# Zertifizierungserklärung für die T-Systems Trust Center Public Key Infrastruktur der Root-CA "T-TeleSec GlobalRoot Class 3"

Certification Practice Statement, CPS

Version: 6.0
Stand: 08.05.2017
Status: freigegeben

# Impressum


| Herausgeber |
| --- |
| T-Systems International GmbH<br>Trust Center Services<br>Untere Industriestraße 20<br>57250 Netphen |

| Dateiname | Dokumentennummer | Dokumentenbezeichnung |
| --- | --- | --- |
| CPS_T-TeleSec_GlobalRoot_Class_3_V6.0_DE_freigegeben.docx | 1.3.6.1.4.1.7879.13.24 | Certification Practice Statement, CPS |

| Version | Stand | Status |
| --- | --- | --- |
| 6.0 | 08.05.2017 | freigegeben |

| Autor | Inhaltlich geprüft von | Freigegeben von |
| --- | --- | --- |
| T-Systems International GmbH<br>Telekom Security Trust Center Services | M. Burkard<br>02.05.2017 | M. Etrich<br>08.05.2017 |

| Ansprechpartner | Telefon | E-Mail |
| --- | --- | --- |
| Servicedesk | Tel: +49 1805 268 204 | telesec_support@t-systems.com |

| Kurzinfo |
| --- |
| Certification Practice Statement für die T-Systems Trust Center Public Key Infrastruktur der T-TeleSec GlobalRoot Class 3 |

## Änderungshistorie

| Version | Stand | Bearbeiter | Änderungen / Kommentar |
|---|---|---|---|
| 0.1 | 08.02.2007 | L. Eickholt | Initialversion Entwurf |
| 0.3 | 13.02.2007 | L. Eickholt | Inhaltliche Aktualisierungen Entwurf |
| 0.7 | 19.03.2007 | M. Ulm, M. Graf, W. Pietrus | Inhaltliche Aktualisierungen Entwurf, Korrekturen |
| 0.9 | 30.03.2007 | L.Eickholt | Inhaltliche Aktualisierungen |
| 0.95 | 04.07.2007 | M. Ulm, L. Eickholt | Inhaltliche Aktualisierungen |
| 1.0 | 15.08.2007 | L.Eickholt | Inhaltliche Aktualisierung |
| 1.1 | 14.09.2007 | L.Eickholt, M. Ulm | Kapitel 3.1.3 aktualisiert, 3.2.4 Gelöscht Begriff „Endteilnehmer“, Kapitel 4.12 ergänzt, 5.4.1 Gelöscht Begriff „Endteilnehmer“, 6.3.1 Gelöscht Begriff „Endteilnehmer, Kapitel 6.2 aktualisiert, Kapitel 4.6 ergänzt, Kapitel 4.3.2 aktualisiert, Kapitel 4.9.3 aktualisiert, Kapitel 5.8 aktualisiert, Kapitel 8 komplett überarbeitet, , Kapitel 9.5 ergänzt, Kapitel 9.9 geändert in Kapitel 9.12, 9.12.1 und 9.12.2 hinzu gefügt, Kapitel 9.13 eingefügt, Kapitel 9.14 aktualisiert |
| 1.2 | 31.08.2010 | L.Eickholt, S.Kölsch, H.Gügel | Kapitel 1 aktualisiert, Kapitel 1.2 aktualisiert, Kapitel 1.3.1 aktualisiert, Kapitel 1.3.2.1 eingefügt, Kapitel 1.3.3.1 eingefügt, Kapitel 1.4.1.2 aktualisiert, Kapitel 1.4.2 hinzugefügt, Kapitel 1.5.1aktualisiert, Kapitel 1.5.2 aktualisiert, Kapitel 2.1 aktualisiert, Kapitel 2.2 aktualisiert, Kapitel 3.1.3 aktualisiert, Kapitel 3.4 aktualisiert, Kapitel 4.1.1 aktualisiert, Kapitel 4.1.2.1 eingefügt, Kapitel 4.2.1 aktualisiert, Kapitel 4.9.1 aktualisiert und ergänzt, Kapitel 4.9.8 aktualisiert, Kapitel 4.9.9 und 4.9.10 ergänzt, Kapitel 4.9.14 bis 4.9.16 hinzu gefügt, Kapitel 4.10 aktualisiert, Kapitel 6 aktualisiert, Kapitel 6.1.3 aktualisiert, Kapitel 6.1.7 aktualisiert, Kapitel 6.2 aktualisiert, Kapitel 6.3.2 aktualisiert, Kapitel 7.1.1.1 aktualisiert, Kapitel 7.2.1 ergänzt und aktualisiert, Kapitel 8 ergänzt, Kapitel 8.1 vervollständigt, Kapitel 9.1 aktualisiert, Kapitel (Finanzielle Verantwortlichkeiten ehem. 9.2) entfernt, Kapitel (Haftungsausschluss ehem. 9.5) entfernt, Kapitel (Haftungsbeschränkungen) aktualisiert, Kapitel 9.10 aktualisiert, Glossar aktualisiert |
| 1.3 | 08.03.2012 | L. Eickholt, C. Dahlenkamp | Kapitel 1.4.1.3 aktualisiert, Kapitel 1.4.2 aktualisiert, Kapitel 4.9.9 aktualisiert, Glossar aktualisiert |
| 1.3.1 | 24.05.2012 | L. Eickholt, C. Dahlenkamp | Klarstellung: Externe Sub-CAs sind nicht zulässig<br>Kapitel 1.3.1,1.3.3,1.4.1.3 und 4.1.2.1aktualisieren<br>Kapitel 1.3.2.1 und 1.3.3.1 gelöscht |
| 1.4 | 01.07.2012 | L. Eickholt, C. Dahlenkamp | Einarbeiten der Anforderungen der Baseline Requirements des CA/Browser Forums in der Version 1.0 |
| 2.0 | 17.06.2013 | L. Eickholt, B. Nakonzer | Anpassungen nach jährlichem Dokumentenreview |
| 2.1 | 23.05.2014 | B. Nakonzer | Wildcard Zertifikate aufgenommen |
| 3.1 | 25.03.2015 | B. Nakonzer | Änderungen nach Review |

| | | | |
|---|---|---|---|
| 4.1 | 15.03.2016 | B. Nakonzer | Revision 2016 |
| 5.0 | 14.04.2016 | A. Roth | Nach Freigabe |
| 5.1 | 05.04.2017 | B. Nakonzer | Kapitel 6.3.2, 7.1, 7.1.3, 8.4 aktualisiert |
| 5.2 | 03.05.2017 | A. Roth | Formelle QS |
| 6.0 | 08.05.2017 | A. Roth | Nach Freigabe |

# Inhaltsverzeichnis

# Abbildungsverzeichnis



# Tabellenverzeichnis

# 1 Einleitung

Das Trust Center wird durch die Konzerneinheit T-Systems International GmbH (im Folgenden „T-Systems“ genannt) betrieben. Es wird im Folgenden als **„T-Systems Trust Center“** bezeichnet.
Das T-Systems Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Stammzertifizierungsstellen (Root-CA). Die Zertifizierungsstellen der Zertifikats-Dienstleistungen unterscheiden sich hinsichtlich der Anwendungskontexte für Zertifikate, der konkreten Ausprägung der technischen Schnittstellen, Registrierungsverfahren, der Zertifikatsprofile, der Prozesse bei Sperrungen oder Suspendierungen, sowie der Veröffentlichung von Informationen.
Sowohl die bauliche als auch die organisatorische Infrastruktur erfüllt die strengen Anforderungen des deutschen Signaturgesetzes. Seit der Betriebsaufnahme hat das T-Systems Trust Center mehr als 4,6 Millionen Zertifikate ausgestellt. Zu den vom Trust Center angebotenen Leistungen gehört unter anderem der TeleSec Public Key Service (PKS), der die Ausstellung eIDAS konformer Signatur-Zertifikateumfasst.

## 1.1 Überblick

Bei dem vorliegenden Dokument handelt es sich um die Zertifizierungserklärung (engl. Certification Practice Statement, kurz CPS) für die PKI der Stammzertifizierungsstelle (Root-CA) „T-TeleSec GlobalRoot Class 3“, die im T-Systems Trust Center betrieben wird.
Das vorliegende CPS beschreibt das für den Betrieb der PKI erforderliche Sicherheitsniveau, siehe Kapitel 3.2 und beinhaltet Sicherheitsvorgaben sowie Erklärungen hinsichtlich technischer, organisatorischer und rechtlicher Aspekte. Das vorliegende CPS kann die Regelungen der CP weiter ergänzen, konkretisieren und verfeinern, nicht jedoch den Regelungen der CP widersprechen oder diese in ihrer Qualität und Wirksamkeit unterschreiten.
Das vorliegende Dokument orientiert sich am internationalen Standard für Zertifizierungsrichtlinien RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) der Internet Society.

Im Einzelnen behandelt das CPS die folgenden Aspekte:

- Veröffentlichungen und Verzeichnisdienst,
- Identifizierung und 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.

### 1.1.1 Einhaltung der Baseline Requirements des CA/Browser-Forums

Das Trust Center der T-Systems sichert zu, dass die Stammzertifizierungsstelle (Root-CA) „T-TeleSec Global-Root Class 3“ und alle untergeordneten Sub-CAs 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.

Nachgeordnete Sub-CAs müssen eine inhaltlich gleichwertige Zusicherung in ihrem jeweiligen CP oder CPS dokumentieren, sofern sie TLS/SSL Zertifikate ausstellen.

## 1.2 Dokumentenidentifikation

| | |
|---|---|
| Name: | Zertifizierungserklärung für die T-Systems Trust Center Public Key Infrastruktur der Root-CA "T-TeleSec GlobalRoot Class 3" |
| Version: | 6.0 |
| Datum | 08.05.2017 |
| Objektbezeichnung (Object Identifier) | 1.3.6.1.4.1.7879.13.24 |

## 1.3 PKI Beteiligte

### 1.3.1 Zertifizierungsstellen

Das T-Systems Trust Center betreibt die „T-TeleSec GlobalRoot Class 3“ Instanz für Zertifikatsdienste.
T-Systems stellt ausschließlich Zertifikate für untergeordnete Zertifizierungsstellen (Sub-CA) aus. Das Ausstellen von Zertifikaten für externe, untergeordnete Zertifizierungsstellen (Sub-CA), ist unter dieser Stammzertifizierungsstelle (Root-CA) nicht erlaubt.
Das Zertifikat der Stammzertifizierungsstelle (Root-CA) ist ein selbst-signiertes Zertifikat und wird durch T-Systems veröffentlicht. Die Veröffentlichung erlaubt eine Gültigkeitsüberprüfung aller in dieser Hierarchie ausgestellten Zertifikate. Die Stammzertifizierungsstellen (Root-CA) Instanz signiert ausschließlich Zertifikate von unmittelbar Untergeordneten Zertifizierungsstellen.
Die Struktur ist in der folgenden Abbildung schematisch dargestellt:

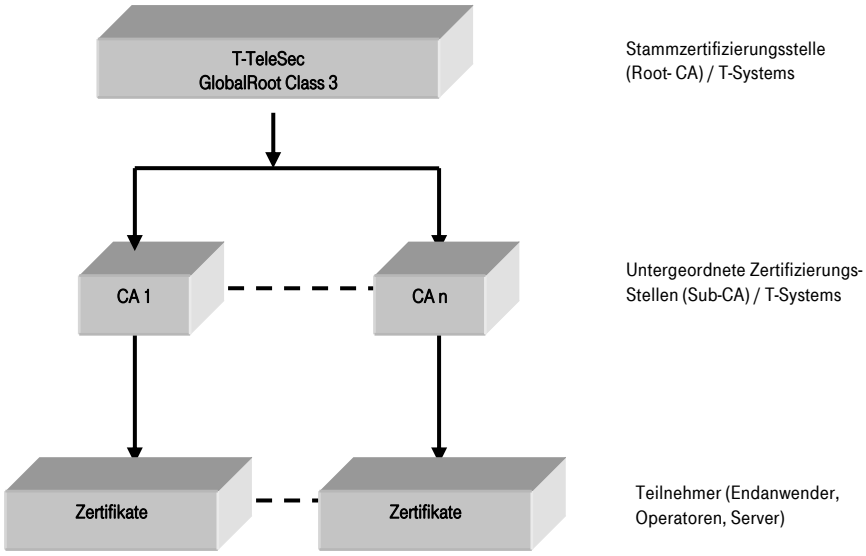


**Abbildung 1: Zertifizierungsstellen unter der „T-TeleSec GlobalRoot Class 3“ Instanz.**

Jede untergeordnete Zertifizierungsstelle (Sub-CA) verfügt über ein oder mehrere von der jeweiligen Stammzertifizierungsstelle (Root-CA) ausgestellte CA- und Dienste-Zertifikate, die in regelmäßigen Abständen neu ausgegeben werden.
Alle oben dargestellten Zertifizierungsstellen werden von T-Systems betrieben und unterliegen der „T-TeleSec-GlobalRoot-CP“.

### 1.3.2 Registrierungsstellen

Die Zertifizierungsstelle „T-TeleSec GlobalRoot Class 3“ betreibt nur eine zentrale Registrierungsstelle.

### 1.3.3 Zertifikatsnehmer

Zertifikate können je nach Zertifizierungsstelle an natürliche oder juristische Personen vergeben werden.
Der Zertifikatsnehmer

- beauftragt das Zertifikat (im Fall von juristischen Personen vertreten durch eine natürliche Person),
- wird von der Registrierungsstelle authentifiziert und durch das Zertifikat identifiziert,
- ist im Besitz des privaten Schlüssels, der zum öffentlichen Schlüssel im Zertifikat gehört.

### 1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle natürlichen oder juristischen Personen bzw. Organisationseinheiten, die Zertifikate von Zertifikatsnehmern im Rahmen von Anwendungen nutzen.

### 1.3.5 Andere Teilnehmer

Teilnehmer, die keine Verpflichtung gegenüber T-TeleSec GlobalRoot Class 3 eingegangen sind, werden in der Richtlinie nicht betrachtet.

## 1.4 Zertifikatsverwendung

### 1.4.1 Zulässige Verwendung von Zertifikaten

#### 1.4.1.1 Verwendung für natürliche Personen

Zertifikate werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Attribute zur Key Usage und den Festlegungen der CPS der jeweiligen Zertifizierungsstelle 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),
- Verschlüsselung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPSec, S/MIME, XML-ENC, SOAP),
- Festplattenverschlüsselung.

| Sicherheitsniveau | Verwendung | | |
|---|---|---|---|
| | signieren | verschlüsseln | Client Authentisierung |
| Hoch | ✓ | ✓ | ✓ |

**Tabelle 1: Verwendung für natürliche Personen**

Das Sicherheitsniveau ist in Kapitel 3.2 beschrieben.

#### 1.4.1.2 Verwendung für Organisationen

Die rechtliche Existenz einer Organisation ist sicherzustellen, des Weiteren sind die Organisationsmerkmale, die in das Zertifikat einfließen zu überprüfen (wie z.B.: der Domain-Name).
Tabelle 2 zeigt die gebräuchlichsten Verwendungen für Organisationszertifikate, es können aber auch weitere Möglichkeiten umgesetzt werden.

| Sicherheitsniveau | Verwendung | | | |
|---|---|---|---|---|
| | Code/Content Signing | SSL (Extended Validation) sichere SSL/TLS Internetsitzungen | Client-Authentisierung | Signieren und Verschlüsselung |
| Hoch | ✓ | ✓ | ✓ | ✓ |

**Tabelle 2: Verwendung für Organisationen**

Das Sicherheitsniveau ist in Kapitel 3.2 beschrieben.

#### 1.4.1.3 Zertifikate bei CA-Verkettung

T-Systems stellt keine Sub-CA-Zertifikate aus, die in einem MitM-Szenario (auch „transparentes Traffic Management genannt) für Domains oder IP-Adressen verwendet werden dürfen, welche der Zertifikatsinhaber (subscriber) nicht rechtmäßig besitzt oder kontrolliert.

### 1.4.2 Unzulässige Verwendung von Zertifikaten

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

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

Es ist außerdem nicht zulässig ein ausgestelltes Sub-CA Zertifikat für ein MitM-Szenario, wie in Kapitel 1.4.1.3 beschrieben, zu verwenden.

## 1.5 Verwaltung der Richtlinie

### 1.5.1 Zuständigkeit für die Richtlinie

Dieses Dokument (CP/CPS) wird herausgegeben von T-Systems International GmbH, ICTO–SDM CSS & Special Services–PSS-Security Solutions- Trust Center Services..

### 1.5.2 Kontaktinformationen

Adresse:
T-Systems International GmbH
Telekom Security
Trust Center Services
Untere Industriestraße 20
57250 Netphen
Deutschland

| | |
|---|---|
| Telefon: | +49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute) |
| E-Mail: | telesec_support@t-systems.com |
| Fax: | +49 (0) 2151 36607972 |
| WWW: | http://www.telesec.de |

### 1.5.3 Pflege der Richtlinie

Dieses CPS behält Gültigkeit, solange sie nicht von der zuständigen Instanz (siehe Kapitel 1.5.1) widerrufen wird. Sie wird bei Bedarf fortgeschrieben, und erhält dann jeweils eine neue aufsteigende Versionsnummer.

### 1.5.4 Genehmigungsverfahren dieses Dokuments (CP/CPS)

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

Die vorliegende CP/CPS wird unabhängig von weiteren Änderungen einem jährlichem Review unterzogen. Verantwortlich für die Durchführung bzw. die Koordination des Reviews ist der in Kapitel 1.5.3 benannte Bereich.
Das jährliche Review ist in der Änderungshistorie des CP/CPS zu vermerken. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden.

## 1.6 Definitionen und Abkürzungen

Siehe Kapitel 10 (Glossar).

# 2 Veröffentlichung und Verantwortlichkeiten für den Verzeichnisdienst

## 2.1 Verzeichnisdienst

Das T-Systems Trust Center stellt den Zertifikatsnutzern der PKI im Internet eine öffentlich und international erreichbare ARL (7 x 24h) zur Verfügung.

LDAP:
ldap://pki.telesec.de/CN=T-TeleSec%20GlobalRoot%20Class%203,OU=T-Systems%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?AuthorityRevocationList

WWW/HTTP:
http://pki.telesec.de/rl/GlobalRoot_Class_3.crl

## 2.2 Veröffentlichung von Zertifikatsinformationen

Das T-Systems Trust Center stellt den Zertifikatsnutzern der PKI folgende Informationen zur Verfügung:

- das Root-CA Zertifikat und dessen Fingerprint (MD5 und SHA1),
- Dokumentation über den Wechsel eines Root-CA oder eines CA-Zertifikats,
- Informationen über eine Kompromittierung, den Verdacht auf Kompromittierung oder die Sperrung eines Root-CA- oder CA-Zertifikats
- CPS im Status Freigegeben.

Die Internetseiten sind unter http://www.telesec.de/pki/index.html zu erreichen.

## 2.3 Veröffentlichungsfrequenz

Sperrinformationen für Root-CA- und CA-Zertifikate werden im Fall einer Sperrung umgehend aktualisiert (CRL, Repository für OCSP Abfragen). CPS und ggf. weitere Informationen werden auf den Internetseiten zur Verfügung gestellt.

## 2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf die in Abschnitt 2.1. und 2.2. aufgeführten Informationen unterliegt für die Zertifikatsnehmer und -nutzer einer Zertifizierungsstelle keiner Zugangskontrolle.
Der schreibende Zugriff auf alle in Abschnitt 2.1.und 2.2 genannten Informationen erfolgt ausschließlich durch berechtigte Mitarbeiter bzw. autorisierte Systeme.

# 3 Identifizierung und Authentifizierung

## 3.1 Namensregeln

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

### 3.1.1 Namensform

Die Namensregeln für den „SubjectDistinguishedName“ (Subject DN) und „IssuerDistinguishedName“ (Issuer DN) müssen nach dem X.501-Standard definiert sein. Die Anforderungen an die Nutzung von Namensattributen im Subject DN und Subject Alternative Name hängen konkret vom Anwendungskontext einer Zertifizierungsstelle ab. Beispielsweise muss für Zertifikate, die für sichere E-Mail genutzt werden, die E-Mail Adresse des Zertifikatsnehmers eingetragen sein. Allgemein sollte im Subject DN das Attribut „CommonName“ (CN) enthalten sein. Im Issuer DN muss das Attribut „CommonName“ (CN) enthalten sein. Zertifikate mit Wildcard-FQDN sind erlaubt. Das gilt nicht für Zertifikate mit EV-Merkmal ( Extended-Validation-Zertifikate). Verwirrende oder missverständliche Angaben sind nicht zulässig.
In den CP/CPS der nachgelagerten Services sind die Konventionen für die Bestandteile des Subject DN zu beschreiben.

### 3.1.2 Aussagekräftigkeit von Namen

Der Name im „SubjectDistinguishedName“ sowie „SubjectAlternativeName“ muss den Zertifikatsnehmer immer eindeutig identifizieren. Abkürzungen des z.B. im Handelsregister eingetragenen Namens sind aufgrund der begrenzten Zeichenanzahl zulässig. Durch die verwendete Abkürzung darf es nicht zu einer Irreführung kommen.

### 3.1.3 Pseudonymität / Anonymität

Wenn Zertifikate mit Pseudonymen erstellt werden, muss die Zertifizierungsstelle die reale Identität des Zertifikatsnehmers in ihren Unterlagen festhalten.
Auf expliziten Wunsch kann dem Antragsteller auch ein anonymes Zertifikat ausgestellt werden. In diesem Fall kann der Antragsteller ein Pseudonym wählen, das in das Zertifikat aufgenommen wird, wobei Pseudonyme mit dem Suffix „:PN“ kenntlich gemacht werden. Falls das gleiche Pseudonym mehr als einmal existiert, wird es durch das Hinzufügen einer Nummer eindeutig gemacht. Die Wahl von Pseudonymen unterliegt verschiedenen Namenseinschränkungen (ausgeschlossen sind z.B. Namen wie „Telekom CA“, politische Parolen, Namen, die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt).

Die Zertifizierungsstelle übermittelt die Identität eines Signaturschlüssel-, Verschlüsselungsschlüssel- und Authentisierungsschlüssel-Inhabers mit Pseudonym an die zuständigen Stellen soweit dies der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Auflagen der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist

oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.

### 3.1.4 Regeln zur Interpretation verschiedener Namensformen

Die Belegung für die Namensfelder müssen sich an den X.501 Standard halten.

### 3.1.5 Eindeutigkeit von Namen

Die Namen von Root-CA und CA-Zertifikaten, die vom T-Systems Trust Center herausgegeben werden, müssen eindeutig sein.

### 3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Es liegt in der Verantwortung des Zertifikatsnehmers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Die Zertifizierungsstelle ist nicht verpflichtet, solche Rechte zu überprüfen.
Allein der Zertifikatnehmer ist für solche Überprüfungen verantwortlich. Falls eine Zertifizierungsstelle über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat widerrufen.

## 3.2 Identitätsprüfungen bei Neuauftrag mit Sicherheitsniveau Hoch

Das beauftragte Sicherheitsniveau ist an jeder Stelle der Vertrauenskette zu gewährleisten. Ein beauftragtes Sicherheitsniveau kann in der Vertrauenshierarchie stärker, jedoch in keiner Stufe schwächer werden.

### 3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

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

### 3.2.2 Authentifizierung einer Organisation

Grundvoraussetzung für die Beauftragung einer Zertifizierungsstelle ist der Abschluss eines Vertrags. Dieses Vertragsverhältnis wird durch T-Systems Vertriebseinheiten mit juristischer Zuhilfenahme generiert.
Für die Authentifizierung von Organisationen gelten die folgenden Validierungsverfahren:

- Feststellung der Existenz der Organisation
- Prüfung von Firmenname und Geschäftsadresse

Um die Validierung durchzuführen verwendet die CA oder die RA, die von staatlicher Stelle oder Behörde ausgestellten Organisationsdokumente.
Für die Authentifizierung von Organisationen werden, dem Sicherheitsniveau entsprechende, Anforderungen gestellt.

### 3.2.3 Authentifizierung einer natürlichen Person

Für die Authentifizierung von natürlichen Personen werden die folgenden Anforderungen gestellt:
Sicherheitsniveau Hoch

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

- Feststellung der Existenz der natürlichen Person anhand von nachprüfbaren Identifikationsmerkmalen.
- Persönliche Vorsprache mit einem amtlich ausgestellten Ausweisdokuments mit Lichtbild, bei einer CA oder RA.

Um nachprüfbare Identifikationsmerkmale zu verifizieren kann die CA oder RA auf einen von T-Systems anerkannten Identitätsprüfungsservice oder eine Identitätsprüfungsdatenbank eines Dritten oder die von staatlicher Stelle oder Behörde ausgestellten Organisationsdokumente zurückgreifen.

### 3.2.4 Nicht verifizierte Teilnehmerinformationen

Alle Informationen, welche in ein Zertifikat übernommen werden, müssen verifiziert werden.

### 3.2.5 Überprüfung der Berechtigung

Die Autorisierung einer natürlichen Person als handlungsberechtigt im Namen einer Organisation oder natürlichen Person ist durch den Vertragsabschluss und die damit im Vorfeld einhergehende Zuordnung der Verantwortlichkeiten gewährleistet.
Es ist zu prüfen , ob der Auftraggeber das Recht zur Verwendung der Domain oder IP-Adresse besitzt. Es wird keine Prüfung gegen CAA-Einträge im DNS durchgeführt.

### 3.2.6 Kriterien für Interoperabilität

Verwendet eine Sub-CA in einem von ihr ausgestellten Zertifikat eine Policy-OID, welche die Erfüllung und Einhaltung der [CAB-BR] repräsentiert, muss das jeweilige CP oder CPS der Sub-CA eine explizite Zusicherung enthalten, dass alle von der Sub-CA ausgestellten Zertifikate, welche diese Policy-OID enthalten, in Übereinstimmung mit den und unter Einhaltung der von den [CAB-BR] gestellten Vorgaben stehen.

## 3.3 Identitätsprüfung und Authentifizierung bei einer Zertifikatserneuerung

Zur Zertifikatserneuerung muss die Identitätsprüfung bei Neuauftrag (siehe Kapitel 3.2) durchlaufen werden.

## 3.4 Identifizierung und Authentifizierung bei Sperranträgen

Das T-Systems Trust Center bietet einen zentralen Sperrservice, um im Falle des Verlustes oder bei Missbrauchsverdacht das eigene Zertifikat sperren zu können. Im Falle der Sperrung wird das Zertifikat in eine Sperrliste aufgenommen. Zur Sperrung autorisierte Personen und Institutionen (siehe Kapitel 4.9) können die Sperrung eines Zertifikates entweder per E-Mail oder telefonisch beauftragen.
Die Authentisierung einer Sperrung geschieht durch die Angabe der Grunddaten (Name, Firma, Rückrufnummer, E-Mailadresse). Der Sperrwunsch wird durch die Angabe des Sperrpasswortes autorisiert.
Für die Sperrung sind die folgenden Eingangskanäle zu verwenden:
Telefonisch: +49 (0) 1805-268204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)
E-Mail: telesec_support@t-systems.com

# 4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

## 4.1 Zertifikatsbeauftragung

### 4.1.1 Wer kann ein Zertifikat beauftragen?

Der Zertifikatsnehmer bzw. eine im Sinn von Kapitel 3.2.2 und 3.2.3 autorisierte Person kann Zertifikate beauftragen.

### 4.1.2 Auftragsstellungsverfahren und Pflichten

Ein Zertifikat für Zertifizierungsstellen kann erst erzeugt werden, wenn der Registrierungsprozess beim Auftragsmanagement für TeleSec Produkte erfolgreich abgeschlossen und dokumentiert wurde.
Telefon Auftragsmanagement: +49 271 708-1500
Telefax: +49 1805 3344900091
PC-Fax.: +49 521 98840091
E-Mail: telesec-auftrag@t-systems.com
Der Registrierungsprozess beinhaltet mindestens die folgenden Schritte:
Abgeschlossener Vertrag liegt vor,

- Vorlage des Zertifikatsauftrags unter Verwendung der von der Zertifizierungsstelle vorgegebenen Mechanismen (z.B. signierter Online Auftrag im Format PKCS#10),
- ggf. Vorlage weiterer Dokumente zur Autorisierung und Identifizierung gemäß dem Sicherheitsniveau für Organisationen oder natürliche Personen,
- Nachweis des Besitzes des privaten Schlüssels gemäß Kapitel 3.2.1,
- vollständige Überprüfung der Auftragsdaten durch die Registrierungsstelle,
- Archivierung der Auftragsdaten.

#### 4.1.2.1 Registrierungsprozess bei CA-Verkettung

Um als Sub-CA der „T-TeleSec GlobalRoot Class 3“ fungieren zu können, ist die Beantragung eines Root-Zertifikats zur CA-Verkettung notwendig (nur für interne Dienste verfügbar – siehe 1.3.1 Zertifizierungsstellen). Der Registrierungsprozess beinhaltet mindestens die in Kapitel 4.1.2 genannten Schritte. Zusätzlich müssen die in [TSYSROOTSIGN] genannten Anforderungen erfüllt werden.

## 4.2 Bearbeitung des Zertifikatsauftrags

### 4.2.1 Durchführung der Identifikation und Authentifizierung

Die zuständige Registrierungsstelle führt die Identifizierung und Authentifizierung gemäß den Festlegungen dieses CPS durch.

### 4.2.2 Genehmigung oder Abweisung von Zertifikatsaufträgen

Nur bei erfolgreicher Überprüfung wird ein Zertifikatsauftrag angenommen und zur Bearbeitung weitergeleitet. Dies ist gegeben, wenn die Identifikation und Authentifikation aller erforderlichen Kundendaten erfolgreich war. (siehe Kapitel 3.2)
Im Falle einer Abweisung des Auftrags wird der Zertifikatsnehmer in geeigneter Weise unter Angabe von Gründen benachrichtigt.

### 4.2.3 Bearbeitungsdauer von Zertifikatsaufträgen

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

## 4.3 Ausstellung von Zertifikaten

### 4.3.1 Maßnahmen der CA während der Ausstellung von Zertifikaten

Die Zertifizierungsstelle erhält in der Regel geprüfte Aufträge von der zuständigen Registrierungsstelle. Die Kommunikation mit der Registrierungsstelle erfolgt durch persönliche Übergabe oder durch signierte und verschlüsselte E-Mail Kommunikation.
In der Zertifizierungsstelle erfolgt eine Prüfung des Auftrags hinsichtlich der zulässigen technischen Formate und Zeichensätze. Danach wird das Zertifikat erzeugt. Sowohl im Fall der Schlüsselerzeugung auf Seiten des Zertifikatsnehmers wie auch im Fall der Schlüsselerzeugung durch die Zertifizierungsstelle muss eine eindeutige Zuordnung zwischen dem Zertifikatsnehmer und dem Schlüsselpaar bestehen.

### 4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung von Zertifikaten

Der Zertifikatsnehmer erhält eine Benachrichtigung über die Ausstellung des Zertifikats in geeigneter Weise. Es bestehen verschiedene Möglichkeiten der Auslieferung des Zertifikats:

- das ausgestellte Zertifikat wird an den Zertifikatsnehmer per E-Mail gesendet,
- das ausgestellte Zertifikat wird an den Zertifikatsnehmer per Datenträger (CD) auf dem Postweg per Einschreiben gesendet.
- das ausgestellte Zertifikat wird an den Zertifikatsnehmer persönlich übergeben.

## 4.4 Zertifikatsannahme

### 4.4.1 Akzeptanz durch den Zertifikatsnehmer

Vom Zertifikatsnehmer ist eine Annahmebestätigung (Akzeptanzbestätigung CA Zertifikat.rtf) innerhalb von 7 Tagen an die Zertifizierungsstelle erforderlich.

### 4.4.2 Veröffentlichung des Zertifikats durch die CA

Die Veröffentlichung von Zertifikaten in öffentlichen Verzeichnissen ist nicht vorgesehen. Es gelten die Regelungen aus Kapitel 2.1.

### 4.4.3 Benachrichtigung anderer Stellen über die Zertifikatsausstellung durch die CA

Die Benachrichtigung weiterer Stellen ist nicht vorgesehen.

## 4.5 Verwendung von Schlüsselpaar und Zertifikat

### 4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die im Rahmen dieses CPS ausgestellten Zertifikate werden ausschließlich für Zertifizierungsstellen ausgestellt. Der Zertifikatsnehmer sichert die Einhaltung der Sicherheitsanforderungen zu.

### 4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Vertrauende Dritte (Relying Parties)

Jeder, der ein Zertifikat, welches im Rahmen dieses CPS ausgestellt wurde, einsetzt sollte

- vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert und
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit dem jeweiligen CPS einsetzen.

## 4.6 Zertifikatserneuerung (Re-Zertifizierung)

Sub-CA-Zertifikate:
Eine Zertifikatserneuerung von CA-Zertifikaten ist nicht vorgesehen.

EE-Zertifikate:
Bei einer Re-Zertifizierung wird dem Zertifikatsnehmer ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaares ausgestellt, sofern die im Zertifikat enthaltenen Informationen sich nicht geändert haben. Dies setzt voraus, dass die 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. Re-Key von EE-Zertifikaten ist möglich, siehe Kapitel 4.7.

### 4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung von CA-Zertifikaten ist nicht vorgesehen.

### 4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Die Zertifikatserneuerung kann nur durch den Zertifikatsnehmer beauftragt werden.

### 4.6.3 Ablauf der Zertifikatserneuerung

Es gelten die Regelungen von Kapitel 3.3.

### 4.6.4 Benachrichtigung des Zertifikatsnehmers

Es gelten die Regelungen gemäß Kapitel 4.3.1.

### 4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.1.

### 4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

### 4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.3.

## 4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

Beim Re-Key wird ein neues Schlüsselpaar verwendet. Ansonsten gelten sinngemäß alle Aussagen aus Kapitel 4.6.
Detailinformationen sind in den CP/CPS der nachgelagerten Services zu beschreiben.

## 4.8 Änderung von Zertifikatsdaten

Wenn sich Informationen im vorhandenen Zertifikat ändern, dann muss das Zertifikat neu beauftragt werden.
Detailinformationen sind in den CP/CPS der nachgelagerten Services zu beschreiben.

## 4.9 Zertifikatssperrung und Suspendierung

### 4.9.1 Gründe für eine Sperrung

Die folgenden Gründe erfordern die Zertifikatssperrung durch den Zertifikatsnehmer:

- Der private Schlüssel wurde kompromittiert, verloren, gestohlen oder offen gelegt oder es besteht ein dringender Verdacht, dass dies geschehen ist.
- Die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr aktuell, ungültig oder falsch.
- Der zertifizierte Schlüssel (öffentliche Schlüssel) oder die damit verwendeten kryptografischen Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.

- Ein Missbrauch oder Verdacht auf Missbrauch durch zur Nutzung des Schlüssels berechtigte Personen liegt vor.
- Gesetzliche Vorschriften oder richterliche Urteile.
- Das Zertifikat wird nicht mehr benötigt bzw. der Zertifikatnehmer verlangt ausdrücklich die Sperrung des Zertifikats.
- Bei CA-Verkettung: Es wird von den vertraglich geregelten und in [TSYSROOTSIGN] dargelegten Regelungen abgewichen.

Das T-Systems Trust Center sperrt Zertifikate, wenn folgende Gründe vorliegen:

- Bekanntwerden des Abhandenkommens 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.
- Die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Informationen) sind nicht mehr korrekt.
- Es liegt ein Missbrauch oder Verdacht auf Missbrauch des Zertifikats durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen vor.
- Verwendung und Handhabung des Zertifikats im Widerspruch zu den AGB (Allgemeine Geschäftsbedingungen) oder der Zertifikats- bzw. Zertifizierungsrichtlinie (CP/CPS).
- Der zertifizierte Schlüssel oder die damit verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.
- Bei Feststellung, dass eine wesentliche Voraussetzung für die Ausstellung des Zertifikats weder erfüllt war noch auf deren Erfüllung verzichtet wurde.
- Die Zertifizierungsstelle stellt den Betrieb ein.
- Gesetzliche Vorschriften oder richterliche Urteile.
- Der Zertifikatnehmer verfügt nicht mehr über die Berechtigung, das Zertifikat zu nutzen.

### 4.9.2 Wer kann eine Sperrung beauftragen?

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

- autorisierte Personen in Vertretung für juristische Personen.
- Registrierungsmitarbeiter des T-Systems Trust Centers.

Insbesondere gelten die Regelungen aus Kapitel 3.4.

### 4.9.3 Ablauf einer Sperrung

Zur Sperrung autorisierte Personen und Institutionen können die Sperrung eines Zertifikates entweder per E-Mail oder telefonisch beauftragen. Die Authentisierung einer Sperrung geschieht in geeigneter Art und Weise. Sind die Voraussetzungen zur Sperrung erfüllt, wird die Sperrung vorgenommen und das gesperrte Zertifikat in die Sperrinformationen übernommen. Die Sperrinformationen werden standardkonform (ARL) bereitgestellt. Die autorisierte Person oder Institution wird über die Durchführung der Sperrung in geeigneter Weise informiert.

### 4.9.4 Fristen für einen Sperrauftrag

Der Zertifikatsnehmer muss bei Vorliegen entsprechender Gründe unverzüglich die Sperrung initiieren.

### 4.9.5 Fristen für die Bearbeitung eines Sperrauftrags durch die CA

Die Sperraufträge werden vom Sperrservice siehe Kapitel 3.4 entgegen genommen und per Trouble-Ticket-System an das T-Systems Trust Center weiter geleitet. Dort wird die Sperrung nach Erhalt umgehend durchgeführt und die Sperrliste erstellt und veröffentlicht.

### 4.9.6 Überprüfungsmethoden für Vertrauende Dritte

Sperrinformationen werden in standardisierter Form (ARL) im DER–Format bereitgestellt und können daher mit Standard-konformen Anwendungen geprüft werden.

### 4.9.7 Frequenz der Veröffentlichung von Sperrinformationen

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

### 4.9.8 Maximale Latenzzeit von Sperrlisten

Die Sperrlisten stehen innerhalb einer wirtschaftlich angemessenen Zeit nach der Generierung im Verzeichnisdienst zur Verfügung.

### 4.9.9 Online Verfügbarkeit von Sperr-/Statusinformationen

Sperrinformationen, werden für die Zertifikatsnutzer online, siehe Kapitel 2.1, mit einem standardkonformen Verfahren bereitgestellt. Es sind alle von dieser Zertifizierungsstelle gesperrten CA-Zertifikate enthalten. Es stehen Online-Informationen zum Zertifikatsstatus via OCSP unter http://ocsp.telesec.de/ocspr bereit.

T-Systems betreibt einen von der Root-CA signierten OCSP-Responder um die Gültigkeit ausgestellter Sub-CA-Zertifikate zu validieren. OCSP-Antworten haben eine Gültigkeit von fünf (5) Tagen. Die OCSP-Datenbank wird bei Sperrung eines Zertifikates innerhalb eines Tages aktualisiert.

Vorgaben Sub-CAs:
Nachgeordnete Sub-CAs müssen einen eigenen OCSP-Responder für von ihnen ausgestellte EE-Zertifikate betreiben. OCSP-Antworten dürfen eine maximale Gültigkeit von zehn (10) Tagen haben (Feld nextUpdate). Sub-CAs haben mindestens alle vier (4) Tage ihre OCSP-Datenquelle (repository) zu aktualisieren.

### 4.9.10 Anforderungen an Online Überprüfungsverfahren

Vertrauende Dritte müssen den Status eines Zertifikats überprüfen, um Informationen darüber zu erhalten, ob ein Zertifikat, dem sie vertrauen möchten, vertrauenswürdig ist. Für den Abruf aktueller Statusinformationen steht der OCSP-Service (OCSP-Responder) zur Verfügung (siehe Kapitel 4.9.9).

### 4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Derzeit werden keine anderen Formen der Bekanntmachung eingesetzt.

### 4.9.12 Besondere Anforderungen bezüglich der Kompromittierung privater Schlüssel

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat möglichst unverzüglich zu sperren.

### 4.9.13 Suspendierung von Zertifikaten

Eine Suspendierung (Sperrgrund „on-hold“) für eine Zertifizierungsstelle ist nicht zulässig.

### 4.9.14 Wer kann eine Suspendierung beauftragen?

Nicht definiert.

### 4.9.15 Verfahren der einer Suspendierung

Nicht definiert.

### 4.9.16 Beschränkung des Suspendierungszeitraums

Nicht definiert.

## 4.10 Statusauskunftsdienste für Zertifikate

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

## 4.11 Beendigung der Zertifikatsnutzung

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

## 4.12 Schlüsselhinterlegung und Wiederherstellung

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

# 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. Zertifizierungsstellen, die in der Hierarchie von „T-TeleSec GlobalRoot Class 3“ des T-Systems Trust Center stehen, aber extern betrieben werden, müssen Regelungen wie die im folgenden beschriebenen in adäquater Weise umsetzen und in ihrer CPS beschreiben. Bei Bedarf müssen ergänzend auch sicherheitsrelevante Dokumente der externen Zertifizierungsstellen zur Prüfung auf Konformität mit diesem CPS der T-Systems vorgelegt werden.

## 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 verfügt. Je nach Kundenanforderung kann im Trust Center ein abgestuftes Ausfallsicherungskonzept mit definierten Sicherungsstufen realisiert werden.

Die Errichtung und der Betrieb des Trust Centers erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und 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 Putzkräfte), die Anlieferung von Material (Hardware, Zubehör, Betriebsmittel) und Ordnung am Arbeitsplatz sowie in Rechnerräumen beinhalten.

### 5.1.2 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 Ausnahmefälle und nach vorheriger Anmeldung empfangen. Hier gelten besondere Sicherheitsvorschriften.

### 5.1.3 Stromversorgung und Klimatisierung

Die Ansaugöffnungen für die Außenluft sind so angeordnet, dass keine Schadstoffe wie Staub und Schmutz, ätzende, giftige oder leicht brennbare Gase eindringen können. Die Systeme werden mit einem sehr geringen

Außenluftanteil betrieben. Die erforderlichen Zuluftöffnungen sind zugangsgeschützt. Zum Schutz gegen Luftverunreinigung durch schwebende Partikel sind Filter installiert. Die Frischluftansaugung wird ständig auf aggressive Gase überwacht. Im Notfall (z.B. Brand in der Umgebung) wird die Außenluftansaugung automatisch durch Luftklappen verschlossen.
Zum Ausfallschutz der Energieversorgung ist eine unabhängige Wechselspannungsversorgung entsprechend VDE-Vorschriften installiert. Sie bietet Schutz gegen Spannungsschwankungen, unterbrechungsfreie Kurzzeitüberbrückung, eine Langzeitüberbrückung mit zwei getrennten, ortsfesten Notstromaggregaten mit einer Leistung die der Volllast des Rechenzentrums entspricht.

### 5.1.4 Wassergefährdung

Das Trust Centers liegt in einer geschützten Lage, d.h. es liegt nicht in der Nähe von Gewässern und Niederungen (Hochwassergefahr). Die Brandbekämpfung erfolgt mit inertem Gas

### 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 Brandfrüherkennungssysteme (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut.

### 5.1.6 Aufbewahrung von Datenträgern

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

### 5.1.7 Entsorgung

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

### 5.1.8 Externe Sicherung

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

## 5.2 Organisatorische Maßnahmen

### 5.2.1 Vertrauenswürdige Rollen

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 CP/CPS festgelegten Anforderungen (siehe Kapitel 5.3.1) 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 Sicherheitskonzepten, im CP/CPS der vom T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

### 5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Die Aufrechterhaltung des Betriebs der Zertifizierungsstelle und des Verzeichnisdienstes (Administration, Sicherung, Wiederherstellung) wird von fachkundigen und vertrauenswürdigen Mitarbeitern wahrgenommen. Arbeiten an hochsensitiven Komponenten (z.B. Schlüsselerstellungssystem, HSM) sind durch besondere interne Kontrollverfahren geregelt und werden von mindestens zwei Mitarbeitern durchgeführt.

### 5.2.3 Identifizierung und Authentifizierung für jede Rolle

T-Systems Mitarbeiter, die als vertrauenswürdige Personen eingestuft sind und vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer T-Systems-internen Sicherheitsüberprüfung (siehe Kapitel 5.3.2).
T-Systems stellt sicher, dass Mitarbeiter einen vertrauenswürdigen Status erlangt haben und die Zustimmung der Abteilung erteilt wurde, bevor diese Mitarbeiter:

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

### 5.2.4 Rollen, die eine Aufgabentrennung erfordern

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

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

## 5.3 Personelle Maßnahmen

### 5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

T-Systems verlangt von seinen Mitarbeitern, die als vertrauenswürdige Personen tätig werden möchten, Nachweise vorzulegen über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.
In regelmäßigen Abständen, spätestens jedoch nach drei Jahren, ist ein neues Führungszeugnis der T-Systems vorzulegen.

### 5.3.2 Sicherheitsüberprüfung

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 der Kündigung von vertrauenswürdigen Personen beinhalten.
Die Verwendung von in einer Sicherheitsüberprüfung ermittelten Informationen zur Ergreifung solcher Maßnahmen unterliegt geltendem Recht.

### 5.3.3 Schulungs- und Fortbildungsanforderungen

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 von T-Systems sind auf die individuellen Tätigkeitsbereiche abgestimmt und beinhalten u.a.:

- fortgeschrittene PKI-Kenntnisse,
- Verfahrensweisen nach ITIL,

- 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).

### 5.3.4 Nachschulungsintervalle und -anforderungen

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

### 5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

### 5.3.6 Sanktionen bei unbefugten 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.

### 5.3.7 Anforderungen an unabhängige Auftragnehmer

T-Systems behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter von T-Systems in vergleichbarer Position.
Obiger Personenkreis, der die in Kapitel 5.3.2 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von T-Systems nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

### 5.3.8 Dokumentation für das Personal

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 Protokollereignisse

### 5.4.1 Art der aufgezeichneten Ereignisse

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

#### 5.4.1.1 CA-Schlüsselpaare und CA-Systeme

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

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

#### 5.4.1.2 5.4.1.2 EE- und CA-Zertifikate

Für das Lifecycle-Management von sowohl EE- als auch CA-Zertifikaten protokolliert das T-Systems Trust Center mindestens die folgenden Ereignisse:

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

#### 5.4.1.3 Sonstige sicherheitsrelevante Ereignisse

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

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

### 5.4.2 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft T-Systems die Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen.
Eingeleitete Maßnahmen, die als Reaktion aus der Auswertung von Audit-Protokollen/Logging-Dateien stammen, werden ebenfalls protokolliert.

### 5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Audit-Protokolle/Logging-Dateien werden nach Bearbeitung gemäß Kapitel 5.5.2 archiviert.

### 5.4.4 Schutz der Audit-Protokolle

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

### 5.4.5 Sicherungsverfahren für Audit-Protokolle

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

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

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

### 5.4.7 Benachrichtigung des Ereignisauslösenden Subjekts

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

### 5.4.8 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 Datensätze

T-Systems archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener Form,
- alle Audit-/Event-Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden.

### 5.5.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommener Sperrungen, sind für mindestens zehn (10) Jahre nach Ablauf der Zertifikatsgültigkeit vorzuhalten,
- Audit- und Event Logging Daten sind entsprechend den aktuellen gesetzlichen Bestimmungen zu archivieren.

### 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 inkrementelle Sicherung der elektronischen Archive wird täglich durchgeführt.

### 5.5.5 Anforderungen an Zeitstempel von Datensätzen

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

### 5.5.6 Archiverfassungssystem (intern oder extern)

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

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

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

Die Generierung neuer Schlüssel und Zertifikate wird dokumentiert und gemäß den Regelungen des Schlüsselgenerierungsverfahrens (Key Generation Ceremony) überwacht. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3).
Zertifikate können nur innerhalb des Gültigkeitszeitraums der hierarchisch übergeordneten Stammzertifizierungsstelle (Root-CA) erneuert werden. Abgelaufene oder gesperrte Zertifikate stehen weiterhin zu Validierung auf einer Webseite zur Verfügung.

## 5.7 Kompromittierung privater Schlüssel von Root-CA und Untergeordnete Zertifizierungsstelle (Sub-CA)

### 5.7.1 Umgang mit Störungen und Kompromittierungen

Störungen werden über in Kapitel 1.5.2 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 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 von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme einer Kompromittierung des privaten Schlüssels einer CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.
Endteilnehmer werden über die mögliche Kompromittierung über die einschlägigen Webseiten informiert (siehe hierzu Kapitel 2.3). Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechende Zertifizierungsstellen-Sperrliste (ARL) zu generieren und zu veröffentlichen.

### 5.7.4 Geschäftskontinuität nach einem Notfall

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

Der Notfallplan enthält mindestens die folgenden Informationen:

- Die notwendigen Kriterien für die Aktivierung des Planes
- Mögliche Notfallmaßnahmen (je nach Situation)
- Fallback Verfahren
- Wiederanlauf Verfahren
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung
- Bewusstsein-schaffende Maßnahmen
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals
- Die Verantwortung der Individuen (Rollenbeschreibung und -zuweisung)
- Wiederanlaufzeit (RTO)
- Regelmäßige Durchführung der Notfallpläne zu Testzwecken
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der Geschäftstätigkeit nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse
- Eine Verpflichtung kritische kryptographische Geräte und Informationen an einem anderen Standort zu sichern bzw. vorzuhalten.
- Festlegung der maximal tolerierbaren Ausfallzeit (MTD) und entsprechende Zeiten zur Wiederherstellung
- Häufigkeit, in der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur Hauptgeschäftsstelle bzw. zum Rechenzentrum des Trust Centers
- Verfahren zur bestmöglichen Sicherung der Betriebsstätten und –Einrichtungen nach einer Katastrophe (Notbetrieb) bis zur Wiederherstellung eines den Anforderungen entsprechend gesicherten Normalbetriebs

Im Rahmen eines Compliance-Audits (siehe Kapitel 8) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

## 5.8 Einstellung des Betriebes

Eine Betriebsbeendigung kann nur durch die T-Systems Geschäftsleitung ausgesprochen werden.
Falls eine T-Systems RA/CA den Betrieb einstellen muss, wird ein Beendigungsplan erstellt. Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen, betroffene nachgeordnete Stellen vorab über diese Betriebsbeendigungen zu informieren.

Ein Beendigungsplan kann die folgenden Regelungen enthalten:

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

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

# 6 Technische Sicherheitsmaßnahmen

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 in einem Sicherheitskonzept (nicht öffentlich verfügbar) dokumentiert.
Die folgenden Aussagen gelten für die vom T-Systems Trust Center betriebenen Zertifizierungsstellen. Zertifizierungsstellen, die in der Hierarchie von „T-TeleSec GlobalRoot Class 3“ des T-Systems Trust Center stehen, aber extern betrieben werden, müssen Regelungen wie die im folgenden beschriebenen in adäquater Weise umsetzen und in ihrer CPS beschreiben

## 6.1 Generierung und Installation von Schlüsselpaaren

### 6.1.1 Generierung von Schlüsselpaaren

Alle Schlüsselpaare für Root-CA- und CA-Zertifikate werden in abgeschirmter Umgebung und in einer sicherheitsüberprüften Hardwarekomponente erzeugt und auf einer Hardwarekomponente gespeichert.
Im Fall von Root-CA und CA-Zertifikaten werden die privaten Schlüssel auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140-2 evaluiert) erzeugt und abgelegt.

### 6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Der private Schlüssel einer Stammzertifizierungsstelle (Root-CA) oder einer untergeordneten Zertifizierungsstelle (Sub-CA) wird gesichert an den Zertifikatsnehmer ausgeliefert.

### 6.1.3 Lieferung öffentlicher Schlüssel der Zertifizierungsstelle an Zertifikatsnutzer

Öffentliche Schlüssel einer Zertifizierungsstelle können sowohl aus dem jeweiligen Verzeichnis als auch von den Webseiten der Zertifizierungsstelle (dort sind auch die entsprechenden Fingerprints veröffentlicht) bezogen werden (siehe hierzu auch Kapitel 1.5.3).

### 6.1.4 Lieferung öffentlicher Schlüssel an vertrauende Dritte

Die Lieferung von CA-Zertifikaten wird vertraglich mit dem Kunden vereinbart.

### 6.1.5 Schlüssellängen

RSA Schlüssel müssen eine Mindestlänge von 2048 besitzen.

### 6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Nicht relevant.

### 6.1.7 Schlüsselverwendungen

Die Schlüsselverwendungen der Root-CA- und CA-Zertifikate sind im Attribut „key usage“ festgelegt. Bei Root-CA- und CA-Zertifikaten ist das Attribut „key usage“ auf die Werte „keyCertSign“ und „cRLSign“ beschränkt. Bei CA-Zertifikaten, deren Schlüssel auch zur Signatur von Protokollnachrichten eingesetzt werden, kann zusätzlich der Wert „digitalSignature“ gesetzt sein.

## 6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

T-Systems hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA-Schlüsseln gewährleisten zu können.
Endteilnehmer sind verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um den Verlust, die Offenlegung oder die unberechtigte Nutzung von privaten Schlüsseln zu verhindern.

### 6.2.1 Standards und Kontrollen für kryptografische Module

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

### 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 kryptografische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels 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 von privaten Schlüsseln

Eine Hinterlegung von privaten Schlüsseln bei Treuhändern außerhalb von T-Systems wird nicht durchgeführt.

### 6.2.4 Sicherung von privaten Schlüsseln

T-Systems erstellt für Wiederherstellungs- und Notfallzwecke Sicherungskopien (Back-Up) des Schlüsselmaterials des CA-Zertifikates. Diese Schlüssel werden in verschlüsselter Form innerhalb von kryptografischen Hardware-Modulen (HSM) und zugehörigen Schlüsselspeichergeräten gespeichert.

### 6.2.5 Archivierung von privaten Schlüsseln

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

### 6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

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

### 6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

T-Systems speichert CA-Schlüssel in sicherer Form auf kryptografischen Hardware-Modulen (HSM).

### 6.2.8 Methode zur Aktivierung privater Schlüssels

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 des vorliegenden CP/CPS schützen.

#### 6.2.8.1 Schlüssel von Endteilnehmern

Der Endteilnehmer verpflichtet sich wirtschaftlich angemessene Maßnahmen zum physikalischen Schutz der verwendeten Hardware/Software zu ergreifen, um die Nutzung des Platzes/Komponente und seines zugehörigen privaten Schlüssels ohne Genehmigung des Endteilnehmers zu verhindern.

#### 6.2.8.2 Schlüssel von Administratoren

Der Administrator oder Operator hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer ähnlichen Sicherheitsmaßnahme, um den Administrator oder Operator vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann z. B. auch ein Kennwort zum Betrieb des privaten Schlüssels, ein Windows Anmelde- oder Bildschirmschonerkennwort, ein Anmeldekennwort für das Netzwerk beinhalten.
- Ergreifung geeigneter Maßnahmen zum physikalischen Schutz des Administrator- oder Operator-Arbeitsplatzes vor unberechtigtem Zugriff.

### 6.2.9 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.

### 6.2.10 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.

## 6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

### 6.3.1 Archivierung von öffentlichen Schlüsseln

Im Rahmen der regelmäßigen Backup Maßnahmen von T-Systems werden die Zertifikate gesichert und archiviert. Andere Vorgehensweisen werden einzelvertraglich festgelegt.

### 6.3.2 Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren

Das „T-TeleSec GlobalRoot Class 3“ Zertifikat hat eine Gültigkeit von 25 Jahren. CA-Zertifikate können mit der maximalen Gültigkeit der Root-CA ausgestellt werden (siehe hierzu Kapitel 7.1).
TLS/SSL EE Zertifikate haben eine maximale Laufzeit von 39 Monaten. Ab dem 01.03.2018 wird die Laufzeit von diesen Zertifikaten auf maximal 825 Tage begrenzt. und die Unterlagen zur Prüfung der Zertifikatsinformationen haben eine Gültigkeit von 825 Tagen.

## 6.4 Aktivierungsdaten

### 6.4.1 Generierung und Installation von Aktivierungsdaten

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

### 6.4.2 Schutz von 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 von 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 strengstens 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

T-Systems führt alle PKI-Funktionen mit Hilfe vertrauenswürdiger und geeigneter Systeme durch.

### 6.5.1 Spezifische technische Anforderungen an die Computersicherheit

T-Systems stellt sicher, dass die Verwaltung der CA-Systeme vor unbefugtem Zugriff Dritter gesichert ist.

T-Systems verwendet Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, 4-Augen-Prinzip), um die CA-Funktionalitäten, Verzeichnisdienste und OCSP-Responder 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.

### 6.5.2 Bewertung der Computersicherheit

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

## 6.6 Technische Kontrollen des Lebenszyklus

### 6.6.1 Systementwicklungskontrollen

Keine Bestimmungen.

### 6.6.2 Sicherheitsverwaltungskontrollen

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

### 6.6.3 Sicherheitskontrollen des Lebenszyklus

Keine Bestimmungen.

## 6.7 Netzwerk-Sicherheitskontrollen

Folgende Netzwerk-Sicherheitsmaßnahmen sind zu implementieren:

- Die Netzwerke der untergeordneten Zertifizierungsdienste sind durch aktuelle, dem Stand der Technik entsprechende Firewalls, vom Internet zu trennen. Der Datenverkehr ist auf das für die Funktionen notwendige Maß zu beschränken.
- Sicherheitskritische Komponenten und Systeme, die vom Internet aus erreichbar sind (z.B. Verzeichnisdienst, OCSP-Responder) sind durch Firewalls vom Internet und den internen Netzen zu trennen. Alle anderen sicherheitskritischen Komponenten und Systeme (z.B. CA, DB, Signer) müssen in einem separaten Netz betrieben werden.

## 6.8 Zeitstempel

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

# 7 Zertifikats-, Sperrlisten- und OCSP-Profile

## 7.1 Zertifikatsprofil

In der folgenden Tabelle wird das Zertifikatsprofil des Root Zertifikats „T-TeleSec GlobalRoot Class 3“ dargestellt:

| Zertifikatsfeld | Inhalt | | Bemerkungen |
|---|---|---|---|
| Version | v3 | | |
| SerialNumber | 01 | | Hexadezimal (Dezimal 1) |
| SignatureAlgorithmIdentifier | RSA, SHA-256 | | |
| Issuer | | | |
| Country Name | DE | | |
| Organization Name | T-Systems Enterprise Services GmbH | | |
| Organizational Unit Name 1 | T-Systems Trust Center | | |
| Common Name | T-TeleSec GlobalRoot Class 3 | | |
| Validity | | | |
| Not Before | Oct 1 10:29:56 2008 | | GMT |
| Not After | Oct 1 23:59:59 2033 | | GMT |
| Subject | | | |
| Country Name | DE | | |
| Organization Name | T-Systems Enterprise Services GmbH | | |
| Organizational Unit Name 1 | T-Systems Trust Center | | |
| Common Name | T-TeleSec GlobalRoot Class 3 | | |
| SubjectPublicKeyInfo | | | |
| Algorithm | <OID für RSA> | | |
| Subject Public Key | <Schlüssel> | | Schlüssellänge: 2048 Bit |
| Extensions | | | |
| Subject Key Identifier | non critical | B5:03:F7:76:3B:61:82:6A:12:AA:18:53:EB:03:21:94:BF:FE:CE:CA | |
| Basic Constraints | critical | CA:TRUE | |
| Key Usage | critical | Certificate Signing, CRL Signing, Off-line CRL Signing | |

**Tabelle 3: Zertifikatsprofil**

Die Seriennummer muss mit einem kryptographisch sicheren Zufallszahlengenerator (CSPRNG) erstellt werden. Sie muss größer als Null und durch 8 teilbar sein und mindestens 64 bit Entropie besitzen.

Die Zertifikatsprofile für CA- und Teilnehmerzertifikate werden im CPS einer Zertifizierungsstelle definiert.

### 7.1.1 Versionsnummer(n)

Siehe hierzu die Ausführungen im CPS der entsprechenden Zertifizierungsstelle.

### 7.1.2 Zertifikatserweiterungen

Um den Standard X.509v3 zu erfüllen, ergänzt T-Systems, je nach Anforderung der untergeordneten Zertifizierungsstellen (Sub-CA), das Zertifikatsprofil um entsprechende Erweiterungen. Diese sind in den CP/CPS der nachgelagerten Services beschrieben.

### 7.1.3 Objekt-Kennungen von Algorithmen

Folgende Signaturalgorithmen werden zur Zeit in CA- und EE-Zertifikaten verwendet:
- SHA256 RSA (OID 1.2.840.113549.1.1.11)
- SHA256 ECDSA (OID 1.2.840.10045.4.3.2)

Sub-CA, EE und OCSP Zertifikate dürfen nicht mit dem SHA-1 Hash-Algorithmus ausgestellt werden. Von einer SHA-1 Sub-CA dürfen keine SHA-2 EE Zertifikate ausgestellt werden.
Root-CA und Cross-CA Zertifikate, die mit dem SHA-1 Hash-Algorithmus ausgestellt wurden, dürfen weiterhin benutzt werden.

### 7.1.4 Namensformen

Die Endteilnehmer-Zertifikate der untergeordneten Zertifizierungsstellen (Sub-CA) müssen einen, für diesen Service, eindeutigen Ausstellernamen (Issuer DN) und einen eindeutigen Auftragstellernamen (Subject DN), gemäß den Ausführungen aus Kapitel 3.1.1 enthalten.

### 7.1.5 Namensbeschränkungen

Namensbeschränkungen können sich aus dem verwendeten Zeichensatz und/oder Feldlängen ergeben.

### 7.1.6 Objekt-Identifikatoren für Zertifizierungsrichtlinien

#### 7.1.6.1 Endteilnehmer Zertifikate

Öffentliche Geräte-Zertifikate, welche von einer Sub-CA unterhalb der Root-CA „T-TeleSec GlobalRoot Class 3“ ausgestellt werden, müssen eine Policy-OID enthalten, welche dediziert die Zusicherung repräsentiert, dass das öffentliche Geräte-Zertifikat und dessen Management während seines Lebenszyklus die Anforderungen der [CAB-BR] erfüllt. Diese Policy-OID muss im CP und/oder CPS der jeweiligen Sub-CA definiert und beschrieben sein.

Von der T-Systems betriebene Sub-CAs (affiliate) müssen die vom CA/Browser-Forum definierten Policy-OIDs 2.23.140.1.2.1 (DV) bzw. 2.23.140.1.2.2 (OV) verwenden. Auf besonderen Kundenwunsch kann eine zusätzliche OID verwendet werden.

Bei externen Kunden (non affiliate) muss mit diesen abgestimmt werden, welchen Policy-OID die externe Sub-CA für diesen Zweck verwendet.

#### 7.1.6.2 Sub-CA-Zertifikate

Dieses Kapitel bezieht sich ausschließlich auf Sub-CA-Zertifikate, welche nach dem 01.07.2012 unter der Root-CA „T-TeleSec GlobalRoot Class 3“ ausgestellt wurden:

Externe Sub-CA-Zertifikate enthalten eine Policy-OID, die dediziert die Zusicherung repräsentiert, dass die Sub-CA während ihres Lebenszyklus die Anforderungen der [CAB-BR] erfüllt.

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

In interne Sub-CA-Zertifikaten (affiliate) werden die vom CA/Browser-Forum definierten OIDs 2.23.140.1.2.1 (DV) bzw. 2.23.140.1.2.2 (OV) verwendet um die Konformität zu den [CAB-BR] zuzusichern. Auf besonderen Kundenwunsch kann außerdem eine zusätzliche OID verwendet werden.

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

Die Regelungen dieses Kapitels gelten für alle Hierarchie-Ebenen hierachisch unterhalb der Root-CA „T-TeleSec GlobalRoot Class 3“, d.h. auch für die Verkettung von Sub-CA-Zertifikaten.

### 7.1.7 Objekt-Identifikatoren für Zertifizierungsrichtlinien der Baseline Requirements

Für die durch das CA/Browser-Forum in den [CAB-BR] definierten Policy-OIDs gelten die folgenden Anforderungen, welche von allen Sub-CAs hierarchisch unterhalb der Root-CA „T-TeleSec GlobalRoot Class 3“ einzuhalten ist.

1. Policy-OID 2.23.140.1.2.1
   Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.1 (DV) verwendet, dürfen folgende Felder des Subject DN nicht ausgefüllt sein:
   - organizationName
   - streetAddress
   - localityName
   - stateOrProvinceName
   - postalCode

2. Policy-OID 2.23.140.1.2.2
   Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.2 (OV) verwendet, müssen zwingend folgende Felder des Subject DN ausgefüllt sein:
   - organizationName
   - localityName
   - stateOrProvinceName (falls ein sinnvoller Wert existiert, z.B. Bundesland in der BRD)
   - countryName

## 7.2 Sperrlistenprofile

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)

Authority Revocation List (ARL) T-TeleSec GlobalRoot Class 3

| | | |
|---|---|---|
| Version | | 2 (0x1) |
| Signature Algorithm | | sha1WithRSAEncryption |
| Issuer | | C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 3 |
| Last Update | | Last Update GMT |
| Next Update | | Last Update + 6 Monate |
| | | |
| CRL extensions | | |
| | X509v3 Authority Key Identifier | B5:03:F7:76:3B:61:82:6A:12:AA:18:53:EB:03:21:94:BF:FE:CE:CA |
| | X509v3 CRL Number | Serialnumber of CRL |
| | | |
| Revoked Certificates | | |
| | Serial Number | Serial number of certificate |
| | Revocation Date | Revocation date of certificate |
| CRL entry extensions | | |
| | X509v3 CRL Reason Code | Reason of revocation |
| | | |

**Tabelle 4: Sperrlistenprofile**

### 7.2.1 Versionsnummer(n)

Siehe hierzu die Ausführungen in der CPS der entsprechenden Zertifizierungsstelle.

### 7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Siehe hierzu die Ausführungen in der CPS der entsprechenden Zertifizierungsstelle.

## 7.3 OCSP-Profil

### 7.3.1 Versionsnummer(n)

Siehe hierzu die Ausführungen in der CPS der entsprechenden Zertifizierungsstelle.

### 7.3.2 OCSP-Erweiterungen

T-Systems bietet keine OCSP-Erweiterungen an.

# 8 Compliance-Audits und andere Prüfungen

Für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile wird eine jährliche ETSI Überprüfung für Zertifizierungsstellen (z.B. ETSI TS 102 042 oder eine äquivalente Überprüfung) durchgeführt. T-Systems behält sich das Recht vor, bei Betreibern von Zertifizierungsstellen Überprüfungen oder Untersuchungen durch zu führen. Die Häufigkeit dieser Überprüfungen wird einzelvertraglich festgelegt. Besondere sicherheitskritische Ereignisse können außerplanmäßig eine Überprüfung erforderlich machen. Bei CA-Verkettung mit CAs von externen Kunden gelten die Regelungen aus [TSYSROOTSIGN].

## 8.1 Intervall von Prüfungen

Entsprechend den Anforderungen findet mindestens einmal jährlich eine Überprüfung statt. Besondere Ereignisse oder zusätzliche Anforderungen können weitere Prüfungen erforderlich machen.

Für EV-Zertifikate werden regelmäßige Selbst-Überprüfungen im Abstand von 3 Monaten durchgeführt. Hierbei wird mindestens eine 3% große Stichprobe aller EV-Zertifikate herangezogen.

## 8.2 Identität/Qualifikation des Prüfers

Für die Feststellung der ETSI Konformität wird eine anerkannte, renommierte Wirtschaftsprüfergesellschaft beauftragt.

## 8.3 Beziehung des Prüfers zur prüfenden Stelle

Für die Feststellung der ETSI Konformität wird eine anerkannte, renommierte und unabhängige Wirtschaftsprüfergesellschaft beauftragt.

## 8.4 Abgedeckte Bereiche der Prüfung

Den Umfang der Prüfung legt der Prüfer selbst fest. Zielsetzung der Überprüfung ist die Umsetzung dieses Dokuments. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Identitätsprüfungen der Endteilnehmer,
- Zertifikatsbeauftragungsverfahren,
- Zertifikatsauftragstellungsverfahren,
- Bearbeitung von Zertifikatsaufträgen,
- Zertifikatssperrungen,
- Zutrittsschutz,
- Berechtigungs- und Rollenkonzept ,
- Einbruchshemmende Maßnahmen,
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen dieser Audit-Kriterien geprüft:

- Root-CAs und Sub-CAs, die Server-Zertifikate ausstellen, müssen nach den folgenden Kriterien überprüft werden:
  ETSI TS 102 042 - DVCP, OVCP, PTC-BR
  oder
  ETSI EN 319 411-1 - DVCP, OVCP, PTC-BR
- Root-CAs und Sub-CAs, die SMIME-Zertifikate ausstellen, müssen nach den folgenden Kriterien überprüft werden:
  ETSI TS 101 456 und ETSI TS 102 042 - LCP, NCP, NCP+
  oder
  ETSI EN 319 411-1 und ETSI EN 319 411-2 - LCP, NCP, NCP+
-
- Baseline Requirements

### 8.4.1 Risikobewertung und Sicherheitsplan

Das T-Systems Trust Center führt jährlich eine Risikobewertung durch. Die Überprüfung beinhaltet mindestens die folgenden Punkte:

- Identifikation vorhersehbarer externer, als auch interner Gefährdungen (d.h. insbesondere die zu Grunde liegenden Schwachstellen), welche
  - zu unbefugten Zugriffen auf relevante Daten oder Systeme,
  - zur Weitergabe oder einem Missbrauch von relevanten Daten,
  - zu Veränderungen oder Zerstörung von relevanten Daten,
  - zur Beeinträchtigung, Störung oder Ausfall von Teilen oder des gesamten Zertifikatsverwaltungsprozesses führen können.
- 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.
- 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 Management der während der Risikobewertung identifizierten Risiken zu unterstützen. Der Sicherheitsplan enthält entsprechend der Sensibilität der Daten und des Zertifikatsverwaltungsprozesses administrative, organisatorische, technische und physische Sicherheitsmaßnahmen.

## 8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Werden bei einem Compliance-Audit von einem Prüfer schwerwiegende Mängel oder Fehler bei dem Betreiber der Zertifizierungsstelle festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durch zu führen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten 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, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der T-Systems.

Die relevanten Auditberichte werden auf der Website des T-Systems Trust Centers unter https://www.telesec.de/de/trust-center veröffentlicht.

# 9 Sonstige geschäftliche und rechtliche Angelegenheiten

## 9.1 Entgelte

### 9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

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

### 9.1.2 Entgelte für den Zugriff auf Zertifikate

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

### 9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

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

### 9.1.4 Entgelte für andere Leistungen

T-Systems berechnet keine Entgelte für den Abruf dieses Dokuments und der damit verbundenen einfachen Betrachtung.
Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1, 9.5), die das Urheberrecht des Dokuments besitzt.
Die Nutzung dieses Dokuments ist ebenfalls entgeltfrei, wenn Sie als mitgeltende Vertragsunterlage für die Vertragsbeziehung zwischen Kunden und T-Systems dient.

### 9.1.5 Erstattung von Entgelten

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

## 9.2 Finanzielle Verantwortlichkeiten

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

### 9.2.1 Versicherungsschutz

Der Versicherungsschutz ist in den Allgemeinen Geschäftsbedingungen (AGB) beschrieben.

### 9.2.2 Sonstige finanzielle Mittel

Nicht anwendbar.

### 9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

## 9.3 Vertraulichkeit von Geschäftsinformationen

### 9.3.1 Umfang von vertraulichen Informationen

Unter vertraulichen Informationen werden alle Informationen von PKI-Beteiligten (siehe Kapitel 1.3) eingestuft, die nicht unter Kapitel 9.3.2 fallen.

### 9.3.2 Umfang von nicht vertraulichen Informationen

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

### 9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortlichkeit für den Schutz der vertraulichen Informationen sowie über die Einhaltung der datenschutzrechtlichen Bestimmungen liegt bei T-Systems als PKI-Diensteanbieter. Die Registrierungsstelle Dritter hat die einschlägigen gesetzlichen Bestimmungen sowie ggf. weiteren Regelungen zum Datenschutz zu beachten.

## 9.4 Schutz von personenbezogenen Daten (Datenschutz)

### 9.4.1 Datenschutzkonzept

Personenbezogene Daten von Zertifikatsnehmern werden in einem Umfang erhoben und verifiziert, wie es zur Ausstellung der Teilnehmerzertifikate und zur Sicherstellung des Vertrauens in diese Zertifikate notwendig ist. T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 BDSG sicher.

### 9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.1.

### 9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.2.

### 9.4.4 Verantwortung für den Schutz vertraulicher Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.3.

### 9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

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

### 9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

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

### 9.4.7 Andere Umstände zur Offenlegung von Daten

Keine Bestimmungen.

## 9.5 Rechte des geistigen Eigentums (Urheberrecht)

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von T-Systems unzulässig. Die geistigen Eigentumsrechte an den Zertifikaten und der ARL verbleiben bei T-Systems. Die Nutzungsrechte an den Zertifikaten werden durch Einzelverträge ausgestaltet.

## 9.6 Zusicherungen und Gewährleistungen

T-Systems verpflichtet sich,

- keine Angaben im Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsauftrag 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 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 und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) allen wesentlichen Anforderungen der geltenden CP/CPS erfüllen.

### 9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle (CA)

Zusätzliche Vereinbarungen sind in den CP/CPS der nachgelagerten Services zu beschreiben.

### 9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Zusätzliche Vereinbarungen sind in den CP/CPS der nachgelagerten Services zu beschreiben.

### 9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Zusätzliche Vereinbarungen sind in den CP/CPS der nachgelagerten Services zu beschreiben.

### 9.6.4 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

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

### 9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Keine Bestimmungen.

## 9.7 Haftungsausschluss

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

## 9.8 Haftungsbeschränkungen

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

## 9.9 Schadensersatz

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

## 9.10 Laufzeit und Beendigung

### 9.10.1 Laufzeit

Die CP/CPS tritt mit der Veröffentlichung auf den T-Systems Webseiten in Kraft.

Änderungen treten ebenfalls mit der Veröffentlichung auf den öffentlichen Webseiten (siehe Kapitel 2.3) in Kraft.

### 9.10.2 Beendigung

Diese CP/CPS bleibt in der jeweils gültigen Version in Kraft, bis sie durch eine neue Version ersetzt wird.

### 9.10.3 Wirkung der Beendigung und Fortbestand

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

## 9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

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

## 9.12 Änderungen der CP/CPS

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

### 9.12.1 Verfahren für Änderungen

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

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

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

### 9.12.2 Benachrichtigungsverfahren und -zeitraum

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

## 9.13 Bestimmungen zur Beilegung von Streitigkeiten

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

## 9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland.

## 9.15 Einhaltung geltenden Rechts

Das vorliegende Dokument unterliegt den geltenden deutschen Gesetzen, Vorschriften, Richtlinien, Verordnungen, Erlassen und Anordnungen, insbesondere den darin beschriebenen Import und Export Bestimmungen

von Security-Komponenten (Software, Hardware oder technischer Informationen). Geltende zwingende Gesetze, Vorschriften, Richtlinien, Verordnungen, Erlasse und Anordnungen setzen die entsprechenden Bestimmungen des vorliegenden Dokuments außer Kraft.

## 9.16 Verschiedene Bestimmungen

### 9.16.1 Vollständiger Vertrag

Nicht anwendbar.

### 9.16.2 Abtretung

Nicht anwendbar.

### 9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieses 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.

### 9.16.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Nicht anwendbar.

### 9.16.5 Höhere Gewalt

Mit dieser Regelung soll sichergestellt werden, dass der Vertragspartner mit seinen Endteilnehmern vereinbart, dass er nicht in Verzug gerät, wenn sich die Leistung infolge höherer Gewalt verzögert oder unmöglich wird.

## 9.17 Sonstige Bestimmungen

Nicht anwendbar.

# 10 Glossar

| | |
|---|---|
| AICPA | American Institute of Certified Public Accountants |
| ARL | Siehe Authority Revocation List. |
| Authority Revocation List | Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf. |
| CA | Certification Authority. Siehe Zertifizierungsstelle. |
| CAA | Certification Authority Authorization DNS Resource Record |
| Certificate Policy | Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest. |
| Certificate Revocation List | Siehe Sperrliste. |
| Certification Authority | Siehe Zertifizierungsstelle. |
| Certification Practice Statement | 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. |
| CP | Siehe Certificate Policy. |
| CPS | Siehe Certification Practice Statement. |
| CRL | Certificate Revocation List. Siehe Sperrliste. |
| CV Zertifikat | card verifiable Zertifikat: Zertifikat in einem Tag/Value Format (kein X.509 Format) |
| Digitale Signatur | Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten. |
| Digitales Zertifikat | Datensatz, der den Namen einer Person oder eines Systems, deren öffentlichen Schlüssel, gegebenenfalls einige andere Angaben und eine Signatur einer Zertifizierungsinstanz enthält. |
| Distinguished Name | Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein. |
| DN | Siehe Distinguished Name. |
| DMZ | Demilitarisierte Zone: dabei handelt es sich um einen geschützten Rechnerverbund, der sich zwischen 2 Netzwerken befindet. Der Rechnerverbund wird jeweils durch einen Paketfilter gegen das dahinterstehende Netz abgeschirmt. |
| Dual Key | Variante, bei der für Verschlüsselung und Signatur getrennte Schlüsselpaare verwendet werden, das heißt, ein Benutzer besitzt zwei entsprechende Zertifikate. |
| Elektronische Signatur | Siehe digitale Signatur. |
| Endteilnehmer-Zertifikat | Ein Zertifikat, welches nicht die Basiseinschränkung (basis constraints) „Zertifizierungstelle“ verwendet, daher selber keine Zertifikate signieren kann. |
| Geräte-Zertifikat | X.509 V3 Zertifikat, welches im commonName-Feld (CN) des distinguishedName des Zertifikatsnehmers (Subject) und/oder in mindestens einer subjectAltName-Erweiterung entweder |

| | |
|---|---|
| | einen Hostname oder eine IP-Adresse enthält. |
| Hardware Security Modul | Hardwarebox zur sicheren Erzeugung und Speicherung privater Schlüssel. |
| Hash-Wert | In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert. |
| HSM | Siehe Hardware Security Modul. |
| ISIS-MTT | Gemeinsame Spezifikation von TeleTrust und T7 Gruppe für elektronische Signaturen, Verschlüsselung und Public Key Infrastrukturen |
| Key Recovery | Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert. |
| Kompromittierung | Ein geheimer 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). |
| Latenzzeit | Zeit zwischen Generierung und Veröffentlichung, zum Beispiel einer Sperrliste |
| LDAP | Siehe Lightweight Directory Access Protocol. |
| LDAP-Server | Server, der Informationen speichert, die über LDAP abrufbar sind. |
| Lightweight Directory Access Protocol | 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-Request | Variante eines Zertifikatsauftrags, bei dem die Daten per E-Mail an die Zertifizierungsinstanz übermittelt werden. |
| MitM | Man-in-the-Middle |
| Öffentliches Geräte-Zertifikat | Ein Geräte-Zertifikat, welches in der CA-Hierarchie von einer Sub-CA unterhalb eines öffentlichen Root-Zertifikates ausgestellt ist. |
| OCSP | Das Online Certificate Status Protocol ermöglicht die Online-Abfrage der Gültigkeit von Zertifikaten. |
| PIN | Personal Identification Number. Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird. |
| PKI | Siehe Public-Key-Infrastruktur. |
| PKIX | Public Key Infrastructure X.509. Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert. |
| PKS | Public Key Service. Service des T-Systems Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate. |
| Policy | Richtlinien, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden. |

| | |
|---|---|
| PSE | Personal Security Environment. 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 | Gesamtheit der Komponenten, Prozesse und Konzepte, die zur Verwendung von Public-Key-Verfahren verwendet werden. Typischerweise besteht eine Public-Key-Infrastruktur aus zentralen Komponenten wie einer Zertifizierungsinstanz und einem Verzeichnisdienst und verschiedenen Client-Komponenten. |
| RA | Registration Authority. Siehe Registrierungsstelle. |
| Registration Authority | Siehe Registrierungsstelle. |
| Registrierungsstelle | Komponente, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten. |
| Root CA | Siehe Wurzelzertifizierungsstelle. |
| RSA | Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist. |
| 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. |
| SCEP | Simple Certificate Enrollment Protocol. Protokoll zur Beauftragung und zum Laden von Zertifikaten in IPSec Devices. |
| 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. |
| Schlüssel | Ein Schlüssel bezeichnet in der Kryptografie eine geheime Information (geheimer Schlüssel) oder ein öffentliches Gegenstück dazu (öffentlicher Schlüssel). Es gibt Verfahren, bei denen jeweils mit dem gleichen geheimen Schlüssel ver- und entschlüsselt wird sowie Verfahren bei denen ein öffentlicher Schlüssel zum Ver- und ein geheimer zum Entschlüsseln verwendet wird. |
| Secure Socket Layer | Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet. Kann in vielen Fällen statt dem komplexeren IPSec verwendet werden. |
| SigG | Signaturgesetz |
| SigV | Signaturverordnung |
| Signatur | Siehe digitale Signatur. |
| Single Key | Variante, bei der für Verschlüsselung und Signatur das selbe Schlüsselpaar verwendet wird, das heißt, ein Benutzer besitzt ein Zertifikat. |
| Smart Card | Chipkarte mit Rechenfunktionalität, die für kryptografische Zwecke verwendet werden kann. |
| 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 | Durch Verschlüsselung geschützte Datei zur Speicherung des privaten Schlüssels eines Benutzers. |
| Sperrinstanz | Komponente, die Zertifikatssperrungen durchführt. |
| Sperrliste | Liste, in der gesperrte digitale Zertifikate aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats sollte anhand einer Sperrliste überprüft werden, ob dieses noch verwendet werden darf. Wird auch als Certificate Revocation List (CRL) bezeichnet. |

| | |
|---|---|
| SSL | Siehe Secure Socket Layer. |
| Verzeichnisdienst | Datenspeicher, der den Abruf von Zertifikaten und Informationen über Zertifikate (insbesondere Sperrlisten) ermöglicht. |
| Web-Request | Variante eines Zertifikatsauftrags, bei dem die Daten über ein Web-Formular an die Zertifizierungsinstanz übermittelt werden. |
| Wildcard-Zertifikat | Ein Zertifikat, das ein Sternchen (*) in der äußersten linken Position eines in dem Zertifikat enthaltenen voll qualifizierten Domain-Namens (Fully-Qualified Domain Names) des Subjekts aufweist. |
| Wurzelzertifizierungsstelle | Oberste Zertifizierungsinstanz einer CA-Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsinstanz ausgestellt wurde, sondern selbstsigniert ist. |
| 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. |
| Zertifikat | Siehe digitales Zertifikat. |
| Zertifizierungsstelle | Komponente, die digitale Zertifikate ausstellt, indem sie einen Datensatz bestehend aus öffentlichem Schlüssel, Name und verschiedenen anderen Daten digital signiert. Ebenso werden von der Zertifizierungsstelle Sperrinformationen herausgegeben. |
| Zertifikatsnehmer | Instanz, die ein Zertifikat und den dazu gehörenden privaten Schlüssel verwendet. |
| Zuständigkeitsbereich | Teilbereich in der CA Administrationshierarchie, der von einem RA Operator verwaltet wird. |

# 11 Referenzen


| | |
|---|---|
| BDSG] | Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66. |
| [CAB-BR] | Zum jeweiligen Zeitpunkt gültige Version des vom CA/Browser-Forum unter http://www.cabforum.org/documents.html veröffentlichten Dokuments „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ |
| [EU-RL] | Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 1999/93/EG, EU, 1999 |
| [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 |
| [SigG] | Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften, Bundesgesetzblatt I 2001, S. 876 |
| [SigV] | Signaturgesetzverordnung, „Verordnung zur elektronischen Signatur“, BGBl. I S. 3074, 21.November 2001 |
| [TSYSROOTSIGN] | Leistungsbeschreibung T-Systems Root Signing |
| [X.509] | Information technology - Open Systems Interconnection - The Directory:authentication framework, Version 3, ITU, 1997 |