neue kryptographische Schlüssel erzeugt.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Zur Folge-Beauftragung nach einer Sperrung (Replace) muss die Identitätsprüfung wie bei Neuauftrag durchlaufen werden siehe 3.2.3, dabei werden für alle Verwendungszwecke

neue Zertifikate ausgestellt. Darüber hinaus werden für den Verwendungszweck Verschlüsselung neue kryptographische Schlüssel erzeugt..

3.4 Identifizierung und Authentifizierung von Sperraufträgen

Das T-Systems Trust Center bietet einen zentralen Sperrservice, um im Falle des Verlustes eines Schlüsselträgermediums (MyCard oder Software-PSE) oder bei unbefugtem Nutzungsverdacht Zertifikate sperren zu können. Im Falle der Sperrung wird das Zertifikat in eine Sperrliste aufgenommen. Der Sperrwunsch wird mittels einer im System durch den Zertifikatsinhaber hinterlegte Frage bzw. Antwort autorisiert.

Die Sperrung von Zertifikaten kann über das Self Service Portal der cPKI oder telefonisch beauftragt werden. Für eine telefonische Erteilung von Sperraufträgen sind die innerhalb des Konzerns DTAG kommunizierten Eingangskanäle des jeweils zuständigen Help-Desk zu verwenden.

4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsantrag

4.1.1 Wer kann Zertifikate beantragen

Zertifikate können durch

- natürliche Personen (interne oder externe Mitarbeiter der DTAG mit aktivem Vertrag) und
- Organisationen, vertreten durch handlungsbevollmächtigte DTAG Mitarbeiter (z.B. Inhaber von Funktionspostfächern oder Server-Administratoren)

beantragt werden.

4.1.2 Registrierungsprozess und Verantwortlichkeiten

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

Beteiligt sind daran:

- SAP HR Personalverwaltungssystem (HR-Systeme),
- CIAM als Identity & Access Management-System,
- Corporate Active Directory als zentrales Bezugsdirectory für die PKI,

und

- TAdmin2 als Provisionierungsplattform für die PKI.

Konkret bedeutet dies, dass die Verarbeitung der Registrierungsdaten sowie deren Verifikation bereits in/durch die Vorsysteme (siehe oben) geschehen ist. Auf Basis dieser Daten erfolgt danach die Ausstellung von Zertifikaten.

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

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Die Authentifizierung der Endteilnehmer erfolgt im Rahmen der etablierten HR-Prozesse durch Stellen des Personalmanagements im Konzern DTAG (siehe Abschnitt 3.2.3)

Subjektdaten von Zertifikaten basieren auf dem Datenbestand der Personaldatenbank SAP HR, welche um zusätzliche Informationen (z.B. Email-Adresse, User GUID) durch Systeme wie CIAM oder das Corporate AD ergänzt werden.

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 Kontrolle ausübt bzw. es betreibt.

Die cPKI nimmt 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 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 ist der Endteilnehmer pro-aktiv aufgefordert wird, die Existenz seiner Mail-Adresse zu bestätigen. Darüber hinaus wird der Domänenteil der Mail-Adresse (optional auch der UPN) auf die in der PKI-Konfiguration eingetragenen „erlaubten Internet-Domänen“ geprüft.

Für Geräte-Zertifikate ist, abhängig vom Zertifikatstyp, der Domänenteil der 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.

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 Corporate Active Directory geprüft.

Abschnitt

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

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

4.2.3 Zeit zur Verarbeitung von Zertifikatsaufträgen

Die Bearbeitung des Zertifikatauftrags beginnt innerhalb eines angemessenen Zeitraums nach Erhalt der Beauftragung. Die maximale Bearbeitungsdauer beträgt 20 Tage. Sollte ein Teilnehmer bis zum Ende dieser Frist seine Zertifikate nicht abgerufen haben, wird der entsprechende Auftrag storniert.

4.3 Zertifikatsausstellung

4.3.1 Aufgaben der Zertifizierungsstelle

Nach der Genehmigung durch die Registrierungsstelle prüft das CA-System den Zertifikatsantrag auf die in der PKI-Konfiguration eingetragenen „erlaubten Email~~Internet~~-Domänen“. Im Falle der 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 verhindert und TAdmin2 als antragstellende Instanz informiert.

4.3.2 Benachrichtigung des Antragstellers

Der Zertifikatsinhaber oder Vertreter erhält eine Benachrichtigung in Form einer E-Mail. In dieser E-Mail enthalten ist eine URL und ein OTP (One-Time Password = Einmalpasswort).

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

Die Karte 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.

4.4 Akzeptanz der Zertifikate

4.4.1 Annahme durch den Zertifikatsinhaber

Der Zertifikatsinhaber ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt zu verifizieren.

Ein Zertifikat wird durch den Zertifikatsinhaber akzeptiert, wenn das Zertifikat verwendet wird oder wenn innerhalb von 14 Tagen nach Erhalt kein Widerspruch erfolgt. Durch Annahme des Zertifikats erkennt der Zertifikatsinhaber die Regelungen des vorleigenden 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

Jedes Zertifikat (interne Mitarbeiter, external Workforce, Funktionspostfächer) wird im Corporate Active Directory als zentrales Bezugsdirectory für die PKI, sowie in einem internen Veröffentlichungsserver (LDAP) veröffenlicht.

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Benachrichtigungen an weitere Instanzen (z.B. Information bei Neuausstellung eines Zertifikates an Vertreter oder Funktionsgruppenmitglieder) erfolgen per E-Mail und sind per Konfigurationseinstellung änderbar.

4.5 Schlüssel- und Zertifikatsverwendung

4.5.1 Nutzung durch den Zertifikatsinhaber

Die Verwendung des privaten Schlüssels, mit dem dazu gehörigen zertifizierten öffentlichen Schlüssel, ist erst gestattet, nachdem der Endteilnehmer das Zertifikat angenommen hat (Abschnitt 4.4.1~~3.8.1~~). Die Zertifikatsnutzung wird durch das Attribut „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ im Zertifikat 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 Geräten gelten darüber hinaus folgenden Anforderungen:

- Der Schlüsselverantwortliche (Abschnitt 1.3.3) ist für das Kopieren bzw. Weitergeben der Schlüssel an den/die Endteilnehmer verantwortlich.
- Zertifikatssperrungen können auf Personen aus dem Kreise der Endteilnehmer übertragen werden. Der Schlüsselverantwortliche muss dem/den Sperrberechtigten die Details zu Sperranlässen und das Sperrpasswort 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 gesperrt wird.
- Eine Übertragung der Verantwortung an einen neuen oder zusätzlichen Schlüsselverantwortlichen ist bei der zuständigen Registrierungsstelle zu beantragen und zu dokumentieren. Der neue Schlüsselverantwortliche ist gemäß dieser Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) zu identifizieren und zu registrieren, seine Autorisierung als Schlüsselverantwortlicher muss nachgewiesen werden.

Eine Sperrung des Zertifikats ist umgehend vorzunehmen, wenndie Angaben im Zertifikat nicht mehr korrekt sind oder der private Schlüssel abhanden gekommen, kompromittiert oder gestohlen wurde.

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 (Zertifizierungs-

hierarchie), 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)

Sofern keine Gründe entgegen sprechen, muss der Benutzer vor Ablauf eines gültigen Zertifikats sich ein neues Zertifikat beschaffen, um die Kontinuität der Zertifikatsnutzung gewährleisten zu können.

Eine Zertifikatserneuerung ist nur innerhalb von 20 Kalendertage vor Ablauf der Gültigkeit des vorhandenen Zertifikats möglich.

4.6.1 Gründe für eine Zertifikatserneuerung

Bei einer Zertifikatserneuerung wird dem Zertifikatsnehmer ein neues Zertifikat mit neuer Seriennummer, neuem Gültigkeitszeitraum und gleichen Subject-DN (Abschnitt 3.1) ein neues Zertifikat ausgestellt.

Eine Zertifikatserneuerungsfunktion ist nur für Benutzer-Zertifikate implementiert. Für andere Zertifikatstyp bedarf es einer Zertifikatsneubeantragung, auch wenn dazu auf die ursprünglichen technischen Requestdaten zurückgegriffen wird.

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

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Eine Zertifikatserneuerung darf nur der Benutzer oder Schlüsselverantwortliche beauftragen.

4.6.3 Ablauf der Zertifikatserneuerung

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. Mit der Erneuerung wird das zu erneuernde Endteilnehmer-Zertifikat automatisch gesperrt. Damit wird ausgeschlossen, dass der Endteilnehmer über zwei gültige Zertifikate verfügen kann. Darüber hinaus gelten die Regelungen ausAbschnitt Abschnitt *3.3*.

4.6.4 Benachrichtigung des Antragstellers nach Zertifikatserneuerung

Es gelten die Regelungen gemäß AbschnittAbschnitt *4.3.2*.

4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß AbschnittAbschnitt 4.4.1.

4.6.6 Veröffentlichungen der erneuerten Zertifikate durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß AbschnittAbschnitt *4.4.2*.

4.6.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß AbschnittAbschnitt 4.4.3

4.7 Schlüssel- und Zertifikatserneuerung (Re-key)

Die Schlüsselerneuerung von Zertifikaten stellt eine Antragsform zur Ausstellung eines neuen Zertifikats unter Verwendung eines neuen öffentlichen Schlüssels dar.

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. Abschnitt

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen?

Es gelten die Regelungen von Abschnitt*4.6.2*.

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

Es gelten die Regelungen von Abschnitt *3.3 und 4.6.3*.

4.7.4 Benachrichtigung des Zertifikatsinhabers

Es gelten die Regelungen gemäß Abschnitt *4.3.2*.

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Es gelten die Regelungen gemäß Abschnitt *4.4.1.*

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Abschnitt *4.4.2*.

4.7.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Abschnitt 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Gründe für Zertifikatsänderung

Eine Modifikation einmal ausgestellter Zertifikate ist nicht vorgesehen. Wenn sich Inhalte von Attributen des Zertifikats ändern, ist eine erneute Identifizierung, Registrierung und Zertifikatsausstellung (z.B. Online Update, Detail Changes) erforderlich. Eine Änderung von Inhalten von Zertifikaten führt somit in jedem Falle zu einer Neuausstellung von Zertifikaten. Die Inhalte dieser Zertifikate, insbesondere Daten des Zertifikatsinhabers, werden in den Bezugssystemen SAP HR, CIAM, Corporate AD und TAdmin2 vorgehalten und gemäß der definierten Prozesskette für die cPKI bereitgestellt, siehe auch 3.2 und 4.1.2.

4.8.2 Wer kann eine Modifikation eines Zertifikates beantragen?

Es gelten die Regelungen gemäß Abschnitt 4.6.2.Abschnitt

4.8.3 Ablauf der Zertifikatsmodifizierung

Wenn sich Zertifikatsinhalte ändern, ist eine erneute Authentifizierung wie im Falle der Erst-Beauftragung erforderlich (siehe 3.2). Das vorhergehende Zertifikat ist umgehend zu sperren.Abschnitt

4.8.4 Benachrichtigung des Zertifikatsinhabers

Es gelten die Regelungen gemäß Abschnitt *4.3.2*.

Abschnitt

4.8.5 Annahme der Zertifikatsmodifizierung

Es gelten die Regelungen gemäß Abschnitt *4.4.1.*

Abschnitt

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Abschnitt *4.4.2*.

Abschnitt

4.8.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Abschnitt 4.4.3.

Abschnitt

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für Widerruf/Sperrung

Die folgenden Gründe des Zertifikatsinhabers müssen zu einer Sperrung des Zertifikats führen:

- Abhandenkommen des privaten Schlüssels (z.B. Verlust oder Diebstahl).
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor.
- Die Angaben im Zertifikat sind nicht mehr korrekt.
- Verwendung und Handhabung des Zertifikats ist im Widerspruch zu vertraglichen Regelungen oder der CP/CPS des Zertifikatsinhabers oder Zertifikatsgebers.
- Ein Unbefugte Nutzung oder Verdacht auf Unbefugte Nutzung durch den Zertifikatsinhaber oder andere zur Nutzung des Schlüssels berechtigte Personen.
- Der Zertifikatsinhaber benötigt kein Zertifikat mehr und kündigt daher das Vertragsverhältnis (Sperrung erfolgt 30 Tage nach Kündigung).
- Gesetzliche Vorschriften oder richterliche Urteile begründen eine Zertifikatssperrung.
- Der Prozess Suspend wurde angestoßen und der Zertifikatsinhaber wird nach einer Suspendierungsdauer von 30 Tagen endgültig gesperrt.

Die folgenden Gründe des T-Systems Trust Centers führen zu einer Sperrung des Zertifikats:

- Bekanntwerden, dass das Zertifikat nicht in Übereinstimmung mit dem zum jeweiligen Zeitpunkt gültigen Version der Baseline Requirements oder dem vorliegenden Dokument (CP/CPS) ausgestellt wurde.
- Abhandenkommen des privaten Schlüssels (z.B. Verlust oder Diebstahl).
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor.
- Über die im Vertrag vereinbarten Zahlungsfristen hinaus gehender, erheblicher Zahlungsverzug des Auftraggebers (Kunde) der cPKI.
- Bei Feststellung, dass für die Ausstellung des Zertifikats eine wesentliche Voraussetzung nicht erfüllt war oder auf deren Erfüllung verzichtet wurde.
- Die Zertifizierungsstelle stellt den Betrieb ein und die Fortführung des Sperrservice (CRL/OCSP) ist nicht gewährleistet.
- Es liegt ein Unbefugte Nutzung oder Verdacht auf Unbefugte Nutzung durch den Zertifikatsinhaber oder andere zur Nutzung des Schlüssels berechtigte Personen vor.
- Vertragsbeendigung bzw. -kündigung zwischen dem Kunden und T-Systems als Auftragnehmer für den Betrieb der cPKI, sofern nichts anderes vereinbart ist.
- Der technische Inhalt, das Format oder die verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen, bildet ein nicht akzeptables Risiko (z.B. wenn Algorithmen vom CA/Browser Forum missbilligt oder untersagt werden).
- Die Berechtigung der Zertifizierungsstelle zur Ausstellung von Zertifikaten im Rahmen der Baseline Requirements läuft aus, wird beendet oder entzogen und die Fortführung des Sperrservice (CRL/OCSP) ist nicht gewährleistet.

4.9.2 Wer kann Widerruf/ Sperrung beantragen?

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

- 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 (z.B. Mitarbeiter des T-Systems Trust Center).

4.9.3 Ablauf von Widerruf / Sperrung

Zur Sperrung autorisierte Personen können die Sperrung eines Zertifikates entweder über die Self-Service Web-Seite der cPKI oder telefonisch beauftragen. Die Authentisierung und Autorisierung einer Person geschieht dabei in geeigneter Art und Weise (z.B. Smartcard basierte Anmeldung auf einem Web-Portal oder 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 Sperrinformationen übernommen. Die Sperrinformationen werden in standardkonformer Weise (CRL) bereitgestellt.

Der Zertifikatsinhaber wird über die Durchführung der Sperrung in geeigneter Weise (via 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 Abschnitt 4.9.1 aufgeführten Sperrgründe, zu sperren.

4.9.4 Fristen für einen Sperrauftrag

Bei Vorliegen von Gründen für eine Sperrung (siehe Abschnitt *4.9.1*), muss unverzüglich ein Sperrantrag gestellt werden. Nach Eingang eines bearbeitbaren Sperrauftrags ergreift T-Systems wirtschaftlich angemessene Schritte, um den Sperrauftrag unverzüglich zu bearbeiten.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Eine Zertifikatssperrung muss durch die CA unverzüglich vorgenommen werden, wenn die Voraussetzungen dafür vorliegen (siehe Abschnitt 4.9.3). Die Sperrfunktion über das Web-Portal der cPKI steht 7*24 zur Verfügung und gibt unmittelbar nach einer erfolgten Sperrung entsprechende Informationen an angeschlossen Verzeichnisdienste weiter. Der OCSP-Dienst, der auf diese Systeme zugreift, verfügt darüber hinaus ebenfalls über den jeweils 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-Zertifikates anzeigt.

Eine weitere Methode, der Validierung eines Endteilnehmer-Zertifikatsstatus, ist die Prüfung der aktuellen Zertifikatssperrliste (CRL), die auf dem Verzeichnisdienst der cPKI veröffentlicht wird (siehe Abschnitt 2.2).

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

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

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

Die Zertifikatssperrliste (CRL), in der Zertifikats-Sperrungen von Endteilnehmern aufgeführt sind, wird mindestens ein Mal pro Tag automatisch vom CA-System aktualisiert und über den Verzeichnisdienst veröffentlicht.

In den Sperrlisten für Zertifizierungsstellen (ARL) werden alle gesperrten CA-Zertifikate (keine Root-CA-Zertifikate!) veröffentlicht, die von der jeweiligen Stammzertifizierungsstelle (Root-CA) ausgestellt wird.

Die Aktualisierung der ARL erfolgt alle sechs (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 vier (4) Tagen aktualisiert. Die OCSP-Antworten haben eine maximale Gültigkeit von zehn (10) Tagen.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Latenzzeit der Zertifikatssperrliste (CRL) nach automatischer Generierung beträgt wenige Minuten.

Die Latenzzeit für Zertifizierungsstellen-Sperrliste (ARL) nach manueller Veröffentlichung beträgt wenige Minuten.

4.9.9 Online Verfügbarkeit von Sperr-Statusinformationen

Zusätzlich, zu den Sperrinformationen über CRL und ARL, 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)“ aufgeführt, siehe auch Abschnitt 2.2.

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 Formen der Veröffentlichung von Sperrinformationen

Derzeit werden keine anderen Formen der Bekanntmachung eingesetzt.

4.9.12 Anforderungen bei Kompromittierung privater Schlüssel

Bei einer bekanntwerdenden Kompromittierung eines privaten Schlüssels von Zertifikatsinhabern ist das entsprechende Zertifikat unverzüglich zu sperren.

Bei einer bekanntwerdenen Kompromittierung des privaten Schlüssels einer CA werden alle von ihr ausgestellten Zertifikate durch das T-Systems Trust Center unverzüglich gesperrt.

4.9.13 Suspendierung von Zertifikaten

Gründe für die Suspendierung von Zertifikaten können

- 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 „Delete User“ im System TAdmin2 bzw. im Corporate Active Directory sein, woraufhin der User für 30 Tage suspendiert wird, bevor er endgültig gelöscht wird.

4.9.14 Wer kann eine Suspendierung beantragen?

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

- 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 (z.B. Mitarbeiter des T-Systems Trust Center).

4.9.15 Ablauf einer Suspendierung

Zur Suspendierung autorisierte Personen können die temporäre Sperrung eines Zertifikates entweder über die Self-Service Web-Seite der cPKI oder telefonisch beauftragen. Die Authentisierung und Autorisierung einer Person geschieht dabei in geeigneter Art und Weise (z.B. Smartcard basierte Anmeldung auf einem Web-Portal oder 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 Sperrinformationen übernommen. Die Sperrinformationen werden in standardkonformer Weise (CRL) bereitgestellt.

Der Zertifikatsinhaber wird über die Durchführung der Sperrung in geeigneter Weise (via 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 Abschnitt 4.9.13 aufgeführten Sperrgründe, zu sperren.

Beschränkung des SuspendierungszeitraumsDie maximale Sperrdauer einer Suspendierung beträgt 30 Kalendertage kann, abhängig von der Zertifikatsgültigkeit verkürzt werden. Insofern die Zertifikatsgültigkeit nicht abgelaufen ist, erfolgt nach Ablauf von 30 Kalendertagen eine endgültige Sperrung durch die cPKI.

4.10 Statusabfrage von Zertifikaten (OCSP, CRL

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

4.10.1 Betriebseigenschaften

Die von der cPKI ausgegebenen OCSP-Antworten von Endteilnehmer-Zertifikaten entsprechen den Vorgaben des RFC 2560. Die OCSP-Antworten werden von einem OCSP-Responder signiert, dessen Zertifikat seinerseits von dem jeweiligen Signer der Sub-CA signiert wurde, welche das betreffende Endteilnehmer-Zertifikat ausgestellt hat. Das Zertifikat des OCSP-Responders enthält die in Kapitel 7.3.2 beschriebenen Erweiterungen.

Die von der cPKI ausgegebenen Zertifikatssperrlisten (CRL) entsprichen den Vorgaben des RFC 5280. Die Zertifikatssperrlisten (CRL) werden von der jeweiligen Sub-CA, die Sperrlisten für Zertifizierungsstellen (ARL) werden von der jeweiligen Root-CA ausgestellt und auf dem LDAP-Verzeichnisdienst veröffentlicht. Gesperrte Zertifikate werden erst nach dem Ablauf der Gültigkeit aus der Zertifikatssperrliste (CRL) entfernt.

4.10.2 Verfügbarkeit

Der OCSP-Dienst als auch die CRL/ARL auf dem LDAP-Verzeichnisdienst stehen 7*24 Stunden zur Verfügung. Die Antwortzeit des OCSP-Responders und LDAP-Verzeichnisdienst beträgt unter normalen Betriebsbedingungen weniger als 10 Sekunden.

4.10.3 Weitere Merkmale

Nicht relevant.

4.11 Beendigung des Vertragsverhältnisses

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 entsprechend des Kündigungsdatums des Vertrages gesperrt und sind danach nicht mehr nutzbar. Eine Zertifikats-Validierung über die Zertifikatssperrliste und OCSP wird weiterhin unterstützt.

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

4.12 Schlüsselhinterlegung und –wiederherstellung (Key Escrow, Key Recovery)

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Die im Rahmen der cPKI verwendeten Schlüsselpaare von CA´s werden auf einem sicherheitsüberprüften Hardware Security Module (HSM) gespeichert und in sicherer Umgebung abgelegt. Die Speicherung des Schlüsselmaterials auf weiteren HSM erfolgt ausschließlich zur Schlüsselsicherung (Key-Back-Up) und dient zur Wiederherstellung und Aufrechterhaltung des Dienstes durch qualifiziertes Personal (Trusted Role) des Trust Centers. Eine Schlüsselhinterlegung (Escrow) bei Dritten (z.B. Treuhänder, Notar) ist nicht realisiert.

Darüber hinaus erfolgt für Endteilnehmer-Verschlüsselungszertifikate eine Schlüsselhinterlegung mit einer gesicherten Ablage von Schlüsselmaterial in der Betriebsumgebung des Trust Centers.

Eine Schlüsselwiederherstellung ist gebunden an die Zustimmung des Zertifikatsinhabers oder der im Konzern verantwortlichen Stellen für IT-Sicherheit, Datenschutz und Personalvertretung gemäß BetrVG. 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 Auftragstellenden.

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Session Key Kapselung: Nicht relevant.

Abläufe und Policies im Rahmen von Wiederherstellungsprozessen: 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.

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 Beauftragung und Erzeugung 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.

5.1 Physikalische Kontrollen

5.1.1 Standort und bauliche Maßnahmen

T-Systems betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Hälften, zwei getrennt arbeitenden Energietrakten (Elektro, Klima, Wasser) mit Gebäudemanagementsystem und Notstromaggregaten sowie einem Verwaltungstrakt 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 Angriffhemmung. 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 Energieversorgung und Klimatisierung

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.

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.

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 (lat. für untätig, unbeteiligt, träge).

5.1.6 Aufbewahrung und Entsorgung von Datenträgern

Datenträger, die Produktionssoftware und -daten, Audit-, Archiv- oder Sicherungsinformationen enthalten,

werden in Räumen gelagert, die mit den entsprechenden physischen und logischen Zutrittskontrollen versehen sind und Schutz vor Unfallschäden (z.B. Wasser-, Brand- und elektromagnetische Schäden) bieten.

5.1.7 Entsorgung

Vertrauliche Dokumente und Materialien werden vor ihrer Entsorgung physisch zerstört. Datenträger, die vertraulichen Informationen enthalten, werden vor ihrer Entsorgung derart behandelt, dass diese Daten nicht auslesbar oder wieder herstellbar sind. 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 Sicherheitsmaßnahmen

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 (siehe Abschnitt5.3.1) erfüllen.

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 Sicherheitskonzept en, in der vorliegenden Sicherheitsrichtlinie (CP) und der Erklärung zum Zertifizierungsbetrieb (CPS) der vom T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.2.2 Anzahl der pro Aufgabe involvierten Personen

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.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

T-Systems Mitarbeiter, die als vertrauenswürdige Personen eingestuft sind und vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer T-Systems-internen Sicherheitsüberprüfung (siehe Abschnitt 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 CA und andere IT-Systeme erhalten,
- zur Durchführung bestimmter Aufgaben im Zusammenhang mit diesen Systemen zugelassen werden.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

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

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

5.3 Personelle Maßnahmen

5.3.1 Anforderungen an Personal

Für den Betrieb der in Abschnitt 1.4 ff. verlangt T-Systems von seinen Mitarbeitern, die als vertrauenswürdige Personen tätig werden möchten, Nachweise vorzulegen über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.

In regelmäßigen Abständen, spätestens jedoch nach drei Jahren, ist ein neues Führungszeugnis der T-Systems vorzulegen.

5.3.2 Sicherheitsüberprüfung von Personal

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.

5.3.3 Schulungsanforderungen

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 CPS und der zugehörigen CP
- Relevante Anforderungen und Vorgaben aus den [CAB-BR]

- Allgemeine Bedrohungs- und Angriffsszenarien bzgl. der Validierungsmethoden (z.B. Social Engineering)

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

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

5.3.4 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Nicht anwendbar..

5.3.5 Sanktionen bei unerlaubten Handlungen

T-Systems behält sich vor, unbefugte Handlungen oder anderer Verstöße gegen dieses CP/CPS und der daraus abgeleiteten Verfahren zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen können Maßnahmen bis einschließlich der Kündigung beinhalten und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.

5.3.6 Anforderungen an unabhängige, selbständige Zulieferer

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 Abschnitt 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.

5.3.7 Dokumentation für das Personal

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

5.4 Überwachung / Protokollierung

Art der aufgezeichneten EreignisseGenerell enthalten alle Protokolleinträge mindestens das Datum und die Uhrzeit des Eintrags, einen Verweis auf die Rolle oder das System, welches den Eintrag generiert hat, sowie eine Beschreibung des Ereignisses.

Veränderungen im Lebenszyklus von Zertifikaten und relevanten Kontextinformationen werden protokolliert, dies bezieht sich im Einzelnen auf:

- Ereignissen im Lebenszyklus von Zertifikaten für Endteilnehmer:
    - Erzeugung

- Sicherung
- Archivierung
-
- Wiederherstellung
- Erneuerung
- Zertifikatssperrung / Suspendierung / Aufhebung der Suspendierung

- Ereignissen im Lebenszyklus von Zertifikaten von Zertifizierungsstellen:
  - Zertifikatsauftrag (erfolgreich / fehlgeschlagene Bearbeitung und beiliegende Dokumente)
  - Erstellung von Zertifikaten
  - Zertifikatserneuerung
  - Zertifikatssperrung / Suspendierung / Aufhebung der Suspendierung
- Erzeugung von Sperrlisten und OCSP-Einträgen
- Änderungen von kryptographischen Geräten (z.B. HSM) und CA-Software

5.4.1 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/Logging-Dateien werden regelmäßig unter Beachtung gesetzlicher Vorgaben (BDSG, BetrVG, …) auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. T-Systems prüft die Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten insbesondere auch als Folge von Unregelmäßigkeiten und Störungen.

Eingeleitete Maßnahmen, die als Reaktion aus der Auswertung von Audit-Protokollen/Logging-Dateien stammen, werden ebenfalls protokolliert. Aufbewahrungszeitraum für Audit-ProtokolleAudit-Protokolle/Logging-Dateien werden nach Bearbeitung gemäß Abschnitt 5.5.2archiviert.

5.4.2 Schutz der Audit-Protokolle

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

Sicherungsverfahren für Audit-ProtokolleEine Sicherung von Audit-Protokollen/Logging-Dateien wird regelmäßig durchgeführt.

Audit-Erfassungssystem (intern vs. extern)Audit-Daten/Logging-Dateien von Anwendungs-, Netzwerk - und Betriebssystemebene werden automatisiert erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von T-Systems-Mitarbeitern aufgezeichnet.

5.4.3 Benachrichtigung bei schwerwiegenden Ereignissen

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

5.4.4 Schwachstellenbewertung

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

5.5 Datenarchivierung

5.5.1 Art der archivierten Daten

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, die über Bulk beantragt wurden,
- alle Audit-Daten/Logging-Dateien, die gemäß Abschnitt 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 zehn (10) 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 Sicherung der elektronischen Archive wird regelmäßig 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 Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (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.

Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Abschnitt 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 Abschnitt 2.3).

Abgelaufene oder gesperrte CA- und Root-CA-Zertifikate stehen weiterhin zur Validierung auf einer Webseite zur Verfügung.

5.7 Kompromittierung und Desaster Recovery

5.7.1 Umgang mit Störungen und Kompromittierungen

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

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 zuständigen T-Systems Sicherheitsabteilung gemeldet. Das Ereignis zieht eine entsprechende Eskalation, Störfalluntersuchung, Störfallreaktion bis hin zur finalen Störungsbeseitigung nach sich. Abhängig von der Störungsklassifizierung erfolgt die Wiederherstellung (Disaster Recovery).

5.7.3 Verfahren bei Kompromittierung des privaten Schlüssels 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 (ARL) 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 Abschnitt 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,
- Bewusstsein-schaffende Maßnahmen,
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals,
- Die Verantwortung der Individuen (Rollenbeschreibung und -zuweisung),
- Wiederanlaufzeit (RTO),
- Regelmäßige Durchführung der Notfallpläne zu Testzwecken,
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der cPKI nach Unterbrechung oder Ausfall,
- 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 Abschnitt 8) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

Schlüsselmaterial des Endteilnehmers, das auf Smartcards ausgestellt wurde, oder welches im Rahmen einer Schlüsselsicherung bereitgestellt wurde (z.B. Key-Restore für Verschlüsselungszertifikate), ist nicht im Rahmen dieses Notfallplans abgedeckt.

Betriebesbeendigung Eine Betriebsbeendigung kann nur durch T-Systems ausgesprochen werden.

Falls T-Systems in Gänze oder für Teile des Services den Betrieb einstellt, wird ein Beendigungsplan erstellt. Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen, betroffene nachgeordnete Stellen (Endteilnehmer, vertrauende Dritte, Registrierungsstellen) vorab über diese Betriebsbeendigungen zu informieren.

Ein Beendigungsplan kann die folgenden Regelungen enthalten:

- Benachrichtigung der Mandanten, 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,
- je nach Ausgestaltung bestehender Einzelverträge entstehende Kostenerstattung,
- Aufbewahrung der Unterlagen und Archive der Zertifizierungsinstanz (CA).

6 Technische Sicherheitsmaßnahmen

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

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 evaluiert) 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.

Schlüsselpaare für ausgegebene Signatur- und Authentifizierungszertifikate von Endteilnehmern basieren auf der MyCard (einer speziellen Smart Card) 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 Versiegelung, die den Auslieferungszustand der Karte definiert, ausgeliefert.

Schlüsselpaare für Verschlüsselungszertifikate von Endteilnehmern werden zentral in einer speziell geschützten Umgebung unter Verwendung von Hardware Security Modulen (HSM) erzeugt und auf der MyCard, durch Mechanismen des TCOS Chipkarten Betriebssystems gesichert, abgelegt.

6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Im Falle der Nutzung von Smart Cards werden für Signatur und Authentifizierung die bei der Produktion auf die Karte aufgebrachten Schlüssel verwendet. Es findet keine Übermittlung dieser privaten Schlüssel außerhalb einer Smartcard statt. Verschlüsselungsschlüssel werden serverseitig generiert und nach vorheriger Authentisierung des Endteilnehmers unter Verwendung eines dedizierten Aktivierungspasswortes (Einmalpasswort bzw. One Time Password) über einen verschlüsselten Tunnel sicher auf die Smart Card übertragen.

6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller

Öffentliche Schlüssel werden in Form signierter PKCS#10 Requests an den Zertifikatsherausgeber ausgeliefert.

6.1.4 Zustellung öffentlicher Zertifizierungsstellenschlüssel an Vertrauende DrittePublikation öffentlicher Schlüssel der Zertifizierungsstelle

Das Stammzertifikat „Deutsche Telekom Root CA 2“, das 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“, das für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich ist, muss in den Zertifikatsspeicher von Arbeitsplatzsystemen nachinstalliert (z.B. mittels automatisierter Softwareverteilung) werden.

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

Darüber hinaus stehen alle Stammzertifikate und Sub-CA-Zertifikate auf der INTRANET-Seite http://corporate-pki.telekom.de/ zum Herunterladen bereit.

6.1.5 Schlüssellängen

Die Schlüssellänge für alle Zertifikate beträgt mindestens 2048 Bit (RSA-Schlüssellänge).

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 SHA1, ~~MD5~~

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

6.1.7 Schlüsselverwendungzwecke (nach X.509 v3, Attribut „key usage“)

Die Schlüsselverwendungen der ausgegebenen Zertifikate ist im Attribut „key usage“ festgelegt.

Mögliche Werte sind:

- Key Encipherment
- Data Encipherment

- Digital Signature

Die erweiterte Schlüsselverwendung ist im Attribut „extended key usage“ festgelegt.

Mögliche Werte sind:

- Server Authentication (1.3.6.1.5.5.7.3.1)
- Client Authentication (1.3.6.1.5.5.7.3.2)
- Secure E-Mail (1.3.6.1.5.5.7.3.4)
- Smartcard Logon (1.3.6.1.4.1.311.20.2.2)

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 Schlüsselsicherung“ für den Kunden gespeichert 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 Zertifikate von Zertifizierungsstellen werden private Schlüssel in Verantwortung der für den Betrieb Verantwortlichen im Trust Center gesichert abgelegt und gegen nicht autorisierte Verwendung geschützt (z.B. Verwendung spezieller Hardwaregeräte).

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

6.2.1 Standards und Kontrollen für kryptographische Module

Im Fall von Root-CA und CA Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140-/2 Level 3 evaluiert) abgelegt.

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 privater Schlüssel von Zertifizierungsstellen wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentification mit Key) geschützt. 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 Abschnitt 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 in der erzeugenden Offline-CA. 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 ~~TeleSec Shared-Business-CA~~ CPKIin 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. einspielen 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.

T-Systems speichert keine Kopien von privaten Schlüsseln des Master-Registrator-Zertifikats.

Das Trust Center der T-Systems bietet für cPKI eine Sicherung des privaten Schlüssels im Auftrag des Endteilnehmers an. Informationen zur Sicherung von privaten Endteilnehmerschlüsseln sind in den Abschnitten 4.12und 6.2.3 beschrieben.

Die Wiederherstellung des Schlüsselmaterials von Endteilnehmern ist erlaubt, sofern der Endteilnehmer bzw. Schlüsselverantwortliche der Wiederherstellung zustimmt. Liegt diese Erlaubnis nicht vor, darf T-Systems 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 des Mandanten oder

diese durch eine autorisierte Stelle der DTAG unter Beachtung gesetzlicher Auflagen des Datenschutzes (BDSG) und der Rahmenbedingungen des Betriebsverfassungsgesetzes (BetrVG) angefordert wurde.

6.2.4.1 Sicherung und Wiederherstellung des Verschlüsselungsschlüssels durch Enrollment-Software

Bei der Personalisierung der Smartcard durch Verwendung geeigneter Enrollment-Software wird die passwortgeschützte Soft-PSE (privater Schlüsselverschlüsselungsschlüssel inkl. Verschlüsselungs-Zertifikat), welches nach vorheriger Authentisierung des

Endteilnehmers/Empfängers zusätzlich transportverschlüsselt übertragen wird, als auch ein korrespondierendes Passwort benötigt.

6.2.4.2 Sicherung und Wiederherstellung von Soft-PSE über das Betriebssystem

Bei der Sicherung von Soft-PSEn kann das Schlüsselmaterial über das Betriebssystem (Zertifikatsspeicher) exportiert und verschlüsselt beim Endteilnehmer gespeichert werden.

Die Soft-PSE ist 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 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.Archivierung des privaten Schlüssels

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

Das Trust Center der T-Systems archiviert Kopien von privaten Schlüsseln von Endteilnehmern, die im Rahmen einer Generierung von Verschlüsselungs-Zertifikaten für Benutzer erstellt wurden und in Verbindung mit der zentralen Schlüsselsicherung (Key-Back-Up) zu einem späteren Zeitpunkt abrufbar sein sollen.

6.2.5 Übertragung privater Schlüssel in oder von einem kryptographischen Modul

Das T-Systems Trust Center generiert CA-Schlüssel auf den kryptografischen Hardware-Modulen (HSM) der Offline-CA. Das Schlüsselmaterial wird anschließend über Security-Token auf die HSMs der entsprechenden Sub-CA der cPKI eingespielt. Dabei erfolgt die Übertragung in verschlüsselter Form zwischen den beiden Hardware Security Modul (HSM).

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 eine Smartcard importiert werden.

6.2.6 Ablage privater Schlüssel in Kryptomodulen

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 speichern extern erzeugte Schlüssel oder selbst generierte Schlüssel in sicherer Form.

6.2.7 Methode zur Aktivierung privater Schlüssel

Alle Endteilnehmer, Registratoren, Administratoren und Operatoren müssen die Aktivierungsdaten (z.B. PIN, Importpasswort) für ihren privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß der vorliegenden Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) schützen.

Endteilnehmer haben zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Nutzung eines Passworts bzw. einer PIN (gemäß Kapitel6.4.1) 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. 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 deaktiviert (abgelaufen, gesperrt) sind, dürfen sie nur in verschlüsselter Form und/oder mit Passwort- bzw. PIN-Schutz aufbewahrt werden.

Schlüsselmaterial für CA- und Root-CA-Zertifikate wird entsprechend durch die autorisierten Personen aktiviert und auf kryptographischen Hardware-Modulen (HSM) aufgebracht. Der zum CA-Zertifikat gehörende private Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt (Abschnitt 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 oder Sperrung (Abschnitt 4.9.3) ist der private Schlüssel nicht mehr nutzbar.
Wenn Zertifikate mit ihren zugehörigen privaten Schlüsseln deaktiviert (gesperrt) werden, dürfen sie nur in verschlüsselter Form und/oder mit Passwort- bzw. PIN-Schutz aufbewahrt werden.

6.2.8 Methode zur Deaktivierung privater Schlüssel

- Die Deaktivierung privater Schlüssel von Administratoren und Operatoren erfolgt ereignisbezogen und obliegt dem Personal des Trust Centers der T-Systems. Für die Deaktivierung von privaten Endteilnehmer Schlüsseln ist der Endteilnehmer verantwortlich.

6.2.9 Methode zur Vernichtung privater Schlüssel

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

Die Vernichtung von privaten Schlüsseln der Endteilnehmer obliegt diesen selbst.

6.2.10 Bewertung kryptographischer Module

Siehe 6.2.1

6.3 Weitere Aspekte des Zertifikats- und Schlüsselmanagements

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 Gültigkeit von Zertifikaten und Schlüsselpaaren

Ein Überblick über die Gültigkeit personenbezogener Zertifikate bzw. Schlüssel der verschiedenen Zertifikate gibt die folgende Tabelle:

Zertifikatstyp	**Gültigkeitsdauer**
Wurzelzertifizierungsstellen (Root-CA)	20 Jahre
Zertifizierungsstellen (Sub-CA)	8 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	3 Jahre
Deutsche Telekom AG External Workforce Signature	3 Jahre
Deutsche Telekom AG External Workforce Authentication	3 Jahre

Tabelle 4: Gültigkeitszeiträume von Zertifikaten

6.4 Aktivierungsdaten

Zertifikate und Schlüssel von Zertifizierungsstellen
Um die auf dem HSM hinterlegten privaten Schlüssel der CA-Zertifikate schützen zu können, werden Aktivierungsdaten (Geheimnisanteile) in einer definierten „Key Ceremony“ generiert und protokolliert.

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

6.4.1 Generierung und Installation von Aktivierungsdaten

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

Bei Zertifikaten von Zertifikatsinhabern (Endteilnehmer) werden One Time Secrets von der PKI generiert. Die Vergabe einer PIN (Smartcard oder Software-PSE) erfolgt durch die jeweiligen Zertifikatsinhaber.

6.4.2 Schutz der Aktivierungsdaten

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.

6.4.3 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.

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

Alle PKI-Funktionen werden mit Hilfe vertrauenswürdiger und geeigneter Systeme durchgeführt.

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahen

T-Systems stellt sicher, das die Verwaltung der PKI-Systeme vor unbefugtem Zugriff Dritter gesichert ist. T-Systems verwendet Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, Mehr-Augen-Prinzip), um die CA-Funktionalitäten, Verzeichnisdienste und OCSP-Responder, welche im Trust Center betrieben werden, vor internen und externen Eindringligen zu schützen. Der direkte Zugriff auf CA-Datenbanken, die die CA-Funktionalitäten unterstützen, ist auf geeignetes, geschultes und vertrauenswürdiges Betriebspersonal beschränkt.

Der Zertifikats Managementprozess umfasst

- Physikalische Sicherheit und Sicherung der Umgebung,
- 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,
- Benutzerverwaltung, Berechtigungsmatrix, Aufklärung, Sensibilisierung und Schulung/Ausbildung sowie
- Verfahrenskontrollen, Aktivitätsprotokollierung und Abschaltung bei Timeouts.

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

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 Maßnahmen der Systementwicklung

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.

6.6.2 Maßnahmen des Sicherheitsmanagements

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.

6.6.3 Sicherheitskontrollen des Lebenszyklus

Keine Bestimmungen.

6.7 Netzwerk-Sicherheitskontrollen

Folgende Netzwerk-Sicherheitsmaßnahmen wurden implementiert:

- Die Netzwerke des Zertifizierungsdienstes sind durch Firewalls vom Internet getrennt und beschränken den Datenverkehr auf das für die Funktionen notwendige Maß.
- 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 Netz.
- Die internen Netzwerke des Zertifizierungsdienstes sind nach dem Schutzbedarf der Systeme und Komponenten aufgeteilt und untereinander durch Firewalls getrennt.

6.8 Zeitstempel

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

7 Zertifikats-, Sperrlisten-, undund OCSP Profile

7.1 Zertifikatsprofile

Die von den CAs ausgestellten Zertifikate sind konform zu:

- [ITU-T Recommendation X.509][2] (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 08/05.
- RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

und

- Common PKI Spezifikation 1.1.

Die ausgestellten Zertifikate enthalten in jedem Fall die im X.509-Standard festgelegten Felder:

Felder	**Wert**
Serial Number	Eindeutige Seriennummer (je Issuer DN)
Signature Algorithm	Object Identifier (OID) des zur Signatur der Zertifikate verwendeten Algorithmus (siehe Abschnitt *7.1.3*)
Issuer DN	siehe Abschnitt *7.1.4*
Valid from („Not before“)	UTC, codiert gemäß RFC 5280
Valid to („Not after“)	UTC, codiert gemäß RFC 5280
Subject DN	siehe Abschnitt *7.1.4*
Subject Public Key	Codiert gemäß RFC 5280
Signature	Erstellt und codiert gemäß RFC 3280

Tabelle 5: Basis-Felder des Zertifikatsprofils

Ein Zertifikatsantrag (Request), der aus einem Gerät oder einer Anwendung stammt, wird auf definierte Inhalte des Subject-DN (siehe Abschnitt 3.1.1 ff.) und Verwendung unerlaubter Zeichen überprüft. Es gilt die Ausprägung des jeweilige Zertifikatsprofil wie in Abschnitt 7.1 ff beschrieben. Die Verwendung von unerlaubten Zeichen wird mit der Überprüfung angezeigt oder dem Antragsteller mitgeteilt.

Die von T-Systems ausgestellten Zertifikate entsprechen folgenden Anforderungen:

- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [X.509] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)
- [CAB-BR] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

7.1.1 Versionsnummern

Zertifikate werden gemäß X.509 Standard in der Version 3 ausgestellt.

7.1.2 Zertifikatserweiterungen

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.

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.

7.1.2.1 Schlüsselverwendung(KeyUsage) Benutzerzertifikate

In der nachfolgenden Tabelle ist die Erweiterung „Schlüsselverwendung“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Zertifikat	Digital Signature	Key Encipherment	Data Encipherment
Deutsche Telekom AG Employee Encryption	Nein	Ja	Ja
Deutsche Telekom AG Employee Signature	Ja	Nein	Nein
Deutsche Telekom AG Employee Authentication	Ja	Nein	Nein
Deutsche Telekom AG External Workforce Encryption	Nein	Ja	Ja
Deutsche Telekom AG External Workforce Signature	Ja	Nein	Nein
Deutsche Telekom AG External Workforce Authentication	Ja	Nein	Nein

Tabelle 6: Schlüsselverwendung Benutzerzertifikate n (hier: Key Usage)

7.1.2.2 Erweiterte Schlüsselverwendung (Extended Key Usage) Benutzerzertifikate

In der nachfolgenden Tabelle ist die „Erweiterte Schlüsselverwendung“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

	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
Deutsche Telekom AG Employee Encryption	Nein	Nein	Nein	Ja	Nein
Deutsche Telekom AG Employee Signature	Nein	Nein	Nein	Ja	Nein
Deutsche Telekom AG Employee Authentication	Nein	Ja	Nein	Nein	Ja
Deutsche Telekom AG External Workforce Encryption	Nein	Nein	Nein	Ja	Nein
Deutsche Telekom AG External Workforce Signature	Nein	Nein	Nein	Ja	Nein
Deutsche Telekom AG External Workforce Authentication	Nein	Ja	Nein	Nein	Ja

Tabelle 7: Erweiterte Schlüsselverwendung Benutzerzertifikate (hier: Extended Key Usage)

7.1.2.3 Schlüsselverwendung (Key Usage) CA-Zertifikate

In der nachfolgenden Tabelle ist die „Schlüsselverwendung“ den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Zertifikatsprofil	**Sub-CA**	**Root-CA**
Risikowert (Critically)	critical	critical
Bezeichnung	Cert/CRL	Cert/CRL

0 digital Signature	Nein	Nein
1 nonRepudiation	Nein	Nein
2 keyEncipherment	Nein	Nein
3 dataEncipherment	Nein	Nein
4 keyAgreement	Nein	Nein
5 keyCertSign	Ja	Ja
6 CRLSign	Ja	Ja
7 encipheronly	Nein	Nein
8 decipherOnly	Nein	Nein
Wert (hex)	06	06

Tabelle 86:Schlüsselverwendung CA (hier: Key Usage)

7.1.2.4 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 der nachfolgenden sind die von der cPKI genutzten Root- und Sub-CA-Zertifikate dargestellt. Die cPKI stellt keine weiteren Sub-CA-Zertifikate aus, die hierarchisch einer der dargestellten Sub-CAs untersteht.

Name/Typ	Risikowert (Critically)	Benutzertyp	Beschränkung des Zertifizierungstyps
Deutsche Telekom Root CA 2	non critical	Zertifizierungsstelle	5
Deutsche Telekom Internal Root CA 1	critical	Zertifizierungsstelle	1
Deutsche Telekom Issuing CA 01	critical	Zertifizierungsstelle	0
Deutsche Telekom Issuing CA 01	critical	Zertifizierungsstelle	0
Deutsche Telekom Issuing CA 01	critical	Zertifizierungsstelle	0

Endteilnehmer	non critical	Endeinheit	keine

Tabelle 96: Basiseinschränkungen (hier: BasicConstraints)

7.1.2.5 Sperrlistenverteilungspunkt (CRLDistributionPoint)

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 (ARL) 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.

7.1.2.6 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 jeweiligen hierarchisch übergeordnete Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.7 Stellenschlüsselkennung (authorityKeyIdentifier)”

In Endteilnehmer-Zertifikaten enthält die Erweiterung „Stellenschlüsselkennung“ als Attributswert einen SHA-1-Hashwert, der mit dem Wert der Erweiterung „Schlüsselkennung des Antragstellers“ (siehe Kapitel 7.1.2.7) des Zertifikats der hierarchisch übergeordneten Zertifizierungsinstanz (CA) mathematisch übereinstimmt.

Es gelten ebenfalls die Regelungen der jeweiligen hierarchisch übergeordnete Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.8 Zugriff auf Stelleninformation (Authority Information Access)”

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 Abschnitt 2.2 unter „Bereitstellung von Zertifikatsstatusdaten über das OCSP-Protokoll“

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.9 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

Als Algorithmus kommt ausschließlich RSA mit dem Object Identifier 1.2.840.113549.1.1.1 zum Einsatz.

7.1.4 Namensformen

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=Deutsche Telekom AG Issuing CA 01, OU = Trust Center, O = Deutsche Telekom AG, C = DE	E = primäre eMail aus AD, CN =Name Vorname, OU = CID OU = Employee, OU = Person O = DTAG
Deutsche Telekom AG Employee Signature	CN=Deutsche Telekom AG Issuing CA 01, OU = Trust Center, O = Deutsche Telekom AG, C = DE	E = primäre eMail aus AD, CN =Name Vorname, OU = CID OU = Employee, OU = Person O = DTAG
Deutsche Telekom AG Employee Authentication	CN = Deutsche Telekom AG Issuing CA 02, OU = Trust Center, O = Deutsche Telekom AG, C = DE	E = primäre eMail aus AD, CN =Name Vorname, OU = CID OU = Employee, OU = Person O = DTAG
Deutsche Telekom AG External Workforce Encryption	CN=Deutsche Telekom AG Issuing CA 01, OU = Trust Center, O = Deutsche Telekom AG, C = DE	E = primäre eMail aus AD, CN =Name Vorname, OU = CID OU = External Workforce, OU = Person O = DTAG
Deutsche Telekom AG External Workforce Signature	CN=Deutsche Telekom AG Issuing CA 01, OU = Trust Center, O = Deutsche Telekom AG, C = DE	E = primäre eMail aus AD, CN =Name Vorname, OU = CID OU = External Workforce, OU = Person O = DTAG
Deutsche Telekom AG External Workforce Authentication	CN = Deutsche Telekom AG Issuing CA 02, OU = Trust Center, O = Deutsche Telekom AG, C = DE	E = primäre eMail aus AD, CN =Name Vorname, OU = CID OU = External Workforce, OU = Person

	O = DTAG

Tabelle 108: 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	none	E-Mail Adresse
Deutsche Telekom AG Employee Signature	none	none	E-Mail Adresse
Deutsche Telekom AG Employee Authentication	none	UPN	E-Mail Adresse
Deutsche Telekom AG External Workforce Encryption	none	none	E-Mail Adresse
Deutsche Telekom AG External Workforce Signature	none	none	E-Mail Adresse
Deutsche Telekom AG External Workforce Authentication	none	UPN	E-Mail Adresse
Deutsche Telekom AG Telekom Computer	DNS	none	none
Deutsche Telekom AG Domain Controller	DNS	none	none

Tabelle 119: Einträge im Subject Alternative Name

7.1.5 Namensbeschränkungen

Nicht anwendbar.

7.1.6 Objektidentifikatoren der Zertifizierungsrichtlinien

7.1.6.1 Objekt-Identifikatoren für Zertifizierungsrichtlinien der cPKI

Alle Endteilnehmer- und CA-Zertifikate enthalten eine Erweiterung „Zertifikatsrichtlinien (certificate policies)“, der die OID der zum Zeitpunkt der Ausstellung gültigen Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) enthält.

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))

Für die durch das CA/Browser-Forum in den [CAB-BR] definierten Policy-OIDs gelten die folgenden Anforderungen, welche von den Sub-CA der cPKI eingehalten werden. Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.2 verwendet, müssen zwingend folgende Felder des Subject DN ausgefüllt sein:

- organizationName
- localityName
- stateOrProvinceName
- countryName

Die Policy-OID 2.23.140.1.2.1 wird von der cPKI nicht verwendet, da keine DV-Zertifikate 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.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien

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, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)

Ausgegebene Sperrlisten (CRL) enthalten mindestens die folgenden Felder:

Felder	Wert
Version	X.509 Version 2
Issuer	Enthält die Instanz, die die Sperrliste ausgegeben und signiert hat.
This update / valid from	Ausgabedatum/-zeit der Sperrliste.
Next update	Datum und Zeit der nächsten Sperrliste.
Signature Algorithm	Algorithmus der zum Signieren der Sperrliste verwendet wurde: sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
Revoked certificates	Liste der gesperrten Zertifikate. Diese beinhaltet die Seriennummer des gesperrten Zertifikats, sowie das Sperrdatum.

Tabelle 1210: CRL Profil (hier: Basiswerte)

7.2.1 Versionsnummer

Sperrlisten werden gemäß Standard X.509 in der Version 2 bereitgestellt.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

7.2.2.1 Erweiterung „Stellenschlüsselkennung (authorityKeyIdentifier)"

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 1311: CRL Profil: Extension-Einträge

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 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

Tabelle 1411: Erweiterung Sperrgrund

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. Access Method: OCSP Access (1.3.6.1.5.5.7.48.1).

Fullname CDP: Die jeweiligen Full Name CDP sind in den jeweils zu überprüfenden Zertifikaten enthalten und können durch eine Applikation aufgerufen werden, siehe auch RFC 5280 Abschnitt 4.2.2.1.

Der eingesetzte OCSP-Responder erfüllt die Anforderungen des RFC 2560.

7.3.1 Versionsnummer

Es wird die Version der OCSP Spezifikation gemäß RFC 2560 (full profile) unterstützt.

7.3.2 OCSP Erweiterungen

Das OCSP-Zertifikat, ausgestellt von T-Systems, enthält das Attribut „Erweiterte Schlüsselverwendung" mit der OID „1.3.6.1.5.5.7.3.9" (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 Prozesse der cPKI werden in regelmäßigen Abständen Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) auf Basis der Anforderungen für „WebTrust for Certification Authorities“ unterzogen.

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 eine ununterbrochenen Folge von Auditperioden durchgeführt, deren Zeitraum die Dauer von einem Jahr nicht überschreitet.

Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits), die die Servicequalität sicher stellen, finden regelmäßig, jedoch mindestens vierteljährlich, 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 die cPKI beauftragt das Trust Center einen qualifizierten T-Systems Mitarbeiter mit entsprechender Fachkunde betreffend PKI, IAM sowie WebTrust-Anforderungen. Dadurch ist die Einhaltung der besonderen Anforderungen an den Auditor bei einer Prüfung des Web-Trust konformen Betriebes der cPKI gewährleistet.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die WebTrust-Konformität der cPKI handelt es sich um einen qualifizierten Auditor (z.B. Gutachter). Prüfungen werden als Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durchgeführt.

8.4 Prüfungsbereiche

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
- Identitätsprüfungen der Endteilnehmer
- 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:

- WebTrust: Trust Service Principles and Criteria for Certification Authorities
- WebTrust for Certification Authorities –SSL Baseline Requirements Audit Criteria

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 Mängelbeseitigung

Werden bei einem ComplianceAudit von T-Systems Mängel oder Fehler festgestellt, wird entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen. Der Leiter Trust Center ist verantwortlich für die Entwicklung eines Maßnahmenplans. Die Umsetzung der Maßnahmen ist in einem wirtschaftlich angemessenen Zeitraum durchzuführen. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheidet 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, welche ein Stammzertifizierungsstellenzertifikat der T-Systems einbetten, müssen spätestens drei Monate nach Ablauf der jeweiligen Auditperiode veröffentlicht werden.

Für die cPKI werden die geforderten Audits nach dem WebTrust-Kriterien abgelegt. Die zugehörigen Berichte werden auf der Internetseite http://cert.webtrust.org veröffentlicht.

9 Geschäftliche und rechtliche Angelegenheiten

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- und Registrator-Zertifikaten Entgelte zu berechnen.

9.1.2 Entgelte für den Zugriff auf Zertifikate

T-Systems berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst der cPKI keine Entgelte.

T-Systems gestattet Dritten, die selbst Produkte und Dienstleistungen vermarkten, nur nach vorheriger ausdrücklicher schriftlicher Genehmigung den Zugriff und Abruf von Zertifikaten.

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.

T-Systems gestattet Dritten, die selbst Produkte und Dienstleistungen vermarkten, nur nach vorheriger ausdrücklicher schriftlicher Genehmigung den Zugriff auf Sperr- und Statusinformationen von Zertifikaten.

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 (Abschnitt 1.6.2), die das Urheberrecht des Dokuments (Abschnitt 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 für die Projektierung und den Betrieb der cPKI, auf die an dieser Stelle verwiesen wird.

9.2.1 Versicherungsschutz

Dem Auftraggeber für den Betrieb der cPKI 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 für den Betrieb der cPKI 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 für den Betrieb der cPKI 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

Unter vertraulichen Informationen werden alle Informationen von PKI-Beteiligten (siehe Abschnitte 1.4.2 und1.4.3) der cPKI eingestuft, die nicht unter Abschnitt 9.3.2 fallen.

9.3.1 Umfang von vertraulichen Informationen

Alle in der Corporate PKI verwendeten, verarbeiteten und gespeicherten Informationen über deren Teilnehmer, die nicht unter Abschnitt 2.2 fallen, gelten als vertraulich.

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 für den Betrieb der cPKI hat die einschlägigen gesetzlichen Bestimmungen sowie ggf. weiteren Regelungen zum Datenschutz zu beachten.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Innerhalb der cPKI müssen zur Leistungserbringung personenbezogene Daten elektronisch gespeichert und verarbeitet werden.

Die T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 BDSG sicher.

Entsprechend den Konzernvorgaben der Deutschen Telekom AG wurde für die cPKI ein kombiniertes Sicherheits- und Datenschutzkonzept (SDSK) im Rahmen eines nach Konzernvorgabe obligatorisch durchzuführenden Verfahrens (sogenanntes PSA-Verfahren9 erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte um PKI-Dienst zusammen.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Abschnitt 9.3.1.

9.4.3 Nicht- vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Abschnitt 9.3.2.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Für personenbezogene Daten gelten die Regelungen analog zu Abschnitt 9.3.3.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsantragsteller stimmt der Nutzung von personenbezogenen Daten durch eine CA oder RA zu, soweit dies zur Leistungserbringung erforderlich ist.

Ferner dürfen alle Informationen veröffentlicht werden, die nach Abschnitt 9.4.3 als nicht vertraulich behandelt werden und deren Veröffentlichung durch den Mandanten nicht widersprochen wurde.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Die Corporate PKI wird in der Bundesrepublik Deutschland betrieben. 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 Ver-

fahrens 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 Abschnitte 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 für die cPKI jegliche geistigen Eigentumsrechte an Zertifikaten, Sperrungs- oder Statusinformationen, öffentlich zugängliche Verzeichnisdienste und Datenbanken mit den ihnen enthaltenen Informationen vor.

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 Vorraussetzung, 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 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.

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 Mandant bzw. dessen Endteilnehmer selbst erzeugte, verbleibt sein Eigentumsrecht. Dies gilt auch für Schlüsselmaterial auf Smartcards, das er erworben hat. Zusicherungen und Gewährleistungen

9.5.5 Zusicherungen und Gewährleistungen der Zertifizierungsstelle

T-Systems verpflichtet sich,

- keine wesentlich unrichtigen Angaben in Zertifikaten aufzunehmen, die 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 dieses Dokuments genügen und
- dass die Sperrfunktionalitäten sowie die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP Responder) allen wesentlichen Anforderungen der vorliegenden Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (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 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 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 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.

T-Systems behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Auftraggeber für den Betrieb der cPKI abzuschließen.

9.5.6 Zusicherungen und Gewährleistungen der Registrierungsstelle

Registrierungsstellen verpflichten sich:

- keine wesentlich unrichtigen Angaben im Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- das 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 Mandant 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,
- das alle Zertifikate den wesentlichen Anforderungen dieser CP/CPS genügen, und
- das 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.

9.5.7 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,

- das 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 der vorliegenden Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) beschriebenen Pflichten entstehen,
- bei Verlust oder Verdacht der Kompromittierung des geheimen Schlüssels, wesentliche Änderungen des Zertifikatsangaben oder Missbrauchsvermutung eine Sperrung des entsprechenden Endteilnehmer-Zertifikat zu veranlassen bzw. selbst durchzuführen,
- 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
- das 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.

9.5.8 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

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

9.5.9 Zusicherungen und Gewährleistungen anderer Teilnehmer

Nicht anwendbar.

9.6 Haftungsausschluss

Der Anbieter haftet nur im vertraglich vereinbarten Umfang.

Schäden (inkl. Imageschäden), die durch missbräuchlichen oder Zertifikatsinhalt (Abschnitt 4.5.1 und) oder missbräuchliche Nutzung von Warenzeichen, Markenrechte (Abschnitt 3.1.6) entstehen, gehen zu Lasten des Auftraggebers für den Betrieb der cPKI.

9.7 Haftungsbeschränkungen

Der Anbieter haftet nur im vertraglich vereinbarten Umfang.

9.8 Schadenersatz

Schadenersatzansprüche sind einzelvertraglich mit dem Auftraggeber für den betrieb der cPKI geregelt.

9.9 Laufzeit und Beendigung

9.9.1 Laufzeit

Die Erstveröffentlichung dieses Dokuments „Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS))“ als auch dessen Änderungen treten mit der Veröffentlichung auf öffentlichen Webseiten der cPKI (siehe Abschnitt 2.2) in Kraft.

9.9.2 Beeindigung

Dieses Dokument verliert seine Gültigkeit mit dem Inkrafttreten einer neuen Version oder wenn der Betrieb der Corporate PKI eingestellt wird.

9.9.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung des Dienstes bleiben der Auftraggeber für den Betrieb der cPKI und alle Benutzer an die, in diesem CP/CPS enthaltenen Regelungen gebunden, bis das letzte ausgegebene Zertifikat seine Gültigkeit verliert oder gesperrt wird.

.

9.10 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Für individuelle Mitteilungen und Absprachen mit den Zertifizierungsstellen werden die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben.

9.11 Änderungen/Anpassungen der Richtlinie

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

9.11.1 Vorgehen bei Änderungen/Anpassungen

Änderungen dieser CP/CPS können nur von T-Systems Advisory Board durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und Veröffentlichungsdatum.

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

Aktualisierte Versionen dieses Dokuments setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet das T-Systems Advisory Board über weitere Vorgehensweise.

Innerhalb bestehender Verträge sind Änderungen dieser Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) mindestens sechs Wochen vor Wirksamwerden schriftlich dem Auftraggeber für den Betrieb der cPKI mitzuteilen. Bei Änderungen zu Ungunsten des Auftraggebers für den Betrieb der cPKI steht diesem ein Sonderkündigungsrecht zum Zeitpunkt des Wirksamwerdens der Änderung zu. Erfolgt seitens des Auftraggebers für den Betrieb der cPKI innerhalb von sechs Wochen nach Zugang der Änderungsmitteilung keine schriftliche Kündigung, werden die Änderungen zum Zeitpunkt des Wirksamwerdens Vertragsbestandteil.

9.11.2 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. Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Falls das T-Systems Advisory Board 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.

9.11.3 Gründe, unter denen die Objekt-Kennung (Objekt – ID) geändert werden muss

T-Systems Advisory Board entscheidet darüber, ob Änderungen der Objekt-ID der Zertifizierungsrichtlinie (Certificate Policy (CP)) / Erklärung zum Zertifizierungsbetrieb (Certifica-

tion Practice Statement (CPS)) notwendig werden. Andernfalls erfordern Änderungen keine Änderungen der Objekt-ID der Zertifikatsrichtlinie

9.12 Regelung von Unstimmigkeiten

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

9.13 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Frankfurt am Main, Deutschland.

9.14 Einhaltung geltenden Rechts

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

9.15 Verschiedene Bestimmungen

9.15.1 Vollständiger Vertrag

Nicht anwendbar.

9.15.2 Abtretung der Rechte

Nicht anwendbar.

9.15.3 Salvatorische Klausel

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

9.15.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Nicht anwendbar.

9.15.5 Höhere Gewalt

Es gelten die einzelvertraglichen Regelungen, welche mit dem Auftraggeber für den Betrieb der cPKI vereinbart wurden, und auf die an dieser Stelle verwiesen wird.

Innerhalb des gesetzlich zulässigen Rahmens müssen Verträge mit Auftrggebern, 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, nicht in Verzug zu geraten, wenn sich die Leistung infolge höherer Gewalt verzögert oder unmöglich wird.

9.16 Sonstige Bestimmungen

Nicht anwendbar.

A Akronyme und Begriffsdefinition

A.1 Akronyme

ARL	Authority Revcation List
DK	Dual Key
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PSE	Personal Security Environment
RA	Registration Authority
RFC	Requests for Comments
SLA	Service Level Agreement
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Socket Layer
TLS	Transport Layer Security
UPN	User Principal Name
URL	Uniform Resource Locator

UTC	Universal Time Coordinated
XML	Extensible Markup Language

A.2 Begriffsdefinition

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.

Authority Revocation List (ARL)

Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (außer Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.

Certificate Policy (CP)

Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.

Certificate Signing Request (CSR)

Von einem Gerät (z.B. Server) elektronisch erstellt und mit dem privaten Schlüssel signierter Zertifikatsantrag, der in kodierter Form den öffentlichen Schlüssel und die Zertifikatsdaten enthält. Die Syntax wird durch den Standard PKCS#11 beschrieben.

Certificate Revocation List (CRL)

Siehe Sperrliste.

Certification Authority (CA)

Siehe Zertifizierungsstelle.

Certification Practice Statement (CPS)

Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.

Chipkarte

Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.

Digitale Signatur

Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.

Distinguished Name

Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.

Domain-Name

Die Bezeichnung, die einem Knoten im Domain Name System (DNS) zugeordnet ist.

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.

Das beninhaltet insbesondere eine Beschreibung der Verfahrensweise, wie die Zertifizierungsstelle (CA) Zertifikate ausstellt, verwaltet, sperrt und erneuert.

Erlaubte Internet-Domänen

Ein Domänenname, der aus der Top-Level-Domain und weiteren Sub-Domains besteht, und nach erfolgreicher Prüfung durch die interne Registrierungsstelle als „erlaubte Internet-Domäne“ in die PKI-Konfiguration des Mandanten (Master-Domäne) aufgenommen wird.

Gerät

Komponente wie beispielsweise Router, Server, Gateway, Applikation, die zertifikatsbasierende Funktionen unterstützen, selbst aber nicht oder nur begrenzt selbst Zertifikate beantragen können. Häufig werden Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.

Geräte-Zertifikat

X.509 V3 Zertifikat, welches im commonName-Feld (CN) des distinguishedName des Zertifikatnehmers (Subject) und/oder in mindestens einer subjectAltName-Erweiterung entweder einen Hostname, IP-Adresse oder Mail-Adresse enthält.

Gültiges Zertifikat

Ein Zertifikat, das dem in RFC 5280 dargelegten Validierungsverfahren besteht.

Gültigkeitsdauer

Der Zeitraum vom Ausstellungsdatum (not before) des Zertifikats bis zum Ablaufdatum (not after).

Hardware Security Modul (HSM)

Hardware zur sicheren Erzeugung und Speicherung privater Schlüssel.

Hashwert

In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem glei-

chen 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.

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 Standrad-Mail-Anwendungen unterstützen.

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.

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)

Ein Protokoll zur Online-Zertifikatsvalidierung, mit dessen Hilfe die Anwendungssoftware der vertrauenden Seite den Status eines identifizierten Zertifikats bestimmen kann. Siehe auch OCSP-Responder.

OCSP-Responder

Ein Online-Server, der der Zertifizierungsstelle (CA) untersteht und mit deren zentrale Datenablage (Repository) zur Bearbeitung von Zertifikatsstatusanfragen verbunden ist. Siehe auch Online Certificate Status Protocol (OCSP).

Öffentlicher Schlüssel

Der Schlüssel eines Schlüsselpaares, der vom Inhaber des entsprechenden privaten Schlüssels offen gelegt werden darf und der von der vertrauenden Seite verwendet wird, um digitale Signaturen zu verifizieren, die mit dem privaten Schlüssel des Inhabers erstellt wurden, und/oder um Mitteilungen zu verschlüsseln, die nur mit dem zugehörigen privaten Schlüssel des Inhabers entschlüsselt werden können.

Personal Identification Number (PIN)

Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.

Personal Security Environment (PSE)

In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.

Privater Schlüssel

Der Schlüssel eines Schlüsselpaares, der vom Schlüsselpaarinhaber geheim gehalten und verwendet wird, um digitale Signaturen zu erstellen und/oder elektronische Daten und Dateien zu entschlüsseln, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.

Public Key Infrastructure X.509 (PKIX)

Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.

Policy

Richtlinien bzw. Erklärung, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.

Personal Security Environment (PSE)

In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.

Public Key Infrastruktur

Hardware, Software, Personen, Verfahren, Regeln, Richtlinien und Verpflichtungen, mit denen die vertrauenswürdige Generierung, Ausstellung, Verwaltung und Verwendung von Zertifikaten und Schlüsseln auf der Basis der Public-Key-Kryptographie ermöglicht wird.

Qualifizierter Auditor

Eine natürliche oder juristische Person, welche die an sie gestellten Anforderungen erfüllt.

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 offen gelegt 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

Das 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.

Software-PSE (Soft-PSE)

Eine verschlüsselte Datei zur Speicherung des Zertifikats und den zugehörigen privaten und öffentlichen Schlüssel.

Smartcard

Spezielle Plastikkarte mit integriertem Computerchip, die auch für kryptografische Anwendungen eingesetzt werden kann.

Sperrberechtigte(r)

Person, die von einem Zertifikatnehmer oder Schlüsselverantwortlichen autorisiert ist, ein Zertifikat für eine Personen- und Funktionsgruppe, juristische Person oder Gerät sperren zu dürfen. Die Autorisierung erfolgt über das Zertifikatssperrpasswort.

Sperrinstanz

Ein Mitarbeiter (Beschäftigter) oder Vertreter einer Organisation, der Zertifikatssperrungen durchführt.

Stammzertifizierungsstelle (Root-CA)

Die oberste Zertifizierungsstelle, deren Stammzertifikat von Anwendungssoftwareanbietern verteilt wird und die untergeordnete CA-Zertifikate (Sub-Zertifikate) ausstellt.

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 Zertifikate. 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.

Triple-Key-Zertifikat

Variante, bei der für Verschlüsselung, Signatur und Microsoft Smartcard-LogOn getrennte Schlüsselpaare verwendet werden. D.h. ein Benutzer besitzt drei entsprechende Zertifikate.

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 untergeordneten Zertifizierungsstelle (CA) signiert wird.

Validierung

Ein Nachweis der Reproduzierbarkeit eines Ergebnisses aus einer beschriebenen Vorgehensweise unter definierten Bedingungen. Je exakter eine Vorgehensweise beschrieben ist und je weniger unbekannte Einflussfaktoren bestehen, desto sicherer ist es, übereinstimmende Resultate zu erzeugen. Für eine Validierung benötigt man die Beschreibung des Zieles und des Weges. Valide bedeutet in diesem Zusammenhang, dass der Weg wiederholbar zum Ziel führt.

Im Kontext einer PKI besteht ein Validierungsprozess an folgenden Stellen:

- Mitteilung und Prüfung einer Identität (z.B. natürliche Person, Gerät) gegenüber dem Zertifikatsantrag.
- Algorithmus zur Überprüfung eines Zertifikats auf Gültigkeitsdauer (Gültigkeitszeitraum), ausstellende Zertifizierungsstellen und Zertifikatsstatus (gültig, gesperrt).

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).

WebTrust

Überprüfung und Bestätigung für Zertifizierungsstellen (WebTrust for Certification Authorities) durch einen unabhängigen Gutachter das die PKI nach den Webtrust-Kriterien „American Institut of Certified Public Accountants“ (AICPA) betrieben werden. Ziel der WebTrust-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken.

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) ausgestellten Sub-Zertifikate unterstützen.

Zertifikatnehmer

Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die rechtlich durch einen Bezugsvertrag oder Nutzungsbedingungen gebunden ist.

Zertifikatsantrag

Ein in elektronischer oder schriftlicher Form erstellter Antrag, der Daten zu einem Antragsteller enthält.

Zertifikatsdaten

Zertifikatsanträge und damit verbundene Daten (vom Antragsteller oder anderweitig eingeholt), die sich im Besitz der Zertifizierungsstelle (CA) befinden, die der Kontrolle durch die CA unterliegen oder auf die die CA Zugriff hat.

Zertifikatsproblembericht

Beschwerde wegen des Verdachts der Gefährdung des Schlüssels, des Zertifikatsmissbrauchs oder hinsichtlich anderer Arten von Betrug, Gefährdung, Missbrauch oder eines Fehlverhaltens im Zusammenhang mit Zertifikaten.

Zertifikatssperrliste (CRL)

Eine regelmäßig aktualisierte, mit Zeitstempel versehene Liste gesperrter (widerrufener) Zertifikate, die von der ausstellenden Zertifizierungsstelle (CA) generiert und digital signiert wird.

Die Authority Revocation List (ARL) ist ein Spezialfall der Zertifikatssperrliste (CRL), da sie nur Sub-CA-Zertifikate enthält

Zertifikatsverwaltungsprozess

Prozesse, Praktiken und Verfahren im Zusammenhang mit der Verwendung von Schlüsseln, Software und Hardware, mit deren Hilfe die Zertifizierungsstelle (CA) Zertifikatsdaten prüft, Zertifikate ausstellt, eine zentrale Datenablage (Repository) unterhält und Zertifikate widerruft/sperrt.

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.

A.3 Quellenverzeichnis

[BDSG] Datenschutzgesetz und BDSG-Novelle 2009

[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“

[PKCS] RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“, http://www.rsasecurity.com/rsalabs

[PKIX] RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)

[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003

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

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

[RFC 2560] X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP

[SAS 70] Statement on Auditing Standards (SAS) No. 70, http://www.sas70.com/

[ISAE3402] ISAE3402-Report, International Standards for Assurance Engagements, http://isae3402.com/ISAE3402_reports.html

A 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 BridgeCA-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.