Trust Center Services
TeleSec Shared-Business-CA

T-Systems International GmbH, PSS - Professional Services & Solutions

Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)

Version 1.0
Stand 06.04.2010
Status Final

öffentlich

Impressum

Herausgeber

T-Systems International GmbH
ICT Operation, PSS – Professional Services & Solutions
Trust Center Services
Untere Industriestraße 20
57250 Netphen
Deutschland

Dateiname	Dokumentennummer	Dokumentenbezeichnung
Shared-Business-CA_CPS_1.0.doc		Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)

Version	Stand	Status
1.0	06.04.2010	Final

Kurzinfo

Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement) der Dienstleistung TeleSec Shared-Business-CA

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	28.04.2008	Matthias Ulm	Initialversion Entwurf
0.2	16.05.2008	Uwe Völkel	1. Überarbeitung des Entwurfs
0.3	01.08.2008	Matthias Ulm, Uwe Völkel	2. Überarbeitung des Entwurfs
0.31	02.12.2008	Uwe Völkel	3. Überarbeitung des Entwurfs
0.32	26.01.2009	Lothar Eickholt, Axel Treßel, Uwe Völkel	4. Überarbeitung des Entwurfs
0.4	25.03.2009	Uwe Völkel	5. Überarbeitung des Entwurfs
0.5	28.07.2009	Claudia Riffer	Juristische Überarbeitung des Entwurfs
0.6	29.07.2009	Uwe Völkel	6. Überarbeitung
0.61	21.08.2009	Uwe Völkel	6. Überarbeitung
0.7	06.10.2009	Uwe Völkel, Lothar Eickholt	7. Überarbeitung
0.8	18.01.2010	Uwe Völkel	8. Überarbeitung
0.81	01.03.2010	Uwe Völkel	8.1 Überarbeitung
0.82	06.04.2010	Uwe Völkel	8.2 Überarbeitung
1.0	06.04.2010	Uwe Völkel	Finale Abstimmung

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Trust Center wird durch die Konzerneinheit T-Systems International GmbH (im Folgenden „T-Systems“ genannt) betrieben.
Im Jahr 1998 nahm das Trust Center (unter der Bezeichnung „Trust Center der Deutschen Telekom“) den Betrieb als erster Zertifizierungsdiensteanbieter auf, das über eine Akkreditierung nach dem deutschen Signaturgesetz (SigG) verfügt.
Zusätzlich zu den genau festgelegten und zertifizierten Arbeitsabläufen zeichnet sich das Trust Center der T-Systems durch einen sehr hohen Sicherheitsstandard aus. Die Vertrauenswürdigkeit des eingesetzten Trust-Center-Personals ist durch öffentliche Stellen überprüft worden. Alle Dienste sind Gegenstand regelmäßiger Qualitätskontrollen. Die eingesetzte Technologie ist Stand der Technik und wird laufend durch ausgebildete Administratoren überwacht.
Das Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Wurzel-Instanzen (Roots), sowohl für die Ausgabe qualifizierter als auch fortgeschrittener Zertifikate. Die Zertifizierungsstellen der Zertifikats-Dienstleistungen unterscheiden sich hinsichtlich der Anwendungskontexte für Zertifikate, der konkreten Ausprägung der technischen Schnittstellen, Registrierungsverfahren, der Zertifikatsprofile, der Prozesse bei Sperrungen, sowie der Veröffentlichung von Informationen.
Sowohl die bauliche als auch die organisatorische Infrastruktur erfüllt die strengen Anforderungen des deutschen Signaturgesetzes. Zu den vom T-Systems Trust Center angebotenen Leistungen gehört unter anderem der TeleSec Public Key Service (PKS), der die Ausstellung qualifizierter Zertifikate gemäß dem deutschen Signaturgesetz (SigG) umfasst. Zusätzlich finden sich im Portfolio weitere Dienstleistungen zu unterschiedlichsten PKI-Lösungen, die nach den Vorgaben des Signaturgesetzes „fortgeschrittener Signaturen“ entsprechen; ferner Einmalpasswortverfahren und qualifizierte Zeitstempel.

1.1 Überblick

TeleSec Shared-Business-CA (im Folgenden „SB-CA“ genannt) ist eine zentral, im Trust Center der T-Systems, betriebene Dienstleistung zur Generierung und Verwaltung von unterschiedlichen Zertifikatstypen, die insbesondere Einsatz finden bei E-Mail-Security, starker Authentifizierung (Client-Server), Remote-VPN, Servern und aktiven Netzkomponenten (z.B. Router, Gateways).
Die Zertifizierungsinstanz SB-CA ist hierarchisch unterhalb der Wurzelinstanz „Deutsche Telekom Root CA 2“ installiert, d.h. das Zertifizierungsstellen-Zertifikat von Shared-Business-CA wurde von der Deutsche Telekom Root CA 2 ausgestellt. Für die Wurzelinstanz „Deutsche Telekom Root CA 2“ besteht eine eigene Zertifikatsrichtlinie (engl. Certificate Policy, CP) als auch Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS).

Die Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) des Dienstes Shared-Business-CA (SB-CA) der T-Systems beinhaltet Sicherheitsvorgaben sowie Richtlinien hinsichtlich technischer, organisatorischer und rechtlicher Aspekte und beschreibt die Tätigkeiten des Trust Center Betreibers in der Funktion als Certification Authority (CA) und Registration Authority (RA).
Im Einzelnen behandelt diese CPS die folgenden Regelungen:

- 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.

Das vorliegende Dokument orientiert sich an den dem internationalen Standard RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ [RFC3647] der Internet Society.

Leistungsumfang und Funktionalitäten der Shared-Business-CA ist im Dokument „Leistungsbeschreibung Shared-Business-CA“ dokumentiert, auf die an dieser Stelle verwiesen wird.

Rechtliche und kommerzielle Aspekte der Shared-Business-CA ist im Dokument „Allgemeine Geschäftsbedingungen Shared-Business-CA“ dokumentiert, auf die an dieser Stelle verwiesen wird.

1.2 Name und Kennung des Dokuments

Das vorliegende Dokument stellt die Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) des Dienstes Shared-Business-CA (SB-CA) der T-Systems dar. Die Verwendung von Objekt-Kennungen (Object Identifier, OID) für Zertifizierungsrichtlinien ist in Kapitel 7.1.6 beschrieben.

1.3 PKI-Beteiligte

1.3.1 Zertifizierungsstellen

Im Folgenden wird explizit auf die PKI-Beteiligten des Dienstes TeleSec Shared-Business-CA eingegangen.

1.3.1.1 Zertifizierungsstelle „Shared-Business-CA“

Mit TeleSec Shared-Business-CA (SBCA) bietet T-Systems dem Kunden eine vollständige PKI-Lösung an, dessen Infrastruktur im hochsicheren T-Systems Trust Center installiert ist und von qualifiziertem Personal betrieben wird. Zur sichern Abgrenzungen erhält jeder Kunde, im Folgenden „Domänen-Betreiber“ genannt, eine eigens für ihn eingerichtete Master-Domäne (auch Betreiber-Domäne genannt), innerhalb der er selbst Zertifikate für Endteilnehmer (z.B. Personen, Infrastrukturkomponenten) beantragen und verwalten kann. Die SB-CA ist als mandantenfähige shared-PKI-Lösung konzipiert. Alle Kunden (Domänen-Betreiber) erhalten einen dedizierten Zugang, über dem sie selbst, nach erfolgreicher zertifikatsbasierender SSL/TLS-Client-Authentifizierung, innerhalb der eigenen Master-Domäne die PKI-Funktionen nutzen können. Alle sicherheitsrelevanten Aktionen erfolgen über eine verschlüsselte Verbindung.

1.3.1.2 Web-Server der „Shared Business CA“

Der Zugriff des Domänen-Betreibers auf die PKI-Funktionen der SB-CA erfolgt über die Kommunikationsplattform Internet nach erfolgreicher Authentifizierung an der rollenspezifischen Webseite.
Benutzersensible Aktionen erfolgen über das sichere Protokoll HTTPS. Zur Initiierung einer SSL/TLS-Verbindung bedarf es, dass der Web-Server mit einem SSL-Zertifikat ausgestattet ist.
Die Zertifikate der Web-Server unterstehen hierarchisch der „GlobalSign-Root CA“ und der Sub-CA-Instanzen „GlobalSign RootSign Partners CA“ und „Deutsche Telekom CA 5“.

1.3.1.3 Übersicht der Zertifikatsinstanzen

Die für den Dienst SB-CA involvierten Zertifikatsinstanzen sind in Abbildung 1 dargestellt.

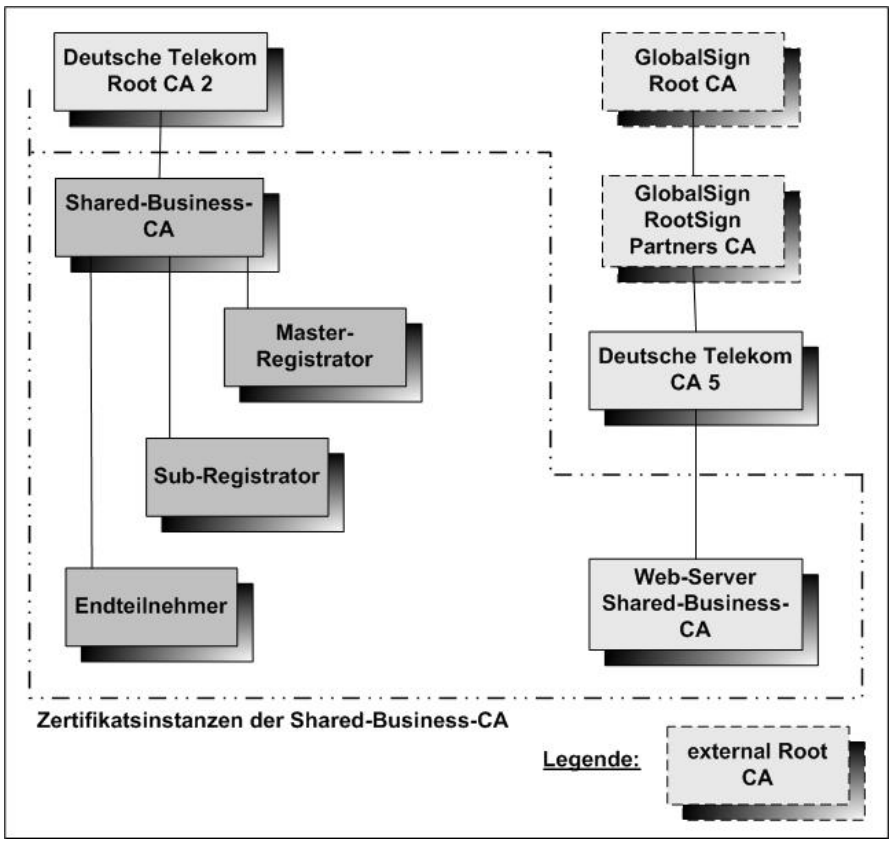

Abbildung 1: Übersicht aller involvierten Zertifikatsinstanzen für SB-CA

1.3.2 Registrierungsstellen

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

Innerhalb der SB-CA sind folgende Registrierungsstellen etabliert:

- Trust Center T-Systems, und
- Registrierungsstelle(n) des Domänen-Betreibers.

1.3.2.1 Registrierungsstelle „Trust Center der T-Systems“

Die Registrierungsstelle der T-Systems, repräsentiert durch den Trust-Center-Operator, ist im Trust Center lokalisiert und nimmt Funktionen einer übergeordneten Registrierungsstelle wahr. Weitere übergeordnete Registrierungsstellen sind nicht etabliert.
Diese Registrierungsstelle hat insbesondere folgende Aufgaben:

- Entgegennahme von Aufträgen und Prüfung der Identifikationsunterlagen zur Einrichtung (Konfiguration) der/von Master-Domäne(n) bzw. Betreiber-Domäne(n),
- Einrichtung der Master-Domäne(n) und Ausstellung von Master-Registrator-Zertifikaten auf Smartcard,
- Konfigurationsänderungen der Master-Domäne(n) nach erfolgreicher Prüfung der Identifikationsunterlagen,
- Ausstellung von weiteren Master-Registrator-Zertifikaten auf Smartcard,
- Sperrung von Master-Registrator-Zertifikaten.

Die Registrierungsstelle der T-Systems darf auch Master-Domänen-übergreifend Master-Registrator-, Sub-Registrator- und Endteilnehmer-Zertifikate sperren, sofern der Domänen-Betreiber dies beauftragt hat oder missbräuchliche Verwendung zu vermuten bzw. nachgewiesen ist.

Optional kann ein eigener Sperrservice beim Domänen-Betreiber eingerichtet werden. Nach Beauftragung durch den Domänen-Betreiber weist der Trust-Center-Administrator einem in der entsprechenden Master-Domäne ausgestellten Zertifikat die Rolle des Sperrservice-Operators zu.

Ebenfalls steht optional eine Schlüsselsicherung von Soft-PSE (zentrales key back-up) zu Verfügung. Dabei wird das Schlüsselmaterial als auch die korrespondierende Passwortdatei im Trust Center der T-Systems hinterlegt und kann per 4-Augen-Prinzip heruntergeladen werden.

Damit übernimmt diese Registrierungsstelle übergeordnete Funktionen und zeigt sich für die Zulassung und den Widerruf untergeordneter Registrierungsstellen verantwortlich, die lokalisiert sind bei den Domänen-Betreibern und dem Service Desk.

1.3.2.2 Registrierungsstellen „Domänen-Betreiber“

Die Registrierungsstellen des Domänen-Betreibers sind der übergeordneten Registrierungsstelle der T-Systems (Kapitel 1.3.2.1) unterstellt und agieren als untergeordnete Instanzen zu den PKI-Endteilnehmern. Jeder nachgeordneten Registrierungsstelle ist genau eine einzige übergeordnete Registrierungsstelle zugeordnet.

Die nachgeordnete Registrierungsstelle hat insbesondere folgende Aufgaben:

- Entgegennahme von Zertifikatsanträge innerhalb des definierten Verantwortungsbereiches,
- Prüfung der Anträge nach den vorgegebenen Richtlinien (z.B. Arbeitsanweisung),
- Beantragung des/der Zertifikat(e) in Folge der Freigabe eines Zertifikatsantrags, oder
- Freigabe dieser Zertifikatsanträge nach erfolgreicher Prüfung, ansonsten Ablehnung oder Zurückstellung (Widervorlage) des Antrags,
- Entgegennahme des/der von der SB-CA erzeugten Zertifikat(e) und Übergabe an den Zertifikatsinhaber bzw. eine autorisierte Person,
- Entgegennahme und Prüfung von Zertifikatssperrungsaufträgen innerhalb des definierten Verantwortungsbereiches oder ggf. Weiterleitung dieser an die übergeordneten Registrierungsstelle oder Service Desk,
- Durchführung einer Zertifikatssperrung als Folge einer positiven Prüfung eines Sperrauftrags, und
- Generierung einer neuen und damit aktuellen Zertifikatssperrliste (CRL).

Der Prozess „zentrale Schlüsselsicherung“ steht dem Domänen-Betreiber optional zur Verfügung.

Die operativen Tätigkeiten der nachgeordneten Registrierungsstellen werden durch die Master- und Sub-Registratoren wahrgenommen, die beim Domänen-Betreiber lokalisiert sind.

1.3.2.2.1 Master-Registrator

Der Master-Registrator stellt die oberste Registrierungsstelle des Domänen-Betreibers dar. Die Verwaltungsfunktionen stehen über der Master-Registrator-Webseite zur Verfügung. Das Master-Registrator-Zertifikat wurde von T-Systems auf Smartcard ausgestellt (siehe Kapitel 1.3.2.1).

Der Master-Registrator hat insbesondere folgende Aufgaben:

- Einrichtung, Konfiguration und Verwaltung von Zuständigkeitsbereichen (Sub-Domänen),
- Ausstellung von Sub-Registrator-Zertifikaten auf Personen, die der Domänen-Betreiber bestimmt,
- Sperrung von Sub-Registrator-Zertifikaten nach Vorliegen eines Sperrgrundes,
- Sperrung von Endteilnehmer-Zertifikaten nach Vorliegen eines Sperrgrundes.

Der Verwendungszweck des Master-Registrator-Zertifikats besteht ausschließlich in der zertifikatsbasierenden SSL/TLS-Client-Authentifizierung an der Master-Registrator-Webseite zur Aufgabenerledigung des Master-Registrators. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

Diese Registrierungsstelle liegt in der vollständigen Verantwortung des Domänen-Betreibers. T-Systems nimmt auch selbst als eigener Domänen-Betreiber die Aufgaben dieser Registrierungsstelle wahr.

Weitere Funktionen sind im Dokument „Leistungsbeschreibung Shared-Business-CA“ beschrieben.

1.3.2.2.2 Sub-Registrator

Der Sub-Registrator stellt die unterste Registrierungsstelle beim Domänen-Betreiber dar. Die Funktionen stehen nach erfolgreicher zertifikatsbasierender SSL/TLS-Client-Authentifizierung an der Sub-Registrator-Webseite zur Verfügung. Das Sub-Registrator-Zertifikat wurde vom Master-Registrator selbst auf Smartcard oder als Soft-PSE ausgestellt (siehe Kapitel 1.3.2.2).

Der Sub-Registrator hat insbesondere folgende Aufgaben:

- Ausstellung von Endteilnehmer-Zertifikaten nach erfolgreicher Identitätsprüfung (siehe auch Zentrale Registrierung, Kapitel 3.2.3),
- Genehmigung, Ablehnung oder Wiedervorlage von Zertifikatsanträgen nach erfolgreicher Identitätsprüfung (siehe auch Dezentrale Registrierung, Kapitel 3.2.3),
- Sperrung von Endteilnehmer-Zertifikaten nach Vorliegen eines Sperrgrundes.

Der Verwendungszweck des Sub-Registrator-Zertifikats besteht ausschließlich in der zertifikatsbasierenden SSL/TLS-Client-Authentifizierung an der Sub-Registrator-Webseite zur Aufgabenerledigung des Sub-Registrators und deren Derivate. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

Diese Registrierungsstelle liegt in der vollständigen Verantwortung des Domänen-Betreibers. T-Systems nimmt auch selbst als eigener Domänen-Betreiber die Aufgaben dieser Registrierungsstelle wahr.

Als optionale Funktion steht eine „Zentrale Schlüsselsicherung“ für Soft-PSE im Trust Center der T-Systems zur Verfügung (weitere Details sind im Dokument „Leistungsbeschreibung Shared-Business-CA“ beschrieben). Das Recht des Hochladens von Schlüsselmaterial (Dateiendung p12 bzw. pfx) und den dazugehörigen korrespondierenden Passwortdateien (Dateiendung pwd) obliegt dem Sub-Registrator. Das Herunterladen dieser Dateien erfolgt jedoch nach dem 4-Augen-Prinzip. Dafür wurden zwei Sub-Registratorrollen um entsprechende Rechte erweitert, um diese Dateitypen dediziert herunterladen zu können.
Folgende Sub-Registratorrollen stehen zur Verfügung:

- Sub-RA-P12 Operator
- Sub-RA-Pwd Operator

In den nachfolgenden Kapiteln werden diese Rollen bzw. Zertifikatstypen auch als „Derivate“ der Sub-Registratoren bezeichnet.

Ein Hinzufügen dieser Rollen zum normalen Sub-Registrator-Zertifikat (SubRA und Sub-RA-P12 bzw. Sub-RA und Sub-RA-Pwd) oder die Vereinigung beider Rollen Sub-RA-P12 und Sub-RA-Pwd ist nicht möglich.

Weitere Funktionen sind im Dokument „Leistungsbeschreibung Shared-Business-CA“ beschrieben.

1.3.3 Endteilnehmer (End Entity)

Im Kontext der SB-CA werden unter Endteilnehmer alle Zertifikatsnutzer verstanden, auf die ein Zertifikat ausgestellt werden kann. Diese sind im Einzelnen

- natürliche Personen (Endnutzer, Pseudonym),
- Personen- und Funktionsgruppen,
- juristische Personen (z.B. Stiftungen bürgerlichen Rechts, Körperschaften des Privatrechts wie Aktien Gesellschaften, eingetragene Vereine, Gesellschaften mit beschränkter Haftung, eingetragene Genossenschaften),
- Infrastrukturkomponenten (z.B. Maschinen wie Router, Gateways, Server, Firewalls oder andere Geräte).

Der Verwendungszweck der Endteilnehmer-Zertifikate ist beschrieben in den Kapiteln 1.4.1.2 und 1.4.1.3. Ferner gelten die in Kapitel 4.5.1 beschriebenen Regelungen.

Eine Personen- und Funktionsgruppe, juristische Person als auch Infrastrukturkomponente wird durch einen „Schlüsselverantwortlichen" vertreten, der durch den Domänen-Betreiber oder andere autorisierte Person bevollmächtigt wird. Dieser wird wie eine natürliche Personen identifiziert und registriert und ist verantwortlich für die sichere Verteilung, Nutzung und ggf. Sperrung des Zertifikats. Der Schlüsselverantwortliche kann die Sperrberechtigung an weitere Sperrberechtigte übertragen.

Benutzer-Zertifikate stellen eine Untermenge von Endteilnehmer-Zertifikate dar. Dies sind im einzelnen Zertifikate für

- natürliche Personen,
- Personen- und Funktionsgruppen und
- juristische Personen.

Im Gegensatz zu natürlichen Personen stimmt im Falle von juristischen Personen und Infrastruktur-Komponenten das Subjekt (Zertifikatantragssteller) nicht mit dem Endteilnehmer überein, auf das sich das Zertifikat bezieht.

Der Begriff Subjekt wird zur Abgrenzung von einem Endteilnehmer verwendet. Das Subjekt repräsentiert die natürliche Person, die bei der Vorlage/Übermittlung des Zertifikats registriert wird und an die das Zertifikat gebunden ist. Der Endteilnehmer ist Inhaber des privaten und öffentlichen Schlüssels und trägt die letztendliche Verantwortung für den Gebrauch des Zertifikats. Im Falle von natürlichen Personen stellt der Endteilnehmer gleichzeitig auch das Subjekt dar.

Als Endteilnehmer ist nicht die Institution Auftraggeber/Vertragspartner oder Domänen-Betreiber (z.B. Musterfirma) zu verstehen. Es ist aber dennoch möglich, dass auf diesem Repräsentant auch ein Endteilnehmer-Zertifikat ausgestellt wird (z.B. Max Mustermann für Musterfirma).
Welche Bedeutung die Verwendung der Begriffe Endteilnehmer und Subjekt im Einzelfall haben, hängt daher vom Kontext ab, in dem die Begriffe verwendet werden.

1.3.4 Vertrauender Dritter

Ein vertrauender Dritter (Relying Parties) ist eine natürliche Person oder Subjekt, die/das sich auf die Vertrauenswürdigkeit des von der SB-CA ausgestellten Zertifikats und/oder digitalen Signatur verlässt. Innerhalb der SB-CA kann ein vertrauender Dritter auch ein Endteilnehmer oder Registrator sein.

1.3.5 Andere Teilnehmer

Nicht anwendbar.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Zertifikate der SB-CA dürfen nur im zulässigen und geltenden gesetzlichen Rahmen verwendet werden. Dies gilt insbesondere unter Beachtung der länderspezifischen geltenden Ausfuhr- und Einfuhrbestimmungen.

1.4.1.1 Sicherheitsniveau

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

1.4.1.2 Zertifikate für natürliche Personen, Funktionsgruppen, Infrastruktur-komponenten

Diese Zertifikatstypen werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Erweiterungen „Schlüsselverwendung“ und „Erweiterte Schlüsselverwendung“ und den Festlegungen der Erklärung zum Zertifizierungsbetrieb eingesetzt. Einige Beispiele sind:

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

In Tabelle 1 sind die Sicherheitsniveaus bezogen auf die Verwendungszwecke dargestellt.

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

Tabelle 1: Verwendung von Zertifikaten für natürliche Personen, Infrastruktur-Komponenten

1.4.1.3 Zertifikate für juristische Personen

Über die in Tabelle 1 aufgeführten Verwendungszwecke hinaus kann ein Zertifikat für juristische Personen zu weiteren Zwecken verwendet werden. Voraussetzung ist aber, das ein Vertrauender Dritter dem Zertifikat in angemessener Weise vertrauen kann und der Verwendungszweck nicht durch gesetzlich oder auf Grund von Einschränkungen dieser Erklärung zum Zertifizierungsbetrieb oder sonstigen Vereinbarungen verboten ist.

In Tabelle 2 sind die Sicherheitsniveaus bezogen auf die Verwendungszwecke dargestellt.

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

Tabelle 2: Verwendung von Zertifikaten für juristische Personen

1.4.2 Unzulässige Verwendung von Zertifikaten

Zertifikate der SB-CA 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.

Die Zertifikate der SB-CA unterstützen nicht das Attribut „Nichtabstreitbarkeit“ (non repudation) in Verbindung mit einer Identität oder Berechtigung.

Aus dem Common Name (CN) muss die eindeutige Identität des Zertifikatsinhabers hervorgehen (z.B. natürliche Person, Infrastrukturkomponenten), ggf. sind die Einträge zu ergänzen (siehe Kapitel 3.1.2 und 3.1.3).

Ferner dürfen Endteilnehmer-Zertifikate nicht als CA- oder Root-CA-Zertifikate verwendet werden.

1.5 Verwaltung der Richtlinie

1.5.1 Zuständigkeit für die Erklärung

Diese Erklärung zum Zertifizierungsbetrieb (CPS) wird herausgegeben von:

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

1.5.2 Kontaktinformationen

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

Telefon: +49 (0) 1805-268204 [1]
E-Mail: telesec_support@t-systems.com
Fax: +49 (0) 2151-36607972
Internet: http://www.telesec.de

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

1.5.3 Eignungsprüfer der Erklärung zum Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie (CP)

In Kapitel 1.5.2 ist die Organisation aufgeführt, die sich verantwortlich zeigt, dass diese Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) oder Dokumente, die diese Erklärung zum Zertifizierungsbetrieb ergänzen oder untergeordnet sind, mit der Zertifizierungsrichtlinie (Certificate Policy, CP) vereinbar sind.

1.5.4 Genehmigungsverfahren dieser Erklärung zum Zertifizierungsbetrieb (CPS)

Der in Kapitel 1.5.1 benannte Herausgeber ist für diese Erklärung zum Zertifizierungsbetrieb (CPS) verantwortlich. Die Genehmigung dieser Erklärung zum Zertifizierungsbetrieb findet durch das Change Advisory Board statt.
Weitere Informationen zum Dokumentenmanagement finden Sie in den Kapiteln 9.12 ff.

1.6 Akronyme und Definitionen

Akronyme und Begriffsdefinitionen finden Sie in Kapitel C.

2 Veröffentlichungen und Verzeichnisdienste

2.1 Verzeichnisdienste

T-Systems betreibt Verzeichnisdienste (Datenbanken) für den Dienst Shared-Business-CA und ist auch für deren Inhalte verantwortlich.
Extrakte dieser Datenbanken stellen in aufbereiteter Form die Basis dar, um Zertifikatsinformationen und Zertifikatssperrlisten (CRL) auf dem Verzeichnisdienst zu veröffentlichen oder den Validierungsdienst (OCSP-Responder) mit Statusinformationen zu versorgen.

2.2 Veröffentlichung von Zertifikatsinformationen

T-Systems veröffentlicht in regelmäßigen Abständen Zertifikatssperrlisten (CRL), in der alle von der SB-CA ausgestellten und gesperrten Zertifikate enthalten sind. Es werden nur Zertifikate gesperrt, die zum Sperrzeitpunkt gültig sind.
In der Sperrliste für Zertifizierungsstellen (ARL) werden alle gesperrten CA-Zertifikate (jedoch keine Root-CA-Zertifikate) veröffentlicht.
T-Systems veröffentlicht alle von der SB-CA ausgestellten Endteilnehmer-Zertifikate auf einem öffentlichen Verzeichnisdienst, sofern der Domänen-Betreiber dieser Veröffentlichung zugestimmt hat. Der Verzeichnisdienst hat die Aufgabe, an einem zentralen Ort alle zur Veröffentlichung anstehenden Zertifikate als auch die aktuelle Sperrinformationen per standard-konforme Sperrlisten (CRL, ARL), für alle PKI-Beteiligten zur Verfügung zu stellen. Der Zugriff auf den Verzeichnisdienst erfolgt über das Protokoll LDAP (Lightweight Directory Access Protocol) und ist hinsichtlich Zugriffsschutz konfigurierbar (öffentlich oder Benutzername/Passwort-Schutz).
Über eine Benutzer-Webseite können Endteilnehmer Zertifikate anderer Domänen-Betreiber suchen, sofern die Veröffentlichung von diesen gestattet ist.
Ferner stellt SB-CA einen Validierungsdienst (OCSP-Responder) zur Verfügung, der über das Internetprotokoll „Online Certificate Status Protocol“ (OCSP) agiert und einem Benutzer den Status von X.509-Zertifikaten zurück liefert.
Die aktuellen Konfigurationsdaten werden im Dokument „Zertifikats- und Konfigurationsdatenblatt der Shared-Business-CA“ veröffentlicht.
T-Systems veröffentlicht die aktuelle Erklärung zum Zertifizierungsbetrieb (CPS) als auch die CA- und Root-CA-Zertifikate unter: http://www.telesec.de

Die Veröffentlichung der Zertifikate ist abhängig vom Zertifikatstyp und den Regelungen gemäß Tabelle 3.

Zertifikatstyp:	Vorgaben:
Root-CA-Zertifikat „Deutsche Telekom Root CA 2“	Dieses Zertifikat ist bei Endteilnehmern und Vertrauenden Dritten als „Vertrauensanker“ Zertifikatsspeicher der Anwendung installiert. Ggf. kann das Zertifikat abgerufen werden über den Verzeichnisdienst der SB-CA oder per Internet über: http://www.telesec.de
CA-Zertifikat „Shared Business CA“	Das Zertifikat kann heruntergeladen werden über den Verzeichnisdienst der SB-CA oder per Internet über: http://www.telesec.de
Master-Registrator-Zertifikat	Dieser Zertifikatstyp zur Verwaltung steht nicht zum Herunterladen zur Verfügung.
Sub-Registrator-Zertifikat und deren Derivate	Dieser Zertifikatstyp zur Verwaltung steht nicht zum Herunterladen zur Verfügung.

Endteilnehmer-Zertifikate (natürliche oder juristische Personen, Personen- und Funktionsgruppen und Infrastruktur- Komponenten (nur Server- und Mail-Gateway-Zertifikate)	Die zur veröffentlichen Zertifikate stehen auf dem Verzeichnisdienst zur Verfügung oder können auch über die Benutzer-Webseite gesucht werden (nach Eingabe von Benutzername/Passwort).
Endteilnehmer-Zertifikate (Router-/Gateway-, Domain-Controller-Zertifikate)	Die Zertifikate stehen nicht zum Herunterladen zur Verfügung. In Abstimmung mit dem Domänen-Betreiber können zusätzliche Zertifikatstypen veröffentlicht werden.
OCSP-Zertifikate	Das Zertifikat kann heruntergeladen werden über den Verzeichnisdienst der SB-CA.

Tabelle 3: Vorgaben für die Veröffentlichung von Zertifikaten

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Aktualisierungen dieser Erklärung zum Zertifizierungsbetrieb (CPS) werden, wie in Kapitel 9.12 beschrieben, veröffentlicht.

Zertifikate werden zum Zeitpunkt der Erzeugung veröffentlicht, sofern der Domänen-Betreiber nicht explizit einen Zugriffsschutz auf den Teilbaum [2] (Ebene Master-Domäne) des Verzeichnisdienstes wünscht. Statusinformationen per OSCP zu Zertifikaten werden gemäß dieser Erklärung zum Zertifizierungsbetrieb veröffentlicht.

2.4 Zugang zu den Verzeichnisdiensten

Der Abruf der Sperrlisten (CRL, ARL) und die Nutzung des OCSP-Dienstes für die Endteilnehmer (Kapitel 1.3.3), Vertrauende Dritte (Kapitel 1.3.4) oder Registrierungsstellen (Kapitel 1.3.2), unterliegt keiner Zugriffskontrolle. Der Lesezugriff auf diese Informationen unterliegt keiner Beschränkung.
Der lesende Zugriff für die Zertifikatsnehmer und -nutzer auf Informationen der CA- und Root-CA (siehe Kapitel 2.1) über einschlägige Webseiten unterliegt ebenfalls keiner Zugriffskontrolle.

Das Suchen von Zertifikaten über den Verzeichnisdienst unterliegt keiner Zugriffskontrolle. Das Suchen von Zertifikaten über die rollenspezifischen Webseiten ist erst nach erfolgreicher Authentifizierung mittels Zertifikat oder Benutzername/Passwort möglich.
Der Domänen-Betreiber bestimmt jedoch durch einen Zugriffsschutz, ob Zertifikate überhaupt im Verzeichnisdienst abrufbar sind.

[2] Der Domänen-Betreiber teilt T-Systems schriftlich mit, ob eine Veröffentlichung der Zertifikate auf Ebene der Master-Domäne gewünscht ist. Dem Domänen-Betreiber steht es frei, eine Zertifikatsveröffentlichung einzelner Sub-Domäne (Zuständigkeitsbereich) einzurichten.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

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

Innerhalb eines Zertifikates ist zu unterscheiden nach

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

Der Issuer DN repräsentiert den eindeutigen Namen der ausstellenden Zertifizierungsinstanz (CA) und soll in diesem Dokument nicht weiter betrachtet werden.

3.1.1 Namensformen

3.1.1.1 Konventionen für die Bestandteile des Subject-DN

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

3.1.1.2 Country Name (C)

Dieses Attribut enthält die Landes-Kennung, in welchem der Zertifikatsinhaber niedergelassen ist. Dies ist ein aus zwei Buchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist. Maßgebend ist dabei die Lokalisierung des Domänen-Betreibers.

Beispiele: C = DE für Deutschland. C = US für Vereinigte Staaten von Amerika.

3.1.1.3 Organization Name (O)

Dieses Attribut enthält den Organisationsnamen (z.B. Firma, Institution, Behörde) des Zertifikatsinhabers. Es ist erlaubt, dieses Attribut innerhalb eines Zuständigkeitsbereiches auch mit unterschiedlichen Namen zu belegen.

Beispiele: O = Musterfirma GmbH, O = Deutsche Telekom AG

3.1.1.4 Organizational Unit Name 1 (OU1)

Dieses Attribut sollte möglichst den DNS-Bezeichner der Internet-Domäne (Master- bzw. Betreiber-Domäne) des Domänen-Betreibers (Domänennamen) enthalten, um eine globale Eindeutigkeit zu erreichen. Andere Namen sind nach Vereinbarung mit T-Systems erlaubt. Der Organizational Unit Name 1 wird vor der Generierung des ersten Master-RA-Zertifikats für eine Master-Domäne festgelegt und kann danach nicht mehr geändert werden (siehe auch Kapitel 1.3.2.1). Der Organizational Unit Name 1 ist im Zertifikats- und Konfigurationsdatenblatt aufgeführt.

Beispiele: OU1 = musterfirma.de, OU1 = t-systems.com

3.1.1.5 Organizational Unit Name 2 (OU2)

Dieses Attribut enthält bei Endanwender-, Gruppen-, Funktions-, Rollen- und Sub-RA-Zertifikate den Bezeichner eines Zuständigkeitsbereichs (Sub-Domäne). Ein Zuständigkeitsbereich muss eindeutig einer Master-Domäne zugeordnet sein.

Beispiele: OU2 = niederlassung-muenchen, OU2 = headquater oder OU2 = ssl-vpn.

3.1.1.6 Organizational Unit Name 3 (OU3)

Bei Endanwender- und Gruppen, Funktions-, Rollenzertifikaten kann mit diesem optionalen Attribut eine weitere Zuordnung des Zertifikatsinhabers zu einer Organisationseinheit erfolgen.

Beispiele: OU3 = Vertrieb, OU3 = Niederlassung Duesseldorf, OU3 = <Vorname Nachname> (wenn CN (Kapitel 3.1.1.7) einer nicht aussagekräftigem Ziffern- bzw. Buchstabenkombination (z.B. Personalnummer) entspricht).

3.1.1.7 Common Name (CN)

Das Attribut „Common Name“ enthält den Vornamen und Nachnamen bzw. die Kennung des Endteilnehmers (IP-Adresse, Server-Name, Name des Mail-Gateways oder Domain-Controllers).
Bei Server-Zertifikaten können auch mehrere Server-Namen eingetragen werden, die nach Zertifikatserzeugung in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name, Kapitel 7.1.2.3) erscheinen.

Beispiele: CN = Max Mustermann, CN = web1.musterfirma.de, CN = <IP-Adresse>, CN = GR: Funktionspostfach technischer Support, CN = PN: <Pseudonym> (siehe auch Kapitel 3.1.3), PersNr 1029384756 (siehe auch Kapitel 3.1.1.6).

Die Kennung „GRP:“ kennzeichnet Gruppen-, Funktions-, Rollenzertifikate, „PN:“ kennzeichnet das Pseudonym.

3.1.1.8 Mail-Address

Das Attribut „E-Mail-Adresse“ enthält bei

- Natürlichen Personen die E-Mail-Adresse des Zertifikatsinhabers,
- Juristischen Personen die E-Mail-Adresse der Personenvereinigungen, Gruppen, Funktionen und Rollen, usw.,
- Personen- und Funktionsgruppe die E-Mail-Adresse der Gruppe oder Rolle,
- Infrastruktur-Komponenten die E-Mail-Adresse eines Administrators oder eines Funktionspostfachs,
- Master-Registrator-Zertifikaten die E-Mail-Adresse des Master-Registrators oder eines Funktionspostfachs,
- Sub-Registrator-Zertifikaten die E-Mail-Adresse des Sub-Registrators oder eines Funktionspostfachs.

Beispiele: max.mustermann@musterfirma.de, pki-registrator@example.com

3.1.1.9 User Principal Name (UPN)

Der User Principal Name ist ein benutzerfreundlichen (d.h. leicht zu merkenden) Namen, der zur Windows-Anmeldung an der Domäne bzw. Active Directory dient. Dieser besteht aus einem Benutzerkontonamen (auch Anmeldenamen genannt) und der Domäne, in der das Benutzerkonto gespeichert ist (Objektname“@„Domänenname).
Der UPN kann, muss aber nicht der Mail-Adresse entsprechen.

Beispiele: mail = max.mustermann@musterfirma.de, mail = max.mustermann@local-server.com

Bei bestimmten Benutzer-Zertifikaten (natürliche Personen, Personen- und Funktionsgruppen, juristische Personen) erscheint der UPN nach Zertifikatserzeugung in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name, Kapitel 7.1.2.3).

3.1.1.10 Fully Qualified Domain Name (FQDN)

Der vollständige Name einer Domäne wird als ihr Fully Qualified Domain Name (FQDN) bezeichnet. Der Domain-Name ist in diesem Fall eine absolute Adresse.

Beispiel: FQDN = www.example.com, FQDN = s-server.pki.example.de

Bei Router-Zertifikaten erscheint der FQDN nach Zertifikatserzeugung in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name).

3.1.1.11 Serial Number (SN)

Innerhalb eines Zuständigkeitsbereiches (Sub-Domäne) können natürliche und juristische Personen gleichlautenden Subject-DN aufweisen. Zur Unterscheidung wird dazu im Subject-DN eine Seriennummer vergeben. Bei manueller Ausstellung von Benutzer-Zertifikaten über die Sub-RA- und Benutzer-Webseiten wird dieses Attribut und dessen Wert automatisch von der Zertifizierungsinstanz erzeugt.
Im Bulk-Prozess wird eine Seriennummer nicht vergeben, da im Beantragungsprozess der gleichlautende Subject DN erkannt wird und der Sub-Registrator diesen anschließend manuell ändern muss.

Beispiel: SN = 1 für 1. Max Mustermann und SN = 2 für 2. Max Mustermann innerhalb gleichem Zuständigkeitsbereichs.

3.1.2 Aussagekraft von Namen

Der Name bzw. die Kennung muss den Endteilnehmer bzw. Zertifikatsnehmer eindeutig und nachprüfbar identifizieren.
Im Falle von Zertifikaten für Personen- und Funktionsgruppen- und Pseudonymen kann T-Systems vom Domänen-Betreiber verlangen, die wahre Identität des Zertifikatsinhabers berechtigten Dritten offenzulegen.

3.1.3 Pseudonymität bzw. Anonymität der Zertifikatsinhaber

Für natürliche Personen können Pseudonyme vergeben werden. Pseudonym-Zertifikate werden mit dem Präfix „PN:“ im Common Name (CN) kenntlich gemacht. Unter Pseudonymen werden auch Gruppen-, Funktions-, Rollenzertifikate verstanden. Diese Zertifikate werden, mit Ausnahme von Zertifikaten für Infrastruktur-Komponenten, mit dem Präfix „GRP:“ im Common Name (CN) gekennzeichnet.

Beispiele: PN: Novalis, PN: George Sand, GRP: Einkauf, GRP: Technischer Support

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

T-Systems gewährleistet, das Zertifikate für natürliche und juristische Personen mit gleichem Subject-DN (siehe Kapitel 3.1.1.1 ff) nur einmal innerhalb des Zuständigkeitsbereiches (Sub-Domäne) vorkommen. Dies wird durch die Vergabe einer Seriennummer im Subject-DN (siehe Kapitel 3.1.1.11) gewährleistet.

Natürliche und juristische Personen als Endteilnehmer können zwei oder mehr Zertifikate mit demselben eindeutigen Subject-DN besitzen, diese unterscheiden sich jedoch in der Schlüsselverwendung bzw. erweiterten Schlüsselverwendung (z.B. Signatur, Schlüsselverschlüsselung, Client-Authentifizierung, Smartcard-Anmeldung) und der Seriennummer. Durch die Erneuerungsfunktion können zeitlich begrenz auch mehrere Zertifikate mit dem gleichen Subject-DN erstellt sein.

Zertifikate für Infrastrukturkomponenten mit gleichem Subject-DN (siehe Kapitel 3.1.1.1 ff) können mehrfach vorkommen.

3.1.6 Erkennung, Authentifizierung und Rolle von Warenzeichen

Es liegt in der Verantwortung des Domänen-Betreibers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. oder Rechte des geistigen Eigentums verletzen. Die Zertifizierungsstelle SB-CA der T-Systems ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Domänen-Betreibers.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Methode zum Besitznachweis des privaten Schlüssels

Der Zertifikatsantragsteller muss bei einer Beantragung 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 in der Zertifizierungsstelle stattfindet (Bulk siehe Kapitel 3.2.3.1.3 und 3.2.3.1.5).

3.2.2 Authentifizierung der Identität von Organisationen

Grundvoraussetzung für die Nutzung der SB-CA ist die Einrichtung einer Master-Domäne (Betreiber-Domäne) innerhalb der Shared-Business-CA. Die T-Systems gewährleistet, dass die Namensgebung der Betreiber-Domäne nur einmal vorkommt. Zur eindeutigen Kennzeichnung erhält die Master-Domäne den Domänennamen (Second-Level-Domain, Third-Level-Domain) des Auftraggebers, der auch gleichzeitig in jedem Zertifikat unter dem Attribut „Organizational Unit Name 1“ (OU1) (siehe Kapitel 3.1.1.4) erscheint.
Sofern der Domänennamen nicht zur Namensbildung herangezogen werden kann, darf auch eine andere Namengebung erfolgen: Es ist jedoch unbedingt sicherzustellen, dass beispielsweise keine Namen die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt, sowie politische Parolen, verwendet werden dürfen. Ebenfalls sind Namen zu vermeiden, die den Verdacht erzeugen, Identitäten von Organisationen zu täuschen oder zu verschleiern. Es sind Namen zu bevorzugen, die Rückschlüsse auf den Domänen-Betreiber zulassen.

Zur Einrichtung der Master-Domäne (Betreiber-Domäne) bedarf es einer Authentifizierung der Identität bzw. Identitätsprüfung des Auftraggebers (Inhaber der Betreiber-Domäne). Im Falle, dass ein Dritter im Namen des Domänen-Betreibers die Beauftragung einer Betreiber-Domäne durchführt, ist zusätzlich noch von diesem eine schriftliche Vollmacht erforderlich.
Im Falle, dass ein Dritter im Namen des Domänen-Betreibers die Zertifikatsverwaltung für diesen durchführt, bedarf es einer schriftlichen Vereinbarung über die Übertragung der Rechte und Pflichten dieser Erklärung zum Zertifizierungsbetrieb zwischen dem Domänen-Betreiber und dem Dritten, die der T-Systems unverzüglich zu übermitteln ist.

T-Systems führt folgende Prüfungen durch:

- Feststellung der Existenz der Organisation durch einen Identitätsprüfungsservice oder Identitätsprüfungsdatenbank eines Dritten oder wahlweise durch entsprechende aktuelle Organisationsdokumente, die von einer zuständigen Stelle oder Behörde ausgestellt oder bei ihr

eingereicht wurden, die die Existenz der Organisation bestätigen (z.B. Handelsregisterauszug oder vergleichbares Dokument, das nicht älter als 30 Tage sein darf, Dienstsiegel),
- Prüfung des/der Domänennamen gegen öffentlich zugängliche Datenbanken (z.B. Denic eG),
- Feststellung der Existenz des im Dokuments „Auftrag zur Einrichtung einer Master-Domäne" angegebenen verantwortlichen Ansprechpartners, der als Master-Registrator bestimmt ist. Ferner ist zu prüfen, ob die genannte Person in der Organisation (Inhaber Betreiber-Domäne) beschäftigt ist oder eine Vollmacht besitzt, im Namen der Organisation zu handeln,
- Zusätzliche Prüfungen nach Bedarf (z.B. zur Erfüllung der US-amerikanischen Exportbestimmungen und -lizenzen der Industrie- und Wissenschaftsbehörde (Bureau of Industry and Science, BIS) des amerikanischen Handelsministeriums).

Die Namensgebung der Master-Domäne(n) (siehe auch Kapitel 3.1.1.4) erfolgt in Absprache zwischen dem Domänen-Betreiber oder Dritten, und der T-Systems.
Bei der Einrichtung der Master-Domäne werden für die Zertifikatstypen Server-, Router/Gateway- und Domain-Controller nur die Domänen eingerichtet, für die der Domänen-Betreiber einen entsprechenden Nachweis (z.B. Denic) erbringen kann. Die Domänennamen gelten für die gesamte Master-Domäne und vererben sich auch auf Zuständigkeitsbereiche (Sub-Domänen).

Die Verwaltung der Master-Domänen erfolgt durch Master-Registratoren (siehe Kapitel 1.3.2.2.1), die vom Domänen-Betreiber bestellt werden.
Das Master-Registrator-Zertifikat dient zur Authentifizierung an der entsprechenden Webseite und dient zur Verwaltung der Betreiber-Domäne.

Für die Ausstellung weiterer Master-Registrator-Zertifikate, Konfigurationsänderungen der Master-Domäne oder Sperrung von Master-Registrator-Zertifikaten werden geeignete und prüfbare Identifikationsunterlagen benötigt, aus denen die Person, Organisation oder der Änderungsanforderung eindeutig hervorgehen.

Die erfolgreiche Identitätsprüfung der Organisation mündet in der Ausstellung eines Master-Registrator-Zertifikats, ausgestellt auf den Namen des Master-Registrators, der innerhalb der Master-Domäne (Betreiber-Domäne) als oberste Registrierungsstelle (Kapitel 1.3.2.2.1) auftritt. Für den höchstmöglichen Sicherheitsanspruch werden Master-Registrator-Zertifikate grundsätzlich auf Smartcard ausgestellt. Ungültige oder gesperrte Master-Registrator-Zertifikate bedürfen einer Neubeantragung mit entsprechender Identitätsprüfung.

Änderungen des Zertifikatsinhaltes eines Master-Registrator-Zertifikats (z.B. anderer Zertifikatsinhaber (CN), Organisationsnamen (O) oder Organizational Unit Name 1 (OU1) sind dem Herausgeber dieser Erklärung zum Zertifizierungsbetrieb unverzüglich anzuzeigen. Bei Zuwiderhandlung behält sich die T-Systems vor, das Master-Registrator-Zertifikat und ggf. auch die daraus hervorgehenden Sub-Registrator-Zertifikate unverzüglich zu sperren.

3.2.3 Authentifizierung der Identität von Endteilnehmern

Die Authentifizierung der Identität bzw. Identifikation von Endteilnehmern (siehe Kapitel 1.3.3) wird von den bei dem Domänenbetreiber etablierten Registrierungsstelle (siehe Kapitel 1.3.2 ff) durchgeführt.
Standardmäßig stehen bei SB-CA folgende Registrierungsvarianten zur Verfügung:
- zentrale Registrierung, d.h. der Sub-Registrator stellt, nach erfolgreicher Registrierung, über die Sub-RA-Webseite die Zertifikate bzw. Schlüsselmaterial für den Endteilnehmer direkt aus.
- dezentrale Registrierung, d.h. der Benutzer stellt über Internet den Zertifikatsantrag, den der Sub-Registrator bearbeitet (Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage)).

Auf eine detailliertere Beschreibung der beiden Registrierungsmodelle wird an dieser Stelle auf das Dokument „Leistungsbeschreibung Shared-Business-CA" verwiesen.

Der Ablauf der jeweiligen Registrierungsvariante wird im entsprechenden Handbuch beschrieben. Es gelten folgende Richtlinien:

- Grundsätzlich erfolgt die Registrierung eines Endteilnehmers über den zuständigen Sub-Registrator. Eine Ausnahme bildet die automatisierte Massengenerierung von Schlüsselmaterial (Bulk).
- Der Sub-Registrator entscheidet über Genehmigung, Ablehnung oder Zurückstellung (Wiedervorlage) des Zertifikatsantrags.
- Für eine Erneuerung von Benutzer-Zertifikate(n) (natürliche Personen, Personen- und Funktionsgruppen, juristische Personen) ist eine erneute Registrierung nicht erforderlich, da auf den gleichen Datenbestand zugegriffen wird. Abweichungen davon liegen im Ermessen des Domänen-Betreibers.

3.2.3.1 Registrierung von Registrierungsmitarbeitern des Domänen-Betreibers

3.2.3.1.1 Registrierung eines Master-Registrators

Die Registrierung des Master-Registrators erfolgt durch T-Systems im Rahmen der Identitätsprüfung einer Organisation (siehe Kapitel 3.2.2).

3.2.3.1.2 Registrierung eines Sub-Registrators

Der Domänen-Betreiber kann ein oder mehrere Zuständigkeitsbereiche (Sub-Domänen) administrieren lassen, die durch Sub-Registratoren verwaltet werden. Dabei gelten folgende Regelungen:

- Die Registrierung eines Sub-Registrators und das Ausstellung des Sub-Registrator-Zertifikats erfolgt durch den Master-Registrator des Domänen-Betreibers.
- Die Registrierung erfolgt durch persönliches Erscheinen des Sub-Registrators oder auf Basis eines integeren Datenbestands des Domänen-Betreibers.

Gleiche Vorgehensweise gilt auch für die Sub-Registrator-Derivate (siehe Kapitel 1.3.2.2.2), die für das optionale Leistungsmerkmal „Zentraler Schlüsselsicherung“ zum Herunterladen von P12- und Pwd-Dateien benötigt werden.

3.2.3.1.3 Registrierung von natürlichen Personen

Die Registrierung einer natürlichen Person (Endnutzer, Pseudonym) erfolgt zentral oder dezentral durch den Sub-Registrator. Dabei gelten folgende Richtlinien:

- Die Registrierung einer natürlichen Person erfolgt durch den zuständigen Sub-Registrator des Domain-Betreibers. Die Registrierung erfolgt durch persönliches Erscheinen des Endteilnehmers, eines sicheren Registrierungsprozesses auf Basis von Identitätsdokumenten (z.B. Personalausweis, Unternehmensausweis, Reisepass) oder auf Basis eines integeren Datenbestands des Domänen-Betreibers.
- Auf expliziten Wunsch kann die natürliche Person an Stelle des realen Namens ein Pseudonym in das Zertifikat aufnehmen lassen. Bei der Verwendung eines Pseudonyms ist die reale Identität des Endteilnehmers bzw. Zertifikatsnehmer durch den Sub-Registrator zu prüfen, bewerten und nach Freigabe zu dokumentieren. Die Verantwortung obliegt dem Domänen-Betreiber.
  Pseudonym-Zertifikate sind mit dem Präfix „PN:“ im Common Name (CN) kenntlich zu machen. Falls das gleiche Pseudonym mehr als einmal existiert, muss die Registrierungsstelle eine Eindeutigkeit herstellen. Die Nutzung von Pseudonymen unterliegt verschiedenen Namenseinschränkungen. Ausgeschlossen werden Namen die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt, sowie politische Parolen, usw.
- Das Ausstellen von Zertifikaten erfolgt entweder einzeln via Web-Antrag oder von Schlüsselmaterial (privater Schlüssel und Zertifikat) automatisiert per Massengenerierung (Bulk).
- Die Registrierung muss auf sichere Art und Weise erfolgen und ist entsprechend schriftlich zu dokumentieren.

Die Registrierungsstelle (Sub-Registrator) muss die reale Identität des Endteilnehmers bzw. Zertifikatsnehmer prüfen und in ihren Registrierungsunterlagen dokumentieren.

Bei der Verwendung von Pseudonymangaben finden die Ausführungen von Kapitel 3.1.3 Beachtung.

3.2.3.1.4 Registrierung von Personen- und Funktionsgruppen

Die Registrierung von Personen- und Funktionsgruppen erfolgt zentral oder dezentral durch den Sub-Registrator. Dabei gelten folgende Richtlinien:

- Die Registrierung von Personen- und Funktionsgruppen erfolgt durch den zuständigen Sub-Registrator des Domain-Betreibers. Die Registrierung erfolgt durch persönliches Erscheinen eines Schlüsselverantwortlichen, eines sicheren Registrierungsprozesses auf Basis von Identitätsdokumenten (z.B. Personalausweis, Unternehmensausweis, Reisepass) oder auf Basis eines integeren Datenbestands des Domänen-Betreibers.
- Gruppen- und Funktionszertifikate sind mit dem Präfix „GRP:“ im Common Name (CN) kenntlich zu machen. Falls die gleiche Namensgebung mehr als einmal existiert, muss die Registrierungsstelle eine Eindeutigkeit herstellen. Die Nutzung von Gruppen- und Funktionszertifikaten unterliegt verschiedenen Namenseinschränkungen. Ausgeschlossen werden Namen die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt, sowie politische Parolen, usw.
- Das Ausstellen von Zertifikaten erfolgt entweder einzeln via Web-Antrag oder von Schlüsselmaterial (privater Schlüssel und Zertifikat) automatisiert per Massengenerierung (Bulk).
- Die Registrierung muss auf sichere Art und Weise erfolgen und ist entsprechend schriftlich zu dokumentieren.

Bei der Verwendung von Personen- und Funktionsgruppen finden die Ausführungen von Kapitel 3.1.3 Beachtung.

3.2.3.1.5 Registrierung von juristischen Personen

Die Registrierung von juristischen Personen erfolgt zentral oder dezentral durch den Sub-Registrator. Dabei gelten folgende Richtlinien:

- Die Registrierung von juristischen Personen erfolgt durch den zuständigen Sub-Registrator des Domänen-Betreibers. Die Registrierung erfordert das persönliche Erscheinen eines Schlüsselverantwortlichen, der sich durch Vorlage geeigneter Identifikationsdokumente ausgewiesen hat und für die ordnungsgemäße Erstellung des Zertifikatsantrages als auch für die Installation des Zertifikats verantwortlich ist. Der Sub-Registrator prüft, ob die juristische Person auch rechtlich existiert und dass andere im Zertifikat enthaltene Organisationsattribute (ausschließlich nicht verifizierter Endteilnehmer-Informationen) identifiziert wurden, wie z.B. der Besitz einer Internet- oder E-Mail-Domäne.
- Die Ausstellung von Zertifikaten erfolgt einzeln via Web-Antrag.
- Das Ausstellen von Schlüsselmaterial (privater Schlüssel und Zertifikat) für juristische Personen per automatisierte Massengenerierung (Bulk) ist verboten.
- Die Registrierung muss auf sichere Art und Weise erfolgen und ist entsprechend schriftlich zu dokumentieren.

3.2.3.1.6 Registrierung von Infrastrukturkomponenten

Die Registrierung von Infrastrukturkomponenten erfolgt zentral oder dezentral durch den Sub-Registrator. Dabei gelten folgende Richtlinien:

- Die Registrierung von Infrastrukturkomponenten erfolgt bei Web-Anträgen durch den zuständigen Sub-Registrator des Domänen-Betreibers. Die Registrierung erfordert das persönliche Erscheinen eines Schlüsselverantwortlichen, der sich durch Vorlage geeigneter Identifikationsdokumente ausgewiesen

hat und für die ordnungsgemäße Erstellung des Zertifikatsantrages als auch für die Installation des Zertifikats verantwortlich ist.
- Bei der Ausstellung von Zertifikaten für Infrastruktur-Komponenten werden nur die erlaubten Domänennamen verwendet (siehe auch Kapitel 3.2.2). Dies gilt auch für einen Dritten, der im Namen des Domänen-Betreibers Zertifikate ausstellt oder für Wiederverkäufer (Reseller) einzelne Zuständigkeitsbereiche (Sub-Domänen).
- Das Ausstellen von Schlüsselmaterial (privater Schlüssel und Zertifikat) für juristische Personen per automatisierte Massengenerierung (Bulk) ist verboten.
- Die Registrierung muss auf sichere Art und Weise erfolgen und ist entsprechend schriftlich zu dokumentieren.

3.2.4 Nicht verifizierte Teilnehmerangaben

Nicht verifizierte Informationen sind Informationen, die ohne Prüfung ins Zertifikat übernommen werden und umfassen:
- Organisationseinheit (OU1, Kapitel 3.1.1.4),
- Zuständigkeitsbereich (Sub-Domäne) (OU2, Kapitel 3.1.1.5),
- sonstige Informationen, die im Zertifikat als nicht verifiziert gekennzeichnet sind (z.B. Schlüsselverwendung, erweitere Schlüsselverwendung).

3.2.5 Überprüfung der Berechtigung

Sofern im Zertifikat der Name einer natürlichen Person dergestalt mit dem Namen einer Organisation verknüpft ist, dass daraus eine Berechtigung erkennbar wird, im Namen dieser Organisation handeln zu können, wird die Registrierungsstelle des Domänen-Betreibers
- die Organisation auf ihre Existenz hin zu überprüfen. Dabei wird ein Identitätsprüfungsservice oder eine Identitätsprüfungsdatenbank eines Dritten genutzt oder wahlweise Dokumente bei der zuständigen Regierung oder Behörde abgefordert, die die Existenz der Organisation bestätigt, und
- Geschäftsinformationen einzuholen, die die Person, die den Zertifikatsantrag stellt, bei der Organisation beschäftigt ist und ob sie ggf. dazu autorisiert ist, im Namen der Organisation zu handeln.

3.2.6 Kriterien für Interoperabilität

Nicht relevant.

3.3 Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung

Sofern keine Gründe entgegen sprechen, muss der Endteilnehmer vor Ablauf eines gültigen Zertifikats sich ein neues Zertifikat beschaffen, um die Kontinuität der Zertifikatsnutzung gewährleisten zu können. Ob für die Folgebeauftragung ein neues Schlüsselpaar generiert wird, ist abhängig von dem verwendeten Schlüsselmaterial (Smartcard, Soft-PSE).

Bei einer Folgebeantragung kann die gleiche Smartcard mit den darauf befindlichen Schlüsselpaar verwendet werden. Andernfalls ist ein Folge-Zertifikat auf einer neuen Smartcard auszustellen. Es gelten die Regelungen der Registrierung wie in den Kapitel 3.2.3.1 ff beschrieben. Sofern die Smartcard eine interne Schlüsselgenerierung unterstützt, können bei einer Folgebeauftragung neue Schlüsselpaare verwendet werden.

Bei Folgebeauftragungen als Soft-PSE werden im Allgemeinen neue Schlüsselpaare erzeugt, für bestimmte Infrastrukturkomponenten (z.B. Web-Server) kann aber auch der vorhandene Schlüssel erneut verwendet werden. Ob eine Schlüsselerneuerung stattfindet, liegt im Ermessen des Domänen-Betreibers.

Bei einer Zertifikatserneuerung wird auf Basis des gleichen Subject-DN (Kapitel 3.1.1.1) ein neues Zertifikat generiert, das einen neuen Gültigkeitszeitraum und Seriennummer besitzt. Eine Zertifikatserneuerung ist grundsätzlich nur mit gültigem Zertifikat möglich.

Für die Ausstellung weiterer Master-Registrator-Zertifikate werden geeignete und prüfbare Identifikationsunterlagen benötigt, aus denen die Person, Organisation oder der Änderungsanforderung eindeutig hervorgehen.

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Gültige Zertifikate können vom Endteilnehmer selbst erneuert werden, sofern die Vorgaben des Domänen-Betreibers nicht entgegenwirken und/oder Einschränkungen einer Schlüsselsicherung (key back-up) dies nicht verhindern. Die Zertifikatserneuerung basiert auf den bestehenden Zertifikatsdaten, eine erneute Registrierung ist nicht vorgesehen.

3.3.2 Identitätsprüfung und Authentifizierung bei Schlüsselerneuerungen nach Zertifikatssperrung

Eine Zertifikatserneuerung eines gesperrten Zertifikats ist nicht möglich. Es steht nur die Option der Neubeauftragung zur Verfügung (siehe Kapitel 3.2.2 und 3.2.3).

3.3.3 Identitätsprüfung nach Ablauf des Gültigkeitszeitraums

Nach Ablauf des Gültigkeitszeitraumes ist die Zertifikatserneuerung nicht möglich. Es steht nur die Option der Neubeauftragung zur Verfügung (siehe Kapitel 3.2.2 und 3.2.3).

3.4 Identifizierung und Authentifizierung bei Sperranträgen

Die Identifizierung von Sperranträgen erfolgt durch die Mitteilung von Zertifikatsinhalten (z.B. Common Name, Organisation/Firma, E-Mailadresse), um das zu sperrende Zertifikat suchen und selektieren zu können. Die Authentifizierung der Sperrung erfolgt über das dem Zertifikatsinhaber bekannte Sperrpasswort.

4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen?

Folgende Personen können einen Zertifikatsantrag stellen:

- Natürliche Personen, die als Subjekt des Zertifikats erscheinen,
- Autorisierte Personen einer Registrierungsstelle (Sub-Registratoren und deren Derivate, Kapitel 1.3.2.2.2),
- Autorisierte Personen von Personen- und Funktionsgruppen, juristischen Personen und Infrastrukturkomponenten,
- Autorisierte Personen der T-Systems im Rahmen der Einrichtung und Verwaltung einer Master-Domäne (Kapitel 3.2.2).

4.1.2 Antragsstellungsverfahren und Pflichten

4.1.2.1 Domänen-Betreiber

Der Domänen-Betreiber geht mit T-Systems ein vertragliches Verhältnis ein.

Zur Einrichtung der Master-Domäne (Betreiber-Domäne) verpflichtet sich der Domänen-Betreiber das Dokument „Auftrag zur Einrichtung einer Master-Domäne für die Shared-Business-CA“ wahrheitsgemäß auszufüllen und mit den erforderlichen Identifikationsdokumenten T-Systems vorzulegen, damit T-Systems wie in Kapitel 3.2.2 die Identifikationsprüfung durchführen kann.
Jede wesentliche Organisationsänderung des Domänen-Betreibers (z.B. Umfirmierung) sind dem Herausgeber dieser Erklärung zum Zertifizierungsbetrieb (siehe Kapitel 1.5.2) unverzüglich schriftlich anzuzeigen.

Der Domänen-Betreiber verpflichtet sich auch, die Regelungen dieses Dokuments „Erklärung zum Zertifizierungsbetrieb (CPS)“ auf seine Registrierungsmitarbeiter (Master- und Sub-Registrator und deren Derivate, Kapitel 1.3.2.2.2) und Endteilnehmer zu übertragen.

Bei Nutzung der Shared-Business-CA mit Auslandsbezug sind die geltenden nationalen Export- und Importbestimmungen zu beachten.

4.1.2.2 Endteilnehmer und Registrierungsmitarbeiter

Alle Endteilnehmer und Registrierungsmitarbeiter (Master- und Sub-Registrator und deren Derivate, Kapitel 1.3.2.2.2) verpflichten sich das Dokument „Erklärung zum Zertifizierungsbetrieb (CPS)“ einzuhalten.

Ferner verpflichtet sich der Endteilnehmer und Registrierungsmitarbeiter,

- das die im Zertifikatsantrag gemachten Angaben wahr und korrekt sind,
- zu einer Übermittlung des öffentlichen Schlüssels und der Zertifikatsdaten an T-Systems zur Zertifikatserzeugung,
- einen Nachweis über den Besitz des privaten Schlüssels zu führen, der in Verbindung mit dem zertifizierten öffentlichen Schlüssel steht.

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

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

4.2.1.1 T-Systems

Zur Einrichtung und Verwaltung der Master-Domäne führt T-Systems Trust Center die Identifikation und Authentifizierung des Domänen-Betreibers durch wie in Kapitel 3.2.2 beschrieben.

4.2.1.2 Domänen-Betreiber

Die Identifizierung und Authentifizierung der Endteilnehmer erfolgt durch Master- und Sub-Registratoren und deren Derivate (siehe Kapitel 1.3.2.2 ff) innerhalb der beim Domänen-Betreibers etablierten zuständigen Registrierungsstelle.
Insbesondere verpflichtet sich der Sub-Registrator, bei der Ausstellung von Zertifikaten für Infrastruktur-Komponenten die einen Domänennamen beinhalten, sorgsam diesen zu prüfen und keine Zertifikate auszustellen, die einen Domänennamen enthalten, der nicht dem Zuständigkeitsbereich (Sub-Domäne) zugewiesen ist.

Für die Massengenerierung von Zertifikaten für natürliche und juristische Personen und Personen- und Funktionsgruppen via Bulk-Beantragung gelten die Regelungen wie in Kapitel 3.2.3.1.3, 3.2.3.1.4 und 3.2.3.1.5 beschrieben.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Nur nach erfolgreicher Registrierung des Zertifikatsnehmers wird ein Zertifikatsantrag angenommen und zur Bearbeitung weitergeleitet. Dies ist gegeben, wenn die Identifikation und Authentifizierung aller erforderlichen Daten erfolgreich war (siehe Kapitel 3.2.3).

Im Falle einer Ablehnung des Antrags ist der Zertifikatsnehmer in geeigneter Weise unter Angabe von Gründen zu benachrichtigen.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

4.2.3.1 T-Systems

Die Bearbeitung des Zertifikatantrags für Master-Registratoren auf Basis des Dokuments „Einrichtung einer Master-Domäne für Shared-Business-CA“ beginnt innerhalb eines angemessenen Zeitraums nach Erhalt der Beauftragung.

4.2.3.2 Domänen-Betreiber

Die Bearbeitung von Zertifikatsanträgen obliegt der Zuständigkeit und Verantwortung des Domänen-Betreibers.

4.3 Zertifikatsausstellung

4.3.1 Maßnahmen der Zertifizierungsstelle während der Ausstellung von Zertifikaten

Eine Zertifikatsausstellung erfolgt erst nach erfolgreicher Registrierung eines Zertifikatsantrags durch T-Systems (für Master-Registratoren) oder durch den Domänen-Betreiber (für Sub-Registratoren oder Endteilnehmer).
Das Zertifikat wird ausgestellt auf die im Zertifikatsantrag enthaltenen Informationen.

Ferner können Zertifikatsanträge gestellt werden von

- Benutzer über die entsprechende Benutzer-Webseite,
- Infrastrukturkomponenten (z.B. Router) über die SCEP-Schnittstelle, oder
- Benutzer/Applikation über die Mail-Schnittstelle.

Die Ausstellung der Zertifikate erfolgt in diesen Fällen erst nach Genehmigung der Anträge durch den zuständigen Sub-Registrator nach erfolgreicher Registrierung. Der Sub-Registrator kann auch die Zertifikatsanträge bearbeiten (editieren, zurückstellen, ablehnen), sofern die Zertifikatsanträge fehlerhaft sind oder die erforderlichen Registrierungsunterlagen nicht vorliegen.

Die CA bearbeitet die im System eingestellten Zertifikatsanträge im Online-Verfahren.

4.3.2 Benachrichtigung von Endteilnehmern über die Ausstellung von Zertifikaten

Der Endteilnehmer, Registrierungsmitarbeiter oder die autorisierte Person erhalten über die Ausstellung des Zertifikats eine Benachrichtigung per E-Mail, in der die relevanten Informationen enthalten sind.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme durch den Zertifikatsinhabers

Das folgende Verhalten stellt die Annahme eines Zertifikats dar:

- Das Herunterladen und Installieren eines Zertifikats auf Basis einer Mitteilung oder deren Anhang durch den Endteilnehmer,
- Die Annahme des Schlüsselmaterials inkl. PIN bzw. Passwort (Smardcard oder Soft-PSE), das für den Endteilnehmer oder Registrator ausgestellt wurde,
- Falls der Endteilnehmer nicht innerhalb einer vom Domänen-Betreiber definierten Frist nach Erhalt des Zertifikats Einwände gegen das Zertifikat oder seinen Inhalt gegenüber der zuständigen Registrierungsstelle erhebt,
- Widerspruch gegenüber der zuständigen Registrierungsstelle innerhalb einer vom Domänen-Betreiber definierten Frist nach Erhalt des Zertifikats bzw. Inhalt des Zertifikats.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Die Veröffentlichung von Zertifikaten erfolgt über einen Verzeichnisdienst oder Web-basierenden Zugriff auf eine Datenbank. Dabei gelten folgende Regelungen:

- Die Veröffentlichung der Zertifikate ist abhängig vom Zertifikatstyp und den Regelungen gemäß Tabelle 3.
- Es können zusätzlich bestimmte Zertifikatstypen (siehe Tabelle 3) nach Absprache mit dem Domänen-Betreiber veröffentlicht werden,
- Ob der Verzeichnisdienst öffentlich oder geschützt ist, liegt im Ermessen des Domänen-Betreibers und wird bei Einrichtung der Master-Domäne (Betreiber-Domäne) konfiguriert. Der Master-Registrator kann in den darunterliegenden Zuständigkeitsbereichen (Sub-Domänen) ebenfalls einen Zugriffsschutz konfigurieren.

4.4.3 Benachrichtigung über die Zertifikatsausstellung durch die Zertifizierungsstelle an weitere Instanzen

Die Benachrichtigung einer weiteren Instanz (z.B. Registratoren, Administratoren) ist möglich.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Das Zertifikat und der zugehörige private Schlüssel darf nur entsprechend den Regelungen der „Allgemeinen Geschäftsbedingungen TeleSec Shared-Business-CA" (AGB SB-CA) und dieser CPS verwendet werden.

Die Verwendung des privaten Schlüssels, mit dem dazu gehörigen zertifizierten öffentlichen Schlüssel, ist erst gestattet, nachdem der Endteilnehmer das Zertifikat angenommen hat (Kapitel 4.4.1). Die Zertifikatsnutzung wird bestimmt durch die Vorgaben und Verwendungszweck des Domänen-Betreibers. Die technische Zertifikatsverwendung ist im Zertifikat als Attribut „Schlüsselverwendung" und „erweiterte Schlüsselverwendung" definiert.

Alle Endteilnehmer und Registratoren sind verpflichtet,

- ihre privaten Schlüssel vor unbefugtem Gebrauch schützen,
- den privaten Schlüssel nach Ablauf des Gültigkeitszeitraums oder der Sperrung des Zertifikats nicht mehr benutzen, außer zur Einsichtnahme verschlüsselter Daten (z.B. Entschlüsselung von E-Mails),
- das Zertifikat sperren zu lassen, falls der zugehörige private Schlüssel nicht mehr verfügbar oder kompromittiert ist bzw. der Verdacht darauf besteht.

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

- Der Schlüsselverantwortliche (Kapitel 1.3.3) ist für das Kopieren bzw. Weitergeben der Schlüssel an den/die Endteilnehmer verantwortlich.
- Der Schlüsselverantwortliche muss den/alle Endteilnehmer zur Einhaltung dieser Regelungen im Umgang mit dem privaten Schlüssel verpflichten.
- Zertifikatssperrungen können auf Personen aus dem Kreise der Endteilnehmer übertragen werden. Der Schlüsselverantwortliche muss dem/den Sperrberechtigten die Details zu Sperranlässen und das Sperrpasswort mitteilen.
- Nach ausscheiden einer Person aus dem Kreise der Endteilnehmer muss ein Missbrauch des privaten Schlüssels durch den Schlüsselverantwortliche verhindern werden, indem das Passwort/PIN geändert oder die Soft-PSE/Smartcard eingezogen wird. Falls dies nicht möglich ist, muss ein neues Zertifikat mit neuem Schlüsselpaar beantragt werden.
- Ein neues Zertifikat ist auch dann zu beantragen, wenn der ausscheidende Endteilnehmer sperrberechtigt war.
- Eine Übertragung der Verantwortung an einen neuen oder zusätzlichen Schlüsselverantwortlichen ist bei der zuständigen Registrierungsstelle zu beantragen und zu dokumentieren. Der neue Schlüsselverantwortliche ist gemäß dieser Erklärung zum Zertifizierungsbetrieb (CPS) zu identifizieren und zu registrieren, seine Autorisierung als Schlüsselverantwortlicher muss nachgewiesen werden.

Für Zertifikate von juristischen Personen als auch Infrastrukturkomponenten gelten darüber hinaus folgenden Anforderungen:

- Der Schlüsselverantwortliche (Kapitel 1.3.3) ist für das Kopieren und Weitergeben der Schlüssel an den/die Endteilnehmer verantwortlich.
- Nach ausscheiden einer Person aus dem Kreise der Endteilnehmer muss ein Missbrauch des privaten Schlüssels durch den Schlüsselverantwortliche verhindern werden, indem das Passwort/PIN geändert oder die Soft-PSE/Smartcard eingezogen wird. Falls dies nicht möglich ist, muss ein neues Zertifikat mit neuem Schlüsselpaar beantragt werden.
- Eine Übertragung der Verantwortung an einen neuen oder zusätzlichen Schlüsselverantwortlichen ist bei der zuständigen Registrierungsstelle zu beantragen und zu dokumentieren. Der neue Schlüsselverantwortliche ist gemäß dieser Erklärung zum Zertifizierungsbetrieb (CPS) zu identifizieren und zu registrieren, seine Autorisierung als Schlüsselverantwortlicher muss nachgewiesen werden.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Vertrauende Dritte

Jeder Vertrauende Dritte, der ein Zertifikat einsetzt, das von der SB-CA ausgestellt wurde, sollte

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

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

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Bei einer Re-Zertifizierung wird dem Zertifikatsnehmer ein neues Zertifikat mit neuer Seriennummer, neuem Gültigkeitszeitraum und gleichen Zertifikatsinhalten des Endteilnehmers (Subject-DN) ausgestellt. Mit der Zertifikatserneuerung kann eine Schlüsselerneuerung verbunden sein. Bei der Verwendung des gleichen Schlüsselpaares wird jedoch vorausgesetzt, dass die eindeutige Zuordnung von Zertifikatsnehmer und Schlüssel erhalten bleibt, keine Kompromittierung des Schlüssels vorliegt und die kryptographischen Verfahren (z.B. Schlüssellänge) für die Gültigkeitsdauer des neuen Zertifikats noch ausreichend sind.

4.6.1 Gründe für eine Zertifikatserneuerung

Sofern keine Gründe entgegen sprechen, muss der Endteilnehmer vor Ablauf eines gültigen Zertifikats sich ein neues Zertifikat beschaffen, um die Kontinuität der Zertifikatsnutzung gewährleisten zu können.
Eine Zertifikatserneuerung ist nur innerhalb eines definierten Zeitraums vor Ablauf der Gültigkeit des vorhandenen Zertifikats möglich.
Abhängig vom Zertifikatstyp muss zur Zertifikatserneuerung das Zertifikat inkl. privaten Schlüssel oder der elektronisch kodierte Zertifikatsantrag (Request, inkl. Referenznummer) vorliegen.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Grundsätzlich liegt die Zertifikatserneuerung im Ermessen des Domänen-Betreibers. Eine Zertifikatserneuerung darf nur von einer natürlichen Personen, Registrierungsmitarbeiter, Administrator oder autorisierte Person beantragt werden.
Ob eine Zertifikatserneuerung überhaupt durch den Zertifikatsinhaber erfolgen soll oder durch den zuständigen Sub-Registrator (zentrale Registrierung), liegt im Ermessen des Domänen-Betreibers und sollte unbedingt vorab im Rahmen der „Schlüsselsicherung (key back-up)“ definiert sein.

4.6.3 Bearbeitung von Zertifikatserneuerungen

Das Erneuerungsverfahren muss gewährleisten, dass nur berechtigte Zertifikatsnehmer (Benutzer, Registrierungsmitarbeiter, Administrator oder autorisierte Person) diesen Prozess durchführen können.

Als Authentifizierungsmerkmal wird bei der Erneuerung von Endteilnehmer-Zertifikaten der Besitz des vollständigen Schlüsselmaterials (Zertifikat und privater Schlüssel) vorausgesetzt. Eine Ausnahme bilden Zertifikate von Infrastrukturkomponenten, bei denen der private Schlüssel auf der Komponente verbleibt. Zur

Erneuerung wird der elektronisch kodierte Zertifikatsantrag (Request) als auch die letzte Referenznummer des Zertifikats erwartet.

Die Erneuerung von Registrator-Zertifikaten (Master-RA- und Sub-RA-Zertifikate und deren Derivate, Kapitel 1.3.2.2.2) erfolgt durch den Zertifikatsinhaber selbst. Es ist zu beachten, dass nach dem Erneuerungsprozess das zu erneuernde Zertifikat nicht automatisch gesperrt wird. Es obliegt Registrator für eine Übergangsfrist (Erneuerungszeitraum bis Ablauf des Zertifikats) über zwei gültige Zertifikate zu verfügen oder das zu erneuernde Zertifikat anschließend zu sperren (Kapitel 4.9.3.3 ff).

Bei Benutzer-Zertifikaten (außer für Registrierungsmitarbeiter, siehe Kapitel 1.3.3) kann der Zertifikatsnehmer die Erneuerung selbst durchführen, sofern die Belange des Domänen-Betreibers dies nicht einschränken.
Die Erneuerung von Zertifikaten von Infrastrukturkomponenten erfolgt durch den zuständigen Sub-Registrator.
Mit der Einrichtung des Zuständigkeitsbereiches (Sub-Domäne) erfolgt eine Konfiguration, ob mit der Erneuerung das zu erneuernde Endteilnehmer-Zertifikat automatisch gesperrt wird oder nicht. Damit kann der Endteilnehmer für eine Übergangsfrist (Erneuerungszeitraum bis Ablauf des Zertifikats) über zwei gültige Zertifikate verfügen. Es obliegt dem Domänen-Betreiber oder autorisierten Person (Registrator, Benutzer) das zu erneuernde Zertifikat anschließend zu sperren (Kapitel 4.9.3.2 ff).

Sofern eine Schlüsselsicherung (key back-up, siehe auch Kapitel 1.3.2.2.2) definiert ist, sollte die Zertifikatserneuerung auch durch einen Sub-Registrator und deren Derivate erfolgen, sofern ihm das vollständige Schlüsselmaterial und PIN vorliegen.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.6.7 Benachrichtigung weiterer Stellen über eine Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

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

4.7.1 Gründe für eine Schlüsselerneuerung

Zur Erhöhung des Sicherheitsaspekts ist eine Schlüsselerneuerung sinnvoll. Die Maßnahme liegt im Ermessen des Domänen-Betreibers.

4.7.2 Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beauftragen?

Es gelten die Regelungen gemäß Kapitel 4.6.2.

4.7.3 Bearbeitung von Schlüsselerneuerungsanträgen

Wenn der autorisierte Benutzer oder autorisierte Person die Zertifikatserneuerung (Schlüsselerneuerung) beauftragt, wird automatisch das erneuerte Zertifikat ausgestellt.

4.7.4 Benachrichtigung des Zertifikatsinhabers über die Ausstellung mit neuem Schlüsselmaterial

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.7.5 Annahme einer Zertifikatserneuerung mit neuem Schlüsselmaterial

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.7.6 Veröffentlichung eines Zertifikats mit neuem Schlüsselmaterial durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.7.7 Benachrichtigung weiterer Stellen über eine Zertifikaterstellung durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Gründe für eine Zertifikatsänderung

Das Ausstellen eines neuen Zertifikats ist zwingend erforderlich, wenn sich die Zertifikatsinhalte (mit Ausnahme des öffentlichen Schlüssels) gegenüber dem bisherigen ausgestellten Zertifikats ändern bzw. geändert haben (z.B. O, OU1, OU2, OU3, CN, E-Mail, siehe auch Kapitel 3.1.1.2 bis 3.1.1.8).

4.8.2 Wer darf eine Zertifikatsänderung beauftragen?

Es gelten die Regelungen gemäß Kapitel 4.6.2.

4.8.3 Bearbeitung von Zertifikatsänderungen

Wenn sich Zertifikatsinhalte ändern, ist eine erneute Identifizierung wie im Falle der Erst-Beauftragung erforderlich (siehe Kapitel 3.2.3.1.2 bis 3.2.3.1.6). Das vorhergehende Zertifikat ist umgehend zu sperren.

4.8.4 Benachrichtigung des Zertifikatsinhabers über die Ausstellung eines Zertifikats

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.8.5 Annahme einer Zertifikatserneuerung mit geänderten Zertifikatsdaten

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.8.6 Veröffentlichung eines Zertifikats mit geänderten Daten durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.8.7 Benachrichtigung weiterer Stellen über eine Zertifikatserstellung durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Gründe für eine Sperrung

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

- Abhandenkommen des privaten Schlüssels (z.B. Verlust oder Diebstahl),
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor,
- Die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr korrekt (siehe auch Kapitel 4.8.1),
- Es liegt ein Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen vor,
- Verwendung und Handhabung des Zertifikats im Widerspruch zu vertraglichen Regelungen oder der Zertifizierungsrichtlinie (CP) / Erklärung zum Zertifizierungsbetrieb (CPS) des Zertifikatsnehmers oder Zertifikatsgebers. Bei der Entscheidungsfindung sind zu beachten:
  - die Art und Anzahl der erhaltenen Beschwerden,
  - die Identität des/der Beschwerdeführer/s,
  - die geltende Rechtsprechung,
  - Reaktionen des Endteilnehmers auf den Verdacht schädlicher Nutzung.
- Der zertifizierte Schlüssel oder die damit verwendeten kryptografischen Algorithmen entsprechen nicht mehr den aktuellen Anforderungen,
- Der Zertifikatsnehmer kündigt das Vertragsverhältnis,
- Sperrung des zu erneuernden Zertifikats nach dem Zertifikatserneuerungsprozess,
- Bei Vertragsbeendigung bzw. -kündigung zwischen dem Domänen-Betreiber und Endteilnehmer, sofern nichts anderes vereinbart ist,
- Bei Feststellung, das eine wesentliche Voraussetzung für die Ausstellung des Zertifikats nicht erfüllt war,
- Gesetzliche Vorschriften oder richterliche Urteile.

Das T-Systems Trust Center kann Endteilnehmer- und Registrator-Zertifikate sperren und in der Zertifikatssperrliste (CRL) veröffentlichen, wenn folgende Gründe vorliegen

- Abhandenkommen des privaten Schlüssels (z.B. Verlust oder Diebstahl),
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor,
- Über die im Vertrag vereinbarten Zahlungsfristen hinaus gehender, erheblicher Zahlungsverzug,
- Die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr korrekt (siehe auch Kapitel 4.8.1),
- Es liegt ein Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen vor,

- Verwendung und Handhabung des Zertifikats im Widerspruch zu vertraglichen Regelungen oder der Zertifizierungsrichtlinie (CP) / Erklärung zum Zertifizierungsbetrieb (CPS) des Zertifikatsnehmers oder Zertifikatsgebers. Bei der Entscheidungsfindung sind zu beachten:
  - die Art und Anzahl der erhaltenen Beschwerden,
  - die Identität des/der Beschwerdeführer/s,
  - die geltende Rechtsprechung,
  - Reaktionen des Endteilnehmers auf den Verdacht schädlicher Nutzung.
- Der zertifizierte Schlüssel (öffentliche Schlüssel) oder die damit verwendeten kryptografischen Algorithmen entsprechen nicht mehr den aktuellen Anforderungen,
- Sperrung des zu erneuernden Zertifikats nach dem Zertifikatserneuerungsprozess,
- Bei Vertragsbeendigung bzw. -kündigung zwischen dem Domänen-Betreiber und T-Systems, sofern nichts anderes vereinbart ist,
- Bei Feststellung, das eine wesentliche Voraussetzung für die Ausstellung des Zertifikats weder erfüllt war noch auf deren Erfüllung verzichtet wurde,
- Gesetzliche Vorschriften oder richterliche Urteile.

Falls der Verdacht auf missbräuchlichen Einsatz eines Zertifikats besteht, kann dies unter Angabe des Common Name (CN) oder Zertifikatsseriennummer sowie der Beschreibung des Missbrauchs dem Service Desk mitgeteilt werden. Diese Fälle werden an T-Systems und/oder zuständigen Domänen-Betreibers bzw. Registrierungsstelle weitergeleitet. Es werden geeignete Prüfmaßnahmen eingeleitet. Bestätigt sich ein begründeter missbräuchlicher Zertifikatseinsatz, kann T-Systems das Zertifikat sperren (siehe auch Kapitel 1.3.2.1, 4.9.1, 4.9.2, und 4.9.3 ff).

4.9.2 Wer kann eine Sperrung beauftragen?

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

- natürliche Personen,
- Schlüsselverantwortliche als auch vom Schlüsselverantwortlichen autorisierte Sperrberechtigten (Personen- und Funktionsgruppen, juristische Personen als auch Infrastrukturkomponenten),
- Registrierungsmitarbeiter des Domänen-Betreibers (Master- bzw. Sub-Registrator und deren Derivate, Kapitel 1.3.2.2.2),
- T-Systems Trust Center.

Insbesondere gelten die Regelungen aus Kapitel 4.9.3.1.

4.9.3 Ablauf einer Sperrung

4.9.3.1 Sperrvarianten

Für Endteilnehmer und Registratoren stehen unterschiedliche Sperrvarianten zur Verfügung. Zertifikatssperrungen sind möglich über

- die Benutzer-Webseite für alle Endteilnehmer (außer Master- und Sub-RA und deren Derivate (Kapitel 1.3.2.2.2), Infrastrukturkomponenten),
- die Sub-RA-Webseite für alle Endteilnehmer (außer Master und Sub-RA und deren Derivate),
- die Master-RA-Webseite für alle Endteilnehmer und Sub-Registratoren (außer Master-RA),
- das T-Systems Service Desk nur für Master-RA, und
- den Sperrservice des Domänen-Betreibers (außer Master-RA).

Tabelle 4 stellt die Sperrvarianten in Abhängigkeit zu den Rolleninhabern dar.

	Benutzer-Webseite:	Sub-RA-Webseite:	Master-RA-Webseite:	T-Systems Service Desk:	Sperrservice-Web-seiten des Domänen-Betreibers:
Master-Registrator	✗	✗	✗	✓	✗
Sub-Registrator und deren Derivate	✗	✗	✓	✗	✓
Natürliche Person	✓	✓	✓	✗	✓
Personen- und Funktionsgruppen	✓	✓	✓	✗	✓
Juristische Person	✓	✓	✓	✗	✓
Infrastruktur-komponenten	✗	✓	✓	✗	✓

Tabelle 4: Sperrvarianten

4.9.3.1.1 Sperrungen über die Benutzer-Webseite

Über die Benutzer-Webseite können vom Benutzer selbst alle Benutzer-Zertifikate gesperrt werden, nicht aber Zertifikate von Infrastruktur-Komponenten und von Master- und Sub-Registratoren und deren Derivate (Kapitel 1.3.2.2.2).

4.9.3.1.2 Sperrungen über Sub-RA-Webseite

Über die Sub-Registrator-Webseite können vom Sub-Registrator (oder deren Derivate, Kapitel 1.3.2.2.2) alle Endteilnehmer-Zertifikate gesperrt werden, nicht aber Zertifikate von Master- und Sub-Registratoren und deren Derivate.

4.9.3.1.3 Sperrungen über Master-RA-Webseite

Über die Master-Registrator-Webseiten können vom Master-Registrator alle Endteilnehmer- und Sub-Registrator-Zertifikate gesperrt werden, außer für Master-Registratoren selbst.

4.9.3.1.4 Sperrungen über T-Systems Service Desk

Über das T-Systems Service Desk können ausschließlich Master-Registrator-Zertifikate gesperrt werden. Zur Sperrung autorisierte Personen und Institutionen (siehe Kapitel 4.9) können die Sperrung des Master-Registrator-Zertifikats entweder per E-Mail oder Telefon beauftragen.

Weitere Informationen zum Service Desk sind im Dokument „Service-Level-Agreement TeleSec Shared-Business-CA“ enthalten.

4.9.3.1.5 Sperrservice-Webseiten des Domänen-Betreibers

Optional kann der Domänen-Betreiber einen eigenen Sperrservice installieren, über den er alle Zertifikatstypen (außer Master-Registrator-Zertifikate) sperren kann.

Über die Sperrservice-Webseiten können alle Endteilnehmer- und Sub-Registrator-Zertifikate gesperrt werden, außer für Master-Registratoren.

4.9.3.2 Sperrung von Endteilnehmer-Zertifikaten

4.9.3.2.1 Zertifikatssperrungen für natürliche Personen

Eine Zertifikatssperrung kann initiiert werden durch eine in Kapitel 4.9.2 aufgeführte Person oder Institution bei Vorliegen von mindestens einem in Kapitel 4.9.1 aufgeführten Sperrgrunds.

Die Sperrung von Zertifikaten für natürliche Personen erfolgt in der Regel durch den Benutzer selbst, den zuständigen Master- oder Sub-Registrator (oder deren Derivate, Kapitel 1.3.2.2.2) oder optional durch den Sperrservice des Domänen-Betreibers über die rollenspezifischen Webseiten (Kapitel 4.9.3.1.1, 4.9.3.1.2, 4.9.3.1.3 oder 4.9.3.1.5).

In jedem Fall sind Inhalte des Subject-DN des Zertifikatsinhabers (z.B. Common Name) erforderlich, um das zu sperrende Zertifikat suchen und selektieren zu können. Die Authentifizierung der Sperrung erfolgt über das dem Zertifikatsinhaber bekannte Sperrpasswort.

Die Sperrung ist endgültig. Anschließend ist manuell vom Master- oder Sub-Registrator bzw. Sperrservice-Operator eine neue Zertifikatssperrliste (CRL) zu generieren.

4.9.3.2.2 Zertifikatssperrungen für juristische Personen, Personen- und Funktionsgruppen und Infrastrukturkomponenten

Eine Zertifikatssperrung kann initiiert werden durch eine in Kapitel 4.9.2 aufgeführte Person oder Institution bei Vorliegen von mindestens einem in Kapitel 4.9.1 aufgeführten Sperrgrunds.

Die Sperrung von Zertifikaten für Personen – und Funktionsgruppen, juristische Personen und Infrastrukturkomponenten erfolgt in der Regel durch oder auf Initiative des Schlüsselverantwortlichen oder Sperrberechtigten, den zuständigen Master- oder Sub-Registrator (oder deren Derivate) oder optional durch den Sperrservice des Domänen-Betreibers über die rollenspezifischen Webseiten (Kapitel 4.9.3.1.2, 4.9.3.1.3 oder 4.9.3.1.5).

In jedem Fall sind Inhalte des Subject-DN des Zertifikatsinhabers (z.B. Common Name) erforderlich, um das zu sperrende Zertifikat suchen und selektieren zu können. Die Authentifizierung der Sperrung erfolgt über das dem Zertifikatsinhaber bekannte Sperrpasswort.

Die Sperrung ist endgültig. Anschließend ist manuell vom Master- oder Sub-Registrator bzw. Sperrservice-Operator eine neue Zertifikatssperrliste (CRL) zu generieren.

4.9.3.3 Sperrung von Registrator-Zertifikaten

4.9.3.3.1 Sperrung eines Master-Registrator-Zertifikats

Eine Zertifikatssperrung kann initiiert werden durch eine in Kapitel 4.9.2 aufgeführte Person oder Institution bei Vorliegen von mindestens einem in Kapitel 4.9.1 aufgeführten Sperrgrunds.

Die Sperrung von Zertifikaten für Master-Registratoren erfolgt in der Regel durch das Service Desk der T-Systems über die rollenspezifischen Webseiten (Kapitel 4.9.3.1.4).

In jedem Fall sind Inhalte des Subject-DN des Zertifikatsinhabers (z.B. Common Name) erforderlich, um das zu sperrende Zertifikat suchen und selektieren zu können. Die Authentifizierung der Sperrung erfolgt über das dem Zertifikatsinhaber bekannte Sperrpasswort. Nach Eingang eines Sperrauftrags beim Service Desk ergreift T-Systems wirtschaftlich angemessenen Schritte, um den Sperrauftrag unverzüglich zu bearbeiten.

Die Sperrung ist endgültig. Anschließend ist manuell vom Master- oder Sub-Registrator bzw. Sperrservice-Operator eine neue Zertifikatssperrliste (CRL) zu generieren.

4.9.3.3.2 Sperrung eines Sub-Registrator-Zertifikats oder deren Derivate

Eine Zertifikatssperrung kann initiiert werden durch eine in Kapitel 4.9.2 aufgeführte Person oder Institution bei Vorliegen von mindestens einem in Kapitel 4.9.1 aufgeführten Sperrgrunds.

Die Sperrung von Zertifikaten für Sub-Registratoren erfolgt in der Regel durch den zuständigen Master-Registrator oder optional durch den Sperrservice des Domänen-Betreibers über die rollenspezifischen Webseiten (Kapitel 4.9.3.1.3 oder 4.9.3.1.5).

In jedem Fall sind Inhalte des Subject-DN des Zertifikatsinhabers (z.B. Common Name) erforderlich, um das zu sperrende Zertifikat suchen und selektieren zu können. Die Authentifizierung der Sperrung erfolgt über das dem Zertifikatsinhaber bekannte Sperrpasswort.

Die Sperrung ist endgültig. Anschließend ist manuell vom Master- oder Sub-Registrator bzw. Sperrservice-Operator eine neue Zertifikatssperrliste (CRL) zu generieren.

4.9.3.4 Sperrung eines CA- bzw. Root-CA-Zertifikats

4.9.3.4.1 Sperrung des Shared-Business-CA-Zertifikats

Die T-Systems wird bei Vorliegen eines Sperrgrundes des CA-Zertifikats diesen unter Berücksichtigung wirtschaftlich angemessener Schritte unverzüglich bearbeitet und bewerten und ggf. Maßnahmen zur Zertifikatssperrung einleiten. T-Systems behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. T-Systems garantiert die Veröffentlichung der Sperrung innerhalb einer Zertifizierungsstellen-Sperrliste (ARL).

4.9.3.4.2 Sperrung des Zertifikats „Deutsche Telekom CA 5“

T-Systems verpflichtet sich zu einer Sperrung des Zertifikats, sobald der Verdacht einer Schlüsselkompromittierung besteht. T-Systems behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. T-Systems garantiert die Veröffentlichung der Sperrung innerhalb einer Zertifizierungsstellen-Sperrliste (ARL).

4.9.3.4.3 Sperrung des Zertifikats „Deutsche Telekom Root CA 2“

Die T-Systems wird bei Vorliegen eines Sperrgrundes des Root-CA-Zertifikats diesen unter Berücksichtigung wirtschaftlich angemessener Schritte unverzüglich bearbeitet und bewerten und ggf. Maßnahmen zur Zertifikatssperrung einleiten. T-Systems behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen Mitarbeiter des Trust Centers durchgeführt. Die Sperrung wird nicht über eine Zertifizierungsstellen-Sperrliste (ARL) bekannt gegeben. Bei einer Sperrung des Root-Zertifikats wird jedoch das damit ausgestellte CA-Zertifikat gesperrt, das wiederum in einer ARL veröffentlicht wird.

4.9.3.5 Sperrung von externen Web-Server-Zertifikaten

T-Systems verpflichtet sich zu einer Sperrung des Zertifikats, sobald der Verdacht einer Schlüsselkompromittierung besteht. T-Systems behält sich eine Sperrung des Zertifikats vor, wenn dies aus betrieblichen Gründen notwendig werden sollte. Die Sperrung dieses Zertifikats wird von einem zuständigen

Mitarbeiter des Trust Centers durchgeführt. Die Sperrung wird über eine Zertifikatssperrliste (CRL) bekannt gegeben. Ein gesperrtes Web-Server-Zertifikat wird unverzüglich durch ein neues ersetzt.

T-Systems garantiert, dass der Zugang zum Web-Server gesperrt wird, wenn dessen Sicherheit durch eine Sperrung dieses Zertifikats gefährdet ist.

4.9.3.6 Sperrung des OCSP-Responder-Zertifikats

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

4.9.4 Fristen für einen Sperrauftrag

Sobald ein Sperrgrund gemäß Kapitel 4.9.1 vorliegt, muss der Sperrauftrag so schnell als möglich innerhalb einer wirtschaftlich angemessenen Frist gestellt werden.

4.9.5 Bearbeitungsfristen der Zertifizierungsstelle für Sperranträge

Die Sperrung durch den Endteilnehmer, Registrator, Operator oder Service Desk wird unmittelbar nach dem Sperrvorgang an die angeschlossen Systems weitergegeben. Der OCSP-Dienst, der auf diese Systems zugreift, verfügt damit über den aktuellen Zertifikatsstatus.

4.9.6 Überprüfungsvorgaben für Vertrauende Dritter

Vertrauende Dritte müssen die Möglichkeit erhalten, den Status von Zertifikaten überprüfen zu können. Zu diesem Zweck kann der OCSP-Responder genutzt werden, der den aktuellen Status eines Endteilnehmer-, Registrator- oder OCSP-Responder-Zertifikat anzeigt.
Eine weitere Methode, wie ein Vertrauender Dritter überprüfen kann, ob ein Zertifikat gesperrt ist, ist die Prüfung der aktuellen Zertifikatssperrliste (CRL), die auf dem Verzeichnisdienst der SBCA veröffentlicht wird.

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

4.9.7 Veröffentlichungsfrequenz von Sperrinformationen

Die Zertifikatssperrliste (CRL) als auch Zertifizierungsstellen-Sperrliste (ARL) wird, wie im Kapitel 2.3 beschrieben, über den Verzeichnisdienst publiziert.
Die Zertifikatssperrliste (CRL), in der Zertifikats-Sperrungen von Endteilnehmern aufgeführt sind, wird mindestens ein Mal pro Tag aktualisiert und über den Verzeichnisdienst veröffentlicht.
In der Sperrliste für Zertifizierungsstellen (ARL) werden alle gesperrten CA-Zertifikate (keine Root-CA-Zertifikate) veröffentlicht. Die Aktualisierung erfolgt alle 6 Monate oder ereignisbezogen, die Veröffentlichung erfolgt über den entsprechenden Verzeichnisdienst.
Gesperrte Zertifikate, die außerhalb des Gültigkeitszeitraums liegen, werden aus der Sperrliste entfernt.

4.9.8 Maximale Latenzzeit von Sperrlisten

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

4.9.9 Online- Verfügbarkeit von Sperr-/Statusinformationen

Sperr- und Statusinformationen von Zertifikaten sind abrufbar über den Verzeichnisdienst und/oder über die rollenspezifischen Webseiten. Zusätzlich stellt T-Systems Online-Informationen zum Zertifikatsstatus via OCSP bereit. Die URL des OCSP-Responders ist im Zertifikat in der Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)"(siehe Kapitel 7.1.2.9) aufgeführt.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

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

4.9.11 Andere verfügbare Formen der Veröffentlichung von Sperrinformationen

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 unverzüglich zu sperren.

4.9.13 Suspendierung von Zertifikaten

Nicht anwendbar.

4.9.14 Wer kann eine Suspendierung beantragen?

Nicht anwendbar.

4.9.15 Verfahren der Suspendierung

Nicht anwendbar.

4.9.16 Beschränkung des Suspendierungszeitraums

Nicht anwendbar.

4.10 Statusauskunftsdienste von Zertifikaten

4.10.1 Betriebseigenschaften

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

4.10.2 Verfügbarkeit des Dienstes

Die Statusauskunftsdienste für Zertifikate stehen, unter Beachtung der Ausführungen des Service-Level-Agreements, zur Verfügung.

4.10.3 Optionale Funktionen

Nicht relevant.

4.11 Beendigung des Vertragsverhältnisses

Im Falle einer Vertragskündigung durch den Domänen-Betreiber oder der T-Systems erfolgt zunächst unmittelbar die Deaktivierung der Master-Domäne(n). Dies hat zur Folge, dass eine Neubeantragung als auch Erneuerung von Sub-Registrator- und Endteilnehmer-Zertifikaten nicht mehr möglich ist, nicht jedoch die Anmeldung an der Webseite, um bestehende Zertifikate sperren zu können.

Zertifikate, die nach dem Tarifmodell Classic und Classic Pro entgeltpflichtig wurden, behalten ihre Gültigkeit bis Ablauf des Zertifikats, eine Erneuerung ist nicht möglich. Eine Sperrung erfolgt durch den Zertifikatsinhaber oder T-Systems bei Vorliegen einer der in Kapitel 4.9.1 beschrieben Sperrgründe.

Zertifikate, die nach dem Tarifmodell Advanced entgeltpflichtig wurden, werden nach dem Kündigungsdatum gesperrt und verlieren die Gültigkeit. Einzelvertraglich kann eine gesonderte Übergangsregelung getroffen werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

Für die im T-Systems Trust Center betriebenen Zertifizierungsstellen Shared-Business-CA und Deutsche Telekom Root CA 2 werden die Schlüsselpaare auf einem sicherheitsüberprüften Hardware Security Module (HSM) gespeichert und in sicherer Umgebung abgelegt. Die Speicherung des Schlüsselmaterials auf weiteren HSM erfolgt ausschließlich zur Schlüsselsicherung (back-up) und dient zu Wiederherstellung und Aufrechterhaltung des Dienstes. Eine Schlüsselhinterlegung (Escrow) bei Dritten (z.B. Treuhänder, Notar) ist nicht realisiert.

Eine Schlüsselsicherung von Endteilnehmer- oder Registrator-Zertifikaten liegt im Ermessen des Domänen-Betreibers.

4.12.1 Richtlinien für Schlüsselhinterlegung und –wiederherstellung

Nicht relevant.

4.12.2 Sitzungsschlüsselkapselung und Richtlinien für die Wiederherstellung

Nicht relevant.

5 Gebäude-, Verwaltungs- und Betriebskontrollen

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

5.1 Physikalische Kontrollen

5.1.1 Standort und bauliche Maßnahmen

T-Systems betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Hälften, zwei getrennt arbeitenden Energietrakten (Elektro, Klima, Wasser) mit Gebäudemanagementsystem und Notstromaggregaten sowie einem Verwaltungstrakt besteht.
Die Errichtung und der Betrieb des Trust Centers erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 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 Reinigungspersonal), die Anlieferung von Material (Hardware, Zubehör, Betriebsmittel) und Ordnung am Arbeitsplatz sowie in Rechnerräumen beinhalten.

5.1.2 Räumlicher Zutritt

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

5.1.5 Brandschutz

Die geltenden Brandschutzbestimmungen (z.B. DIN 4102, Auflagen der örtlichen Feuerwehr, Vorschriften über Feuerresistenz, VDE-gerechte Elektroinstallation) werden eingehalten. Alle Brandschutztüren besitzen automatische Schließeinrichtungen. In Absprache mit der Feuerwehr wird nur in äußersten Notfällen mit Wasser gelöscht.
Brandabschnitte sind durch feuerbeständige Bauteile gesichert. Durchgänge durch Brandschutzwände sind mit selbsttätig schließenden Brandschutztüren ausgestattet
In Bereichen mit Doppelböden sowie abgehängten Decken sind Brandschutzwände durchgehend bis zum Geschoßboden bzw. zur Geschoßdecke ausgeführt.
In alle Systemräume, Systemoperatorräume, Archivräume, USV-Räume, sowie weitere ausgewählte Räume, sind Brandfrühesterkennungssysteme (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut.
Die Brandbekämpfung erfolgt mit inertem Gas (lat. für untätig, unbeteiligt, träge).

5.1.6 Aufbewahrung von Datenträgern

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

5.1.7 Entsorgung

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

5.1.8 Externe Sicherung

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

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Vertrauenswürdige Personen sind alle Personen (Mitarbeiter der T-Systems, Mitarbeiter des Domänen-Betreibers, Auftragnehmer, und Berater) mit Zugang zu oder Kontrolle über Authentifizierungs- oder kryptographische Abläufen, die erhebliche Auswirkungen auf Folgendes haben können:

- die Validierung von Informationen in Zertifikatsanträgen,
- die Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatsanträgen, Sperranträgen oder Erneuerungsanträgen,
- die Vergabe oder den Widerruf von Zertifikaten, einschließlich Personal, das Zugang und Zugriff auf die Datenbanksysteme hat,
- den Umgang mit Informationen oder Anträgen von Endteilnehmern.

Vertrauenswürdige Personen sind insbesondere:

- Mitarbeiter des Trust Centers (z.B. Systemadministration),
- Registrierungsmitarbeiter des Domänen-Betreibers,
- Mitarbeiter kryptographischer Abteilungen,
- Sicherheitspersonal,
- zuständiges technisches Personal und

- für die Verwaltung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

Die o.g. vertrauenswürdigen Personen müssen die in dieser Erklärung zum Zertifizierungsbetrieb (CPS) festgelegten Anforderungen (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 und Erklärungen zum Zertifizierungsbetrieb (CPS) der vom T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.2.2 Anzahl involvierter Personen pro Aufgabe

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

Den Systemadministratoren des Trust Centers stehen im Störungsfalle Master- und Sub-Registrator- oder Trust-Center-Operatorrechte zum Zwecke der Störungsbeseitigung zur Verfügung.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

5.2.3.1 Mitarbeiter T-Systems

Mitarbeiter der T-Systems, 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 die SB-CA und andere IT-Systeme erhalten,
- zur Durchführung bestimmter Aufgaben im Zusammenhang mit diesen Systemen zugelassen werden.

5.2.3.2 Mitarbeiter Domänen-Betreiber

Der Domänen-Betreiber muss gewährleisten, dass nur vertrauenswürdige Personen (Master- bzw. Sub-Registratoren) die die Tätigkeiten der Registrierungsstellen wahrnehmen.

5.2.4 Rollen, die eine Funktionstrennung erfordern

Folgende Rollen sollten einer Funktionstrennung unterliegen:

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

5.3 Personelle Maßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

5.3.1.1 Mitarbeiter T-Systems

Für den Betrieb der in Kapitel 1 beschriebenen PKI-Dienstleistungen verlangt T-Systems von seinen Mitarbeitern, die als vertrauenswürdige Personen tätig werden möchten, Nachweise vorzulegen über Qualifizierung und

Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.
In regelmäßigen Abständen, spätestens jedoch nach drei Jahren, ist ein neues Führungszeugnis der T-Systems vorzulegen.

5.3.1.2 Mitarbeiter Domänen-Betreiber

Der Domänen-Betreiber muss gewährleisten, dass das eingesetzte Personal (Master- bzw. Sub-Registratoren) die Registrierungsstellen bedienen kann.

5.3.2 Sicherheitsüberprüfung

5.3.2.1 Mitarbeiter T-Systems

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt T-Systems eine Sicherheitsüberprüfung durch mit folgendem Inhalt durch:

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

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

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

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

Berichte, die solche Informationen enthalten, werden durch Mitarbeiter der Personalabteilung und Sicherheitspersonal bewertet, die das weitere angemessene Vorgehen festlegen. Das weitere Vorgehen kann Maßnahmen bis einschließlich zur Rücknahme des Einstellungsangebots an Anwärter für vertrauenswürdige Positionen führen oder der Kündigung von vertrauenswürdigen Personen beinhalten.
Die Verwendung von in einer Sicherheitsüberprüfung ermittelten Informationen zur Ergreifung solcher Maßnahmen unterliegt geltendem Recht.

5.3.2.2 Mitarbeiter Domänen-Betreiber

Nicht relevant.

5.3.3 Schulungs- und Fortbildungsanforderungen

5.3.3.1 Mitarbeiter T-Systems

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

5.3.3.2 Mitarbeiter Domänen-Betreiber

Nicht relevant.

5.3.4 Nachschulungsintervalle und -anforderungen

5.3.4.1 Mitarbeiter T-Systems

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

5.3.4.2 Mitarbeiter Domänen-Betreiber

Nicht relevant.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

5.3.6 Sanktionen bei unbefugten Handlungen

5.3.6.1 Mitarbeiter T-Systems

Die T-Systems behält sich vor, unbefugter Handlungen oder anderer Verstöße gegen diese Zertifikatsrichtlinien und der daraus abgeleiten Verfahren zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen können Maßnahmen bis einschließlich der Kündigung beinhalten und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.

5.3.6.2 Mitarbeiter Domänen-Betreiber

Die Ahndung etwaige Verstöße obliegt der Zuständigkeit des Domänen-Betreibers.

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 5.3.2.1 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von T-Systems nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.3.8 Dokumentation für das Personal

5.3.8.1 Mitarbeiter T-Systems

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

5.3.8.2 Mitarbeiter Domänen-Betreiber

T-Systems stellt entsprechende Dokumentation zur Verfügung, aus denen die Funktionen und Betrieb der Registrierungsstellen hervorgehen.

5.4 Protokollereignisse

5.4.1 Art der aufgezeichneten Ereignisse

Veränderungen im Lebenszyklus des Schlüssels der Zertifizierungsinstanz Shared-Business-CA werden protokolliert, dies bezieht sich im Einzelnen auf die folgenden Ereignisse:

- Erzeugung
- Speicherung
- Sicherung
- Wiederherstellung
- Archivierung
- Vernichtung
- Änderungen von Hardware und Software
- Zertifikatsauftrag (erfolgreich / fehlgeschlagene Bearbeitung und beiliegende Dokumente)
- Erstellung von Zertifikaten
- Zertifikatssperrung
- Zertifikatserneuerung
- Schlüsselerneuerung
- Zertifikatssperrlisten
- Protokollierung von Internen und Externen Audits

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 ihre Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen der SB-CA.
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 mit Betriebssystemmechanismen 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 (z.B. Angebote, Aufträge),
- Informationen in Zertifikatsanträgen und zum Zertifikatslebenszyklus (z.B. Sperr- und Erneuerungsanträge),
- Soft-PSE, die über Bulk beantragt wurden,
- alle Audit-Daten/Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden,
- zentrale Schlüsselsicherung (key back-up) von Soft-PSE.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen: Fünf (5) Jahre nach Vertragsbeendigung,
- Zertifikatsanträge und andere Informationen zu Lebenszyklen: Fünf (5) Jahre nach Zertifikatssperrung oder Zertifikatsablauf,
- Soft-PSE (Bulk): Fünf (5) Jahre nach Vertragsbeendigung,
- Auditdaten/Logging-Dateien: Zwei (2) Jahre nach Protokollierung des Ereignisses,
- zentrale Schlüsselsicherung: Es werden einzelvertragliche Regelungen getroffen.

5.5.3 Schutz von Archiven

T-Systems garantiert, das nur autorisierte 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.

T-Systems bewahrt die Datenträger auf, die die Archivdaten und die zur Verarbeitung der Archivdaten erforderliche Anwendungen enthalten, um die Archivdaten für den in dieser Erklärung zum Zertifizierungsbetrieb (CSP) festgelegten Archivierungszeitraum zu gewährleisten.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Datensätze wie beispielsweise Zertifikate, Zertifikatssperrlisten, OSCP-Antworten, Loging-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 damit Zugang und Zugriff auf Archivdaten. Bei der Wiederherstellung der Archivdaten werden diese auf Authentizität verifiziert.

5.6 Schlüsselwechsel

Zertifikate verlieren ihre Gültigkeit nach Überschreitung des Gültigkeitszeitraums.
Innerhalb des Gültigkeitszeitraums kann ein Schlüsselwechsel bzw. Zertifikatswechsel erforderlich werden bei

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

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

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

T-Systems informiert unverzüglich alle Domänen-Betreiber vor Integration der neuen CA- und Root-CA-Zertifikate in die entsprechenden Dienste, damit ein reibungsloser Übergang von altem auf neuem Schlüsselpaar möglich wird.

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

5.7 Kompromittierung und Wiederherstellung (Disaster Recovery)

5.7.1 Umgang mit Störungen und Kompromittierungen

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

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

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

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme auf eine Kompromittierung privater Schlüssel von CA- oder Root-CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.
Der Domänen-Betreiber wird über die mögliche Kompromittierung schriftlich 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. Die Generierung neuer Schlüssel und Zertifikate ist gemäß den Arbeitsanweisungen zu dokumentieren und gemäß den Auflagen des jeweiligen Sicherheitskonzepts zu überwachen. Neue Zertifikate und ihre Fingerprints sind zu veröffentlichen (siehe hierzu Kapitel 2.3).

5.7.4 Geschäftskontinuität nach einem Notfall

T-Systems synchronisiert alle Daten zwischen Betriebs- und Sicherungs-Datenbanken (siehe Kapitel 6.2.4). Im Trust Center sind folgenden Datensicherungskopien räumlich abgesichert gelagert und stehen zur Wiederherstellung bereit:

- Vollständige CA-Datenbanken,
- Komplette Schlüsselmaterial der CA- und Root-CA-Zertifikate,
- ggf. Schlüsselsicherung (key back-up) von Soft-PSE von Endteilnehmern.

T-Systems legt im Notfallhandbuch die Verantwortlichkeiten und Prozeduren für Notfälle fest, z.B. für

- die Kompromittierung des CA-Schlüssels,
- die Kompromittierung eines genutzten Algorithmus,
- Ausfall kritischer Hard- und Software-Komponenten,
- Datenverlust,

Das Notfallhandbuch ist ein nicht öffentliches Dokument und kann nach Terminabsprache eingesehen werden.

Darüber hinaus werden in dem Betriebskonzept folgende Aspekte definiert:

- Regelmäßige Datensicherung mit Back Up an sicheren Standorten, Rücksicherung von Daten,
- Zuständige Rollen für Datensicherungen, Back Up und Rücksicherung,

T-Systems hat ein Notfallplan entwickelt, implementiert und getestet, um Katastrophen jeder Art (Naturkatastrophen oder Katastrophen menschlichen Ursprungs) zu mildern. Dieser Plan wird regelmäßig getestet und aktualisiert, um im Falle einer Katastrophe schnellstmöglich eine Wiederherstellung der EDV-Komponenten, Software und Daten zu ermöglichen.

Schlüsselmaterial des Endteilnehmers, das auf Smartcards ausgestellt wurde, steht nicht als Schlüsselsicherung (key back-up) zur Verfügung.

5.8 Einstellung des Betriebes

Eine Betriebsbeendigung kann nur durch T-Systems ausgesprochen werden.
Falls eine Zertifizierungsinstanz der T-Systems den Betrieb einstellen muss, wird ein Beendigungsplan erstellt. Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen,

betroffene nachgeordnete Stellen (Endteilnehmer, vertrauende Dritte, Registrierungsstellen der Domänen-Betreiber und T-Systems) vorab über diese Betriebsbeendigungen zu informieren.
Ein Beendigungsplan kann die folgenden Regelungen enthalten:

- Benachrichtigung der Domänen-Betreiber, Endteilnehmer und Vertrauende Dritte über die geplante Einstellung des Dienstes,
- Fortführung der Sperrfunktionalitäten einschließlich der regelmäßigen Erstellung von Sperrlisten, Abruf der Zertifikatsstatusinformationen und Service Desk-Funktionen,
- Sperrung von ausgegebenen CA-Zertifikaten,
- eventuell erforderliche Übergangsregelungen auf eine Nachfolge-CA,
- je nach Ausgestaltung bestehender Einzelverträge entstehende Kostenerstattung,
- Aufbewahrung der Unterlagen und Archive der Zertifizierungsinstanz (CA).

6 Technische Sicherheitskontrollen

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Alle Schlüsselpaare für CA- und Root-CA-Zertifikaten werden von geschulten und vertrauenswürdigem Fachpersonal generiert in einem abstrahlarmen Raum auf einer evaluierten Hardware Security Modul (HSM) erzeugt und auf einem HSM gespeichert.
Im Fall von CA- und Root-CA-Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem evaluierten HSM (FIPS 140-1/ Level 2 evaluiert) erzeugt und abgelegt.
Alle CA-Schlüsselpaare werden in einer im Voraus geplanten Schlüsselgenerierungsverfahren (Key Generation Ceremony) gemäß den Vorgaben generiert. Die während eines Schlüsselgenerierungsverfahren durchgeführten Aktivitäten werden ordnungsgemäß aufgezeichnet, datiert und von allen beteiligten Personen unterzeichnet. Diese Aufzeichnungen werden zu Audit- und Nachverfolgungszwecken für einen von T-Systems als wirtschaftlich angemessen Zeitraum aufbewahrt.

Die Generierung von Master-Registrator-Zertifikaten erfolgt in der Regel von der Registrierungsstelle T-Systems und unter Verwendung des auf der Smartcard befindlichen Schlüssels.
Den Registrierungsstellen des Domänen-Betreibers steht es offen, für die Generierung von Sub-Registrator-Zertifikaten (oder deren Derivaten, Kapitel 1.3.2.2.2) die auf der Smartcard befindlichen Schlüssel zu verwenden oder die Schlüsselgenerierung des Betriebssystems zu nutzen (Soft-PSE).
Die Generierung der Endteilnehmer-Schlüsselpaare liegt in der Verantwortung des Domänen-Betreibers. Es können die Schlüssel einer Smartcard, die im Betriebssystem oder die über das Bulk-Modul der Shared-Business-CA erzeugten Schlüssel verwendet werden.

6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Die Zustellung von privaten Schlüsseln an Endteilnehmer erfolgt durch den Domänen-Betreiber bzw. davon autorisierten Personen (Master-, Sub-Registrator). Vorpersonalisierte Smartcards sind mit einem PIN-Brief zu versehen. Zum Schutz des privaten Schlüssels ist die Soft-PSE mit einem Passwort zu versehen. Dies gilt auch für Schlüsselmaterial (Soft-PSE), das im Rahmen einer Schlüsselsicherung (key back-up) erzeugt wurde.

Die Versandart obliegt der Verantwortung des Domänen-Betreibers. Der Eingang der Smartcard oder Soft-PSE des Endteilnehmers ist zu protokollieren. Zur Erhöhung der Sicherheit wird ein zeitversetzter Versand über einen kommerziellem Postdienst empfohlen.

Im Falle, dass der Endteilnehmer selbst Schlüsselpaare generiert (Betriebssystems) bzw. nutzt (Smartcard) oder für den Endteilnehmer Schlüssel generiert werden (z.B. Infrastruktur-Komponenten), entfällt die Zustellung von privaten Schlüsseln an den Endteilnehmer.

6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller

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

6.1.4 Zustellung öffentlicher Zertifizierungsstellenschlüssel an Vertrauende Dritte

Das Root-CA-Zertifikat, das für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich ist, wird für alle Endteilnehmer und Vertrauende Dritte durch die Einbettung in die gängigen Zertifikatsspeicher der Betriebssysteme und Anwendungen zur Verfügung gestellt.

Auf den entsprechenden Webseiten für Master-, Sub-Registrator und Benutzer als auch auf dem Verzeichnisdienst stehen die erforderlichen CA- und Root-CA-Zertifikate ebenfalls zum Herunterladen zur Verfügung.

6.1.5 Schlüssellängen

Um nicht Mithilfe der Kryptoanalyse private Schlüssel ermitteln zu können, müssen die Schlüssellängen innerhalb des definierten Verwendungszeitraums über eine ausreichende Länge verfügen. Nach dem aktuellen Stand betragen die RSA-Schlüssellängen der CA- und Root-CA-Zertifikat 2.048 Bit. Abhängig vom Schlüsselmedium finden Endteilnehmer-Zertifikate mit einer RSA-Schlüssellänge von 1.024 Bit bis 2.048 Bit Verwendung.
T-Systems empfiehlt für Endteilnehmer und Registratoren eine ausreichende Schüssellänge von mindestens 1.024 Bit zu verwenden.

6.1.6 Generierung der Parameter von öffentlichen Schlüssel und Qualitätskontrolle

Nicht relevant.

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

Siehe Kapitel 7.1.2.1.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptographischer Module

T-Systems hat physikalischen, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA- und Root-CA-Schlüsseln gewährleisten zu können.

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

6.2.1 Standards und Kontrollen für kryptographische Module

Im Fall von CA und Root-CA-Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem evaluierten HSM (FIPS 140-1/ Level 2 evaluiert) abgelegt. Die Sicherung (back-up) 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, der nur hierfür zuständigen Personen bekannt ist. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

6.2.3 Hinterlegung von privaten Schlüsseln

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

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

6.2.4 Sicherung von privaten Schlüsseln

T-Systems erstellt zu routinemäßigen Wiederherstellungs- und Notfallzwecken Sicherungskopien (back-up) des Schlüsselmaterials des CA- und Root-CA-Zertifikates. Diese Schlüssel werden in verschlüsselter Form innerhalb von kryptographischen Hardware-Modulen (HSM) und zugehörigen Schlüsselspeichergeräten im Trust Center der T-Systems gespeichert. Die für die Speicherung von privaten CA- und Root-CA-Schlüsseln verwendeten kryptographischen Module erfüllen die Anforderungen der vorliegenden Erklärung zum Zertifizierungsbetrieb (CPS).

T-Systems speichert keine Kopien von privaten Schlüsseln der Master-Registratoren. Informationen zur Sicherung von privaten Endteilnehmerschlüsseln sind in den Kapiteln 4.12 ff und 6.2.3 beschrieben.

T-Systems muss Sicherheitsvorkehrungen treffen, dass im Rahmen der Betriebsarbeiten kein Missbrauch mit privaten Schlüsseln stattfindet.

Der Domänen-Betreiber muss Sicherheitsvorkehrungen treffen, dass nur der Endteilnehmer oder autorisiertes Personal (z.B. Sub-Registratoren und Derivate, Kapitel 1.3.2.2.2) Schlüsselmaterial über die Webseiten beantragen, sichern bzw. hoch- und herunterladen können.

Die Wiederherstellung des Schlüsselmaterials von Endteilnehmern ist erlaubt, sofern der Endteilnehmer bzw. Schlüsselverantwortliche der Wiederherstellung zustimmt. Liegt diese Erlaubnis nicht vor, darf der Domänen-Betreiber dennoch die Wiederherstellung durchführen lassen, wenn rechtliche Gründe vorliegen wie

- Anforderungen in einem gerichtlichen oder behördlichen Verfahren,
- im Rahmen polizeilicher Ermittlungen,
- gesetzliche oder staatliche Vorschriften,
- Organisationsrichtlinien des Domänen-Betreibers.

6.2.4.1 Sicherung und Wiederherstellung des Verschlüsselungsschlüssels durch Enrollment-Software

Der Sub-Registrator kann bei der Personalisierung der Smartcard durch Verwendung geeigneter Enrollment-Software die passwortgeschützte Soft-PSE (privater Schlüsselverschlüsselungsschlüssel inkl. Verschlüsselungs-Zertifikat) als auch die korrespondierende Passwortdatei (enthält das Passwort der Soft-PSE) verschlüsselt abspeichern.
Zur Einhaltung des 4-Augen-Prinzips sollte die Soft-PSE und die Passwortdatei getrennt auf dedizierte Zertifikate verschlüsselt werden, die ausschließlich im Sicherung- und Wiederherstellungsprozess Verwendung finden.
Es empfiehlt sich die Soft-PSE auf Zertifikat Nr. 1 und die Passwortdatei auf Zertifikat Nr. 2 zu verschlüsseln. Zur Wiederherstellung ist die Passwortdatei mit dem privaten Schlüssel des Zertifikat Nr. 2 zu entschlüsseln. Danach erfolgt die Entschlüsselung der Soft-PSE mit Zertifikat Nr. 1. Die Soft-PSE ist erst in den Zertifikatsspeicher importierbar nach Eingabe des Passworts.

6.2.4.2 Sicherung und Wiederherstellung von Soft-PSE über das Betriebssystem

Bei der Sicherung von Soft-PSEn kann das Schlüsselmaterial über das Betriebssystem (Zertifikatsspeicher) exportiert und verschlüsselt beim Domänen-Betreiber gespeichert werden. Der Domänen-Betreiber wählt ein Speichermedium aus, das seinen Ansprüchen entspricht.

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

6.2.4.3 Sicherung und Wiederherstellung von Soft-PSE durch die Bulk-Funktion

Schlüsselmaterialien und Passwortdateien, die per Bulk-Funktion generiert wurden, verbleibt verschlüsselt abgespeichert im Trust Center der T-Systems. Der Sub-Registrator kann diese auch herunterladen.

Der Sub-Registrator authentisiert sich mittels Zertifikat an der Webseite (SSL-Client-Authentifikation). Unter Eingabe der Bearbeitungsnummer (Bulk-ID) steht die Soft-PSE als auch Passwort zum Herunterladen zur Verfügung.

6.2.4.4 Sicherung und Wiederherstellung von Soft-PSE durch Trust Center

Bei einer auf die Master-Domäne konfigurierte „Zentrale Schlüsselsicherung“ sind die passwortgeschützte Soft-PSE und die korrespondierende Passwortdatei (enthält das Passwort der Soft-PSE) getrennt verschlüsselt im Trust Center der T-Systems gespeichert. Das Hochladen der Dateine erfolgt durch den Sub-Registrator. Zur Einhaltung des 4-Augen-Prinzips stehen zusätzlich die Rollen Sub-RA-P12 Operator und Sub-RA-Pwd Operator (siehe auch Kapitel 1.3.2.2.2) zur Verfügung, die Authentifizierung an der Webseite erfolgt mittels Zertifikate. Unter Eingabe der Suchkriterien steht die Soft-PSE als auch korrespondierende Passwortdatei den entsprechenden Rolleninhabern zum Herunterladen zur Verfügung.

6.2.5 Archivierung privater Schlüssel

Wenn der CA-, Root-CA- oder OCSP-Schlüssel das Ende seiner Gültigkeitsdauer erreicht hat, wird dieser vernichtet.

T-Systems archiviert keine Kopien von Schlüsselmaterial von Endteilnehmern. Eine Ausnahme bildet die automatisierte Massengenerierung (Bulk siehe Kapitel 3.2.3.1.3 bis 3.2.3.1.5) und kundenindividuelle Schlüsselsicherung (key back-up). Letzterer Funktion wird einzelvertraglich geregelt.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptographischen Modul

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

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

6.2.7 Speicherung privater Schlüssel auf kryptographischen Modulen

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

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

6.2.8 Methode zur Aktivierung privater Schlüssel

Alle Endteilnehmer, Registratoren, Administratoren und Operatoren müssen die Aktivierungsdaten (z.B. PIN, Importpasswort) für ihren privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß der vorliegenden Erklärung zum Zertifizierungsbetrieb schützen.

6.2.8.1 Endteilnehmer- und Sub-Registrator-Zertifikate (und deren Derivate)

Der Endteilnehmer und Sub-Registrator (und deren Derivate, Kapitel 1.3.2.2.2)) hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer ähnlichen Sicherheitsmaßnahme, um den Endteilnehmer bzw. Sub-Registrator vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann auch z.B. ein Passwort zum Betrieb des privaten Schlüssels, beinhalten. Eine Ausnahme bilden Infrastruktur-Komponenten, die selbst nicht wie beispielsweise eine natürliche Person ein Passwort eingeben kann.
- Ergreifung wirtschaftlich angemessene Maßnahmen zum physikalischen Schutz des Arbeitsplatzes, Registrator-Arbeitsplatzes oder Infrastruktur-Komponente, um die Nutzung des Platzes/Komponente und sein zugehörigen privaten Schlüssel ohne Genehmigung des Registrators, Endteilnehmers oder autorisierten Person zuverlässig zu verhindern.

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

6.2.8.2 Master-Registrator-Zertifikate

Der Master-Registrator hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Verwendung einer Smartcard und Festlegung einer PIN gemäß Kapitel 6.4.1 oder Integration eine ähnliche Sicherheitsmaßnahme, um den Master-Registrator vor der Aktivierung des privaten Schlüssels zu authentifizieren.
- Ergreifung wirtschaftlich angemessene Maßnahmen zum physikalischen Schutz des Registrator-Arbeitsplatzes, um die Nutzung des Platzes und seins zugehörigen privaten Schlüssel ohne Genehmigung des Master-Registrator zuverlässig zu verhindern.

6.2.8.3 Administrator- und Operator-Zertifikate

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 auch z.B. ein Passwort zum Betrieb des privaten Schlüssels, ein Windows Anmelde- oder Bildschirmschonerpasswort, ein Anmeldepasswort für das Netzwerk beinhalten.
- Ergreifung geeigneter Maßnahmen zum physikalischen Schutz des Administrator- oder Operator-Arbeitsplatzes vor unberechtigtem Zugriff.

6.2.8.4 CA- und Root-CA-Zertifikate

Schlüsselmaterial für CA- und Root-CA-Zertifikate wird entsprechend durch die autorisierten Personen aktiviert und auf kryptographischen Hardware-Modulen (HSM) aufgebracht (Kapitel 6.2.2 und 6.4.1).
Der zum CA-Zertifikat gehörende private Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt (Kapitel 4.9.3.4.1).
Der zum Root-CA-Zertifikat gehörende private Schlüssel wird nur zur Erzeugung von weiteren CA-Zertifikaten aktiviert. Nach Ablauf des Root-CA-Zertifikats oder Sperrung (Kapitel 4.9.3.4.3) ist der private Schlüssel nicht mehr nutzbar.

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

6.2.9 Methode zur Deaktivierung privater Schlüssel

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

Die Deaktivierung von privaten Schlüsseln (Endteilnehmer, Registratoren) obliegt dem Domänen-Betreiber.

Eine Deaktivierung von privaten Schlüsseln, die im Rahmen einer zentralen Schlüsselsicherung (key back-up) erstellt wurden, bedarf einer einzelvertraglichen Regelung.

6.2.10 Methode zur Vernichtung privater Schlüssel

Wenn CA- oder Root-CA-Schlüssel das Ende ihrer Gültigkeitsdauer erreicht haben, werden die Schlüssel, wie in Kapitel 6.2.5 beschrieben, auf sicherem Wege vernichtet.
Die Vernichtung von CA- und Root-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.
T-Systems verwendet zur sicheren Schlüsselvernichtung eine integrierte Löschfunktion des HSM.

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

6.2.11 Bewertung kryptographischer Module

Siehe Kapitel 6.2.1.

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

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

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

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

In Tabelle 5 sind die maximalen Gültigkeitszeiträume der in der Hierarchie beteiligten Zertifikate dargestellt, die zum Zeitpunkt des Inkrafttretens dieser Erklärung zum Zertifizierungsbetrieb ausgestellt wurden.
T-Systems stellt sicher, dass die CA- und Root-CA-Zertifikate vor Ablauf ausgewechselt werden, um die entsprechende Zertifikatsgültigkeit von Endteilnehmer-Zertifikaten gewährleisten zu können.

Zertifikatstyp:	Gültigkeitsdauer:
Deutsche Telekom Root CA2	20 Jahre
Shared-Business-CA	Mind. 8 Jahre
Alle Endteilnehmer-Zertifikate (Master- und Sub-Registrator, natürliche und juristische Personen, Personen- und Funktionsgruppen, Infrastruktur-Komponenten)	Standardmäßig 12, 24 oder 36 Monate (bzw. 1, 2 oder 3 Jahre), nach Vereinbarung kann eine abweichende Laufzeit von n Monate [3] administriert werden

Tabelle 5: Gültigkeit von Zertifikaten

Eine Erneuerung von Endteilnehmer-Zertifikaten durch den Inhaber bzw. autorisierten Person ist möglich.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

6.4.1.1 T-Systems

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

6.4.1.2 Domänen-Betreiber

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

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

6.4.2 Schutz von Aktivierungsdaten

6.4.2.1 T-Systems

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

6.4.2.2 Domänen-Betreiber

Die Durchsetzung des Schutzes nach Kapitel 6.4.1 obliegt der Verantwortung des Domänen-Betreibers. T-Systems empfiehlt dringend, die Registratorzertifikate auf Smartcard aufzubringen oder unter Verwendung einer hohen Stufe in den Sicherheitseinstellungen ihres Browsers in verschlüsselter Form als Soft-PSE aufzubewahren

[3] Die Zertifikatsgültigkeit wird bei der Einrichtung der Master-Domäne festgelegt und vererbt sich auch auf die Zuständigkeitsbereiche (Sub-Domänen). Innerhalb der Master-Domäne sind bei gleicher Namensgebung keine unterschiedlichen Gültigkeitszeiträume möglich.

und mit einer schwierigen Kennphrase zu schützen. Der Domänen-Betreiber sollte sich bei den Endteilnehmern eine schriftliche Bestätigung mit dem Umgang der Aktivierungsdaten einholen.
Zur Erhöhung der Sicherheit empfiehlt T-Systems die die regelmäßige Änderung von Kennphrase und PIN der Endteilnehmer-Zertifikate.

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

6.4.3.2 Vernichtung von Aktivierungsdaten

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

6.5 Computer-Sicherheitskontrollen

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

Für die Master- und Sub-Registratoren erhält der Domänen-Betreiber vertrauenswürdige und geeignete Komponenten zur Bedienung der Registrator-Funktionalitäten.

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

6.5.1.1 T-Systems

T-Systems stellt sicher, das 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 und geschultes Betriebspersonal beschränkt.

6.5.1.2 Domänen-Betreiber

T-Systems empfiehlt die Verwendung von Kennwörtern wie in Kapitel 6.4.1 beschrieben.

6.5.2 Bewertung der Computersicherheit

Im Rahmen des Sicherheitskonzeptes, welches sich am Signaturgesetz orientiert, wurden unterschiedliche Bedrohungsanalysen durchgeführt, die die Wirksamkeit aller getroffenen Maßnahmen untersucht.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Systementwicklungskontrollen

T-Systems stellt dem Domänen-Betreiber Infrastrukturkomponenten (Hard- und Software) für Registrator-Arbeitsplätze zur Verfügung, die den Vorgaben der T-Systems entwickelt wurden und der Pflege und Weiterentwicklung unterliegen.

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 für den Dienst Shared-Business-CA implementiert:

- Die Netzwerke des Zertifizierungsdienstes sind durch Firewalls vom Internet getrennt und beschränken den Datenverkehr auf das für die Funktionen notwendige Maß.
- Sicherheitskritische Komponenten und Systeme, die vom Internet aus erreichbar sind (z.B. Verzeichnisdienst, OCSP-Responder), werden durch Firewalls von Internet und den internen Netzen getrennt. Alle anderen sicherheitskritischen Komponenten und Systeme (z.B. CA, DB, Signer) befinden sich in separaten Netz.
- Die internen Netzwerke des Zertifizierungsdienstes sind nach dem Schutzbedarf der Systeme und Komponenten aufgeteilt und untereinander durch Firewalls getrennt.

6.8 Zeitstempel

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

7 Zertifikats-, Sperrlisten- und OCSP-Profile

7.1 Zertifikatsprofil

Die Zertifikatsbeantragung (siehe Kapitel 4.1 ff) erfolgt entweder in Form eines Papierantrages an den zuständigen Sub-Registrator, über eine Webseite (Sub-Registrator, Benutzer) oder technischen Schnittstellen (SCEP- oder Mail-Schnittstelle).
Bedingt durch das Beantragungsverfahren bzw. Schnittstelle wird ein Zertifikatsantrag bereits einem entsprechenden Zertifikatsprofil (z.B. Server, Router) zugeordnet. Ein Zertifikatsantrag (Request), der aus einer Infrastrukturkomponente oder Anwendung stammt, wird auf definierte Inhalte des Subject-DN (siehe Kapitel 3.1.1 ff) und Verwendung unerlaubter Zeichen überprüft. Vorbelegte Inhalte der Attribute Organizational Unit Name 1 und 2 (Kapitel 3.1.1.4 und 3.1.1.5) werden immer mit der Zertifikatsgenehmigung bzw. –ausstellung durch die dem zuständigen Sub-Registrator zugeordneten Einträge überschrieben.
Inhalte, die über den Subject-DN hinausgehen (z.B. Schlüsselverwendung, erweiterte Schlüsselverwendung), werden ohne Benachrichtigung oder Hinweis ignoriert. Es gilt die Ausprägung des jeweilige Zertifikatsprofil wie in Kapitel 7.1 ff beschrieben.
Die Verwendung von unerlaubten Zeichen wird mit der Überprüfung angezeigt oder dem Antragsteller per E-Mail mitgeteilt.

Die von T-Systems ausgestellten Zertifikate entsprechen folgenden Anforderungen:

- **[RFC 5280]** Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- **[X.509]** Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)

X.509.v3-Zertifikate müssen mindestens die in Tabelle 6 aufgeführten Inhalte aufweisen.

Feld:	Wert oder Wertbeschränkung:
Version:	Zertifikatsversion (Kapitel 7.1.1)
Seriennummer:	Eindeutiger Wert
Signaturalgorithmus:	RSA – SHA-1 (alternativ RSA-SHA-256)
Aussteller:	Shared-Business-CA (Kapitel 7.1.4)
Gültig ab:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Gültig bis:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Antragsteller:	Eindeutiger Name (Kapitel 7.1.4)
Öffentlicher Schlüssel:	Gemäß RFC 5280 kodiert
Erweiterungen:	
Schlüsselverwendung:	Kapitel 7.1.2.1
Zertifikatsrichtlinie:	Kapitel 7.1.2.2
Alternativer Antragstellername:	Kapitel 7.1.2.3
Basiseinschränkungen:	Kapitel 7.1.2.4
Erweiterte Schlüsselverwendung:	Kapitel 7.1.2.5
Sperrlistenverteilungspunkt:	Kapitel 7.1.2.6
Schlüsselkennung:	Kapitel 7.1.2.8
Schlüsselkennung des Antragstellers:	Kapitel 7.1.2.7

Zugriff auf Stelleninformation	Kapitel 7.1.2.9
Zertifikatsvorlagename	Kapitel 7.1.2.10

Tabelle 6: Zertifikatsattribute nach X509.v3

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

7.1.1 Versionsnummer(n)

Die von der Shared-Business-CA ausgestellten X.509-Zertifikate für Endteilnehmer entsprechen der z. Zt aktuellen Version 3. Die zusätzlichen Erweiterungen und Eigenschaften werden in den folgenden Kapiteln ausführlicher erklärt.
Die CA- und Root-CA-Zertifikate sind ebenfalls vom Typ X.509v3.

7.1.2 Zertifikatserweiterungen

Um dem Standard X.509v3 zu erfüllen, ergänzt T-Systems das Zertifikatsprofil um entsprechende Erweiterungen, die in den Kapiteln 7.1.2.1 bis 7.1.2.10 beschrieben sind.
Es können vom Domänen-Betreiber selbst keine zusätzlichen Erweiterungen im Zertifikatsprofil aufgenommen werden.

7.1.2.1 Erweiterung „Schlüsselverwendung (KeyUsage)"

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

In Tabelle 7 bis Tabelle 9 ist die Schlüsselverwendung „Schlüsselverwendung" den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

		Infrastruktur-Komponenten:				Registrator-Zertifikate:	
	Zertifikatsprofil:	Server	Router /Mail-Gateway	Gateway	Domain-Controller	Master-Registrator	Sub-Registrator
	Risikowert (Criticality)	critical	critical	critical	critical	critical	critical
Bit	Bezeichnung	Sig/Enc	Sig/Enc	Sig/Enc	Sig/Enc	Sig/Enc	Sig/Enc
0	digitalSignature	✓	✓	✓	✓	✓	✓
1	nonRepudation	×	×	×	×	×	×
2	keyEncipherment	✓	✓	✓	✓	✓	✓
3	dataEncipherment	×	×	×	✓	×	×
4	keyAgreement	×	×	×	×	×	×
5	keyCertSign	×	×	×	×	×	×
6	CRLSign	×	×	×	×	×	×
7	encipherOnly	×	×	×	×	×	×
8	decipherOnly	×	×	×	×	×	×
	Wert (Hex)	A0	A0	A0	B0	A0	A0

Tabelle 7: Zuordnung der Erweiterung „Schlüsselverwendung", Teil 1

		Benutzer-Zertifikate (natürliche Personen, Personen- und Funktionsgruppen, juristische Personen):					
		Single-Key	Dual-Key		Triple-Key		
	Risikowert (Criticality)	critical	critical	critical	critical	critical	critical
Bit	Bezeichnung	Sig/Enc	Sig	Enc	Sig	Enc	LogOn
0	digitalSignature	✓	✓	×	✓	×	✓
1	nonRepudation	×	×	×	×	×	×
2	keyEncipherment	✓	×	✓	×	✓	✓
3	dataEncipherment	×	×	×	×	×	×
4	keyAgreement	×	×	×	×	×	×
5	keyCertSign	×	×	×	×	×	×
6	CRLSign	×	×	×	×	×	×
7	encipherOnly	×	×	×	×	×	×
8	decipherOnly	×	×	×	×	×	×
	Wert (Hex)	A0	80	20	80	20	A0

Tabelle 8: Zuordnung der Erweiterung „Schlüsselverwendung“, Teil 2

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

Tabelle 9: Zuordnung der Erweiterung „Schlüsselverwendung“, Teil 3

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

Obwohl das nonRepudiation-Bit in der Erweiterung „Schlüsselverwendung“ nicht gesetzt ist, unterstützt T-Systems dennoch die Nichtabstreitbarkeit für diese „fortgeschrittenen“ Signatur-Zertifikate. Es ist z. Zt. nicht unbedingt erforderlich, das nonRepudiation-Bit in diesem Zertifikatstyp zu setzen, da die PKI-Industrie noch keinen Konsens darüber erzielt hat, welche Bedeutung das nonRepudiation-Bit tatsächlich hat. Bis ein solcher Konsens erzielt wird, hat das nonRepudiation-Bit für potenzielle Vertrauende Dritte keine Bedeutung.
Diese Aussage gilt nicht für „qualifizierte“ Signatur-Zertifikate.
Darüber hinaus werten die gängigsten Anwendungen (z.B. E-Mail) das nonRepudiation-Bit nicht. Aus diesem Grunde ist eine Definition des Bits für Vertrauende Dritte bei der Entscheidung über die Vertrauenswürdigkeit nicht hilfreich.

7.1.2.2 Erweiterung „Zertifizierungsrichtlinien (Certificate Policies)"

Die Erweiterung „Zertifikatsrichtlinie" besteht aus einem Objekt-Kennungen (Object Identifier, OID, siehe auch Kapitel 7.1.6) und einer URL, hinter der diese Erklärung zum Zertifizierungsbetrieb abrufbar ist. Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.1.2.3 Erweiterung „alternativer Antragstellername (subjectAltName)"

In Tabelle 10 ist die Erweiterung „alternativer Antragstellernamen" den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Zertifikatsprofil:	Benutzer-Zertifikat:			Server-Zertifikat:	Router / Gateway-Zertifikat:	Mail-Gateway-Zertifikat:	Domain-Controller-Zertifikat:	Master-Registrator-Zertifikat:	Sub-Registrator-Zertifikat:
Erweiterung:	SK	DK	TK						
RFC822-Name	✓	✓	✓	✗	✓	✓	✓	✗	✗
Principalname	opt.	opt.	✓	✗	✗	✗	✗	✗	✗
DNS-Name	✗	✗	✗	✓	✗	✗	✓	✗	✗
IP-Address	✗	✗	✗	✗	✓	✗	✗	✗	✗
Other Name 1.3.6.1.4.1.311.25.1	✗	✗	✗	✗	✗	✗	✓	✗	✗

Tabelle 10: Zuordnung der Erweiterung „alternativer Antragstellername"

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.1.2.4 Erweiterung „Basiseinschränkungen (BasicConstraints)"

Die Erweiterung „grundlegende Beschränkung" definiert den Zertifikatstyp (Endteilnehmer, CA- und Root-CA) und die Beschränkung der Zertifizierungspfades (pathLenConstraint).

Bei Endteilnehmer-Zertifikate ist der Benutzertyp „Endeinheit" gesetzt, die Pfadlänge ist nicht gesetzt. Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

Das CA-Zertifikat enthält den Benutzertyp „Zertifizierungsstelle" mit der Pfadlänge „1". Der Risikowert dieser Erweiterung ist als „kritisch" gesetzt.

Das Root-CA-Zertifikat enthält den Benutzertyp „Zertifizierungsstelle" mit der Pfadlänge „5". Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.1.2.5 Erweiterung „Erweiterte Schlüsselverwendung (ExtendedKeyUsage)"

In Tabelle 11 sind die Erweiterten Schlüsselverwendungen den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

	Single-Key	Dual-Key		Triple-Key			Domain-Controller
Risikowert (Criticality)	n.v.	n.v.	n.v.	n.v.	n.v.	critical	critical
Bezeichnung	Sig/Enc	Sig	Enc	Sig	Enc	LogOn	Sig/Enc/DataEnc
Secure E-Mail (1.3.6.1.5.5.7.3.4)	✗	✗	✗	✗	✗	✗	✗

Code Signing (1.3.6.1.5.5.7.3.3)	✗	✗	✗	✗	✗	✗	✗
Server authentication (1.3.6.1.5.5.7.3.1)	✗	✗	✗	✗	✗	✗	✓
Timestamping (1.3.6.1.5.5.7.3.8)	✗	✗	✗	✗	✗	✗	✗
Client authentication (1.3.6.1.5.5.7.3.2)	✗	✗	✗	✗	✗	✓	✓
OCSPSigning (1.3.6.1.5.5.7.3.9)	✗	✗	✗	✗	✗	✗	✗
MS SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	✗	✗	✗	✗	✗	✓	✗

Tabelle 11: Zuordnung der Erweiterung „Erweitere Schlüsselverwendung“

7.1.2.6 Erweiterung „Sperrlistenverteilungspunkt (CRLDistributionPoints)”

Alle Endteilnehmer-Zertifikate verfügen über einen Sperrlistenverteilungspunkt, über dessen URL (HTTP und LDAP) die aktuelle Zertifikatssperrliste (CRL) auf dem Verzeichnisdienst abrufbar ist. Vertrauende Dritte benötigen diese URL zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Das CA-Zertifikat verfügt ebenfalls über einen Sperrlistenverteilungspunkt, über dessen URL (HTTP und LDAP) die aktuelle Sperrliste für Zertifizierungsstellen (ARL) auf dem Verzeichnisdienst abrufbar ist. Vertrauende Dritte benötigen diese zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Das Root-CA-Zertifikat enthält keinen Sperrlistenverteilungspunkt.

7.1.2.7 Erweiterung „Schlüsselkennung des Antragstellers (subjectKeyIdentifier)”

In allen Endteilnehmer- und Registrator-Zertifikaten enthält die Erweiterung „Schlüsselkennung des Antragstellers“ als Attributswert SHA-1 Hashwert, der individuell aus den jeweiligen öffentlichen Schlüssel gebildet wird.

Die Erweiterung „Schlüsselkennung des Antragstellers“ des Shared-Business-CA-Zertifikats enthält als Attributswert einen SHA-1 Hashwert, der aus dem öffentlichen Schlüssel der Shared-Business-CA gebildet wird. Dieser Wert stimmt mathematisch mit dem Wert der Erweiterung „Stellenschlüsselkennung“ (siehe Kapitel 7.1.2.8) des Endteilnehmer- und Registrator-Zertifikats überein.
Es gelten die Regelungen auch für die hierarchisch übergeordnete Zertifizierungsinstanz.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.8 Erweiterung „Stellenschlüsselkennung (authorityKeyIdentifier)”

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

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.9 Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)"

In Endteilnehmer- und Registrierungsstellenmitarbeiter-Zertifikaten enthält die Erweiterung „Zugriff auf Stelleninformation" die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch HTTP-URL des OCSP-Responders.

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.1.2.10 Erweiterung „Zertifikatsvorlagenname (Certificate Template Name)"

Für das Zertifikatsprofil „Domain-Controller" ist die Erweiterung „Zertifikatsvorlagenamen" belegt mit dem Namen „DomainController".

7.1.3 Objekt-Kennungen (OIDs) - von Algorithmen

Das Zertifikat der Wurzelinstanz (Root-CA) und Shared-Business-CA (Sub-CA) wurde unter Verwendung des folgenden Algorithmus signiert:
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}, -> 1.2.840.113549.1.1.5

Mit der Einrichtung der Betreiber-Domäne erfolgt die Festlegung, ob Zertifikate für Endteilnehmer und Registrierungsmitarbeiter mit SHA-1 oder SHA-256 signiert werden.
Folgende Signatur-Algorithmen stehen für diese Zertifikatsinhaber zur Verfügung:

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}, -> 1.2.840.113549.1.1.5
- sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}, -> 1.2.840.113549.1.1.11

7.1.4 Namensformen

Die Endteilnehmer- und Registrator-Zertifikate der Shared-Business-CA enthalten einen, für diesen Service, eindeutigen Ausstellernamen (Issuer-DN).

Die Inhalte des Subject-DN (Antragsteller) sind abhängig vom Zertifikatstyp (z.B. Benutzer, Server, Router/Gateway) und setzen sich wahlweise aus den Feldern wie in den Kapiteln 3.1.1.2 bis 3.1.1.11 beschrieben zusammen. Die Felder enthalten Pflichtangaben (mandatory), optionale oder automatisch erzeugte Angaben.
Pflichtangaben enthalten folgende Felder:

- Country Name (C)
- Organization Name (O)
- Common Name (CN)
- Mail-Address

Vom System werden folgende Felder automatisch erzeugt:

- Organizational Unit Name 1 (OU1)
- Organizational Unit Name 2 (OU2)
- Serial Number (SN)

Folgende Felder sind optional:

- Organizational Unit Name 3 (OU3)
- User Principal Name (UPN)
- Fully Qualified Domain Name (FQDN)

Sofern nicht alle Zertifikatsantragsdaten in den Subject-DN aufgenommen werden können, weil technische oder Interoperabilitätsbeschränkungen (z.B. Dateigröße des Zertifikats, nur ein OU-Eintrag) in Zertifikaten die Verwendung unmöglich machen, sind Abweichungen zu den vorangehenden Bestimmungen zulässig.
Die Mail-Adresse muss nicht zwingen Inhalt des Subject-DN sein, wenn sich diese in der Erweiterung „alternativer Antragstellername (subjectAltName) wieder findet.

7.1.5 Namensbeschränkungen

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

7.1.6 Objekt-Kennungen (OIDs) für Zertifizierungsrichtlinien

Alle Endteilnehmer- und Registrator-Zertifikate als auch das CA-Zertifikat enthalten eine Erweiterung „Zertifikatsrichtlinien (certificate policies)“. Neben der HTTP-URL findet sich folgende Objekt-Kennung für die Erklärung zum Zertifizierungsbetrieb:
policy OBJECT IDENTIFIER ::= {iso(1) iso identified organization(3) us department of defence(6) oid assignments(1) private(4) iana registrated private enterprises(1) T-TeleSec(7879) policy identifier(13) shared-business-ca(25) } -> 1.3.6.1.4.1.7879.13.25

7.1.7 Verwendung der Erweiterung „Richtlinienbeschränkungen (Policy Constraints)”

Keine Bestimmungen.

7.1.8 Syntax und Semantik von Richtlinienkennungen

Es wird auf Kapitel 7.1.2.2 verwiesen.

7.1.9 Verarbeitungssemantik der kritische Erweiterung „Zertifikats-Richtlinien (critical Certificate Policies)”

Keine Bestimmungen.

7.2 Sperrlistenprofil

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)

Zertifikatssperrlisten müssen mindestens die in Tabelle 12 aufgeführten Inhalte aufweisen.

Feld:	Wert oder Wertbeschränkung:
Version:	Sperrlistenversion (Kapitel 7.2.1)
Aussteller:	Shared-Business-CA (siehe Kapitel 7.1.4)
Gültig ab:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Nächste Aktualisierung:	Datum und Uhrzeit der nächsten geplanten Veröffentlichung.
Signaturalgorithmus:	RSA – SHA-1 (alternativ RSA-SHA-256)

Gesperrte Zertifikate:	Liste der gesperrten Zertifikate inkl. Seriennummer mit Sperrdatum- und zeitpunkt des gesperrten Zertifikats.
Erweiterungen:	
Stellenschlüsselkennung:	Es gelten die Regelungengemäß Kapitel 7.2.2.1).
Sperrlistennummer:	Eindeutiger Wert (Kapitel 7.2.2.2)
Sperrgrund:	Kodierung des Sperrgrunds nach RFC 5280 (Kapitel 7.2.2.3).

Tabelle 12: Sperrlistenattribute nach X509.v2

7.2.1 Versionsnummer(n)

Die von der Shared-Business-CA ausgestellten X.509-Zertifikatssperrlisten entsprechen der Version 2.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

7.2.2.1 Erweiterung „Stellenschlüsselkennung (authorityKeyIdentifier)"

Die Sperrlisten enthalten die Erweiterung „Stellenschlüsselkennung" wie in Kapitel 7.1.2.8 beschrieben.

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.2.2.2 Erweiterung „Sperrlistennummer"

Die Sperrlisten enthalten die Erweiterung „Sperrlistennummer" als fortlaufende Seriennummer der Sperrliste.

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.2.2.3 Erweiterung „Sperrgrund"

Bei der Sperrung von Zertifikaten muss zwingend ein Sperrgrund angegeben werden. Nach Tabelle 13 sind folgende Sperrgründe implementiert:

Eingabewert auf Webseite:	Sperrgründe nach RFC 5280:	Wert des Sperrgrundes nach RFC 5280:
Nicht spezifiziert	Nicht angegeben (unspecified)	0
Schlüssel kompromittiert	Schlüsselkompromiss (keyCompromise)	1
Angaben im Zertifikat nicht mehr aktuell	Zuordnung geändert (affiliationChanged)	3
Zertifikat nach Erneuerung gesperrt	Abgelöst (superseded)	4

Tabelle 13: Erweiterung „Sperrgrund"

Der Risikowert dieser Erweiterung ist als „unkritisch" gesetzt.

7.3 OCSP-Profil

OCSP (Online Certificate Status Protocol) stellt auf gleichnamigen Protokoll einen Validierungsdienst zur Verfügung, mit dessen Hilfe dem Vertrauende Dritten eine zeitgerechte Information zum Sperrstatus von Endteilnehmer-Zertifikaten übermittelt wird.

Das OCSP-Zertifikat, ausgestellt von T-Systems durch Shared-Business-CA, enthält das Attribut „Erweiterter Schlüsselverwendung“ mit der OID „1.3.6.1.5.5.7.3.9“ (OCSP noCheck), d.h. das OCSP-Zertifikat wird nicht validiert.

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

7.3.1 Versionsnummer(n)

Es wird die Version 1 gemäß der OCSP-Spezifikation nach RFC 2560 unterstützt.

7.3.2 OCSP-Erweiterungen

T-Systems bietet keine OCSP-Erweiterungen an.

8 Compliance-Audits und andere Prüfungen

Die bei dem Domänen-Betreiber installierten Registrierungsstellen werden nicht grundsätzlich im Rahmen von Compliance-Audits von T-Systems überprüft, es sei denn, der Domänen-Betreiber verlangt dies.

Auf Grundlage dieser Erklärung zum Zertifizierungsbetrieb kann T-Systems jedoch berechtigt sein, nach Bedarf Trust-Center-spezifische Compliance-Audits durchzuführen, um die Vertrauenswürdigkeit der Shared-Business-CA Master-Domäne(n) sicherzustellen. Dies umfasst folgendes:

- T-Systems ist berechtigt, bei einem Domänen-Betreiber jederzeit nach alleinigem und ausschließlichem Ermessen ein „Audit (Untersuchung)“ durchzuführen, falls T-Systems Grund zu der Annahme hat, dass die überprüfte Stelle Regelungen (insbesondere diese Erklärung zum Zertifizierungsbetrieb) und/oder Standards nicht erfüllt hat, bei der Stelle eine Störung oder Kompromittierung stattgefunden hat oder die Stelle eine Handlung begangen oder unterlassen hat, die dazu führte, dass die Störung, die Kompromittierung, die Handlung, der überprüften Stelle eine tatsächliche oder potenzielle Bedrohung der Sicherheit oder Integrität von Service Shared-Business-CA darstellt. Dieses Audit ist auch durchzuführen wenn Verdachtsmomente für Missbrauch des PKI-Dienstes bestehen oder eine Schädigung des Ansehens der T-Systems zu erwarten ist.
- T-Systems ist berechtigt, bei einem Domänen-Betreiber „Ergänzende Risikomanagementüberprüfungen“ aufgrund unvollständiger oder außergewöhnlicher Ergebnisse eines Compliance-Audit oder als Teil des Gesamt-Risikomanagementprozesses im Rahmen der ordentlichen Geschäftstätigkeit durchzuführen.

Die Stellen, die einem Audit, einer Überprüfung oder einer Untersuchung unterzogen werden, müssen T-Systems und/oder einem Beauftragten unterstützen und zusammenarbeiten, damit umgehend zur Aufklärung des untersuchten Falles beigetragen werden kann.
Weiterhin kann T-Systems vertraglich berechtigt sein, die Durchführung dieser Audits, Überprüfungen und Untersuchungen auf Dritte (Kapitel 8.2) zu übertragen.

8.1 Intervall und Gründe von Prüfungen

Unter Berücksichtigung Ausführungen des Kapitel 8 können Trust-Center-spezifische Compliance-Audits nach Bedarf stattfinden und werden auf Kosten der überprüften Stelle durchgeführt. Der Beginn dieser Maßnahme ist mindestens eine Woche vorher schriftlich anzukündigen.

8.2 Identität/Qualifikation des Prüfers

Die Trust-Center-spezifischen Compliance-Audits werden von qualifizierten Mitarbeitern der T-Systems oder einem Dritten (z.B. qualifiziertes Unternehmen wie TÜV IT) durchgeführt, die Erfahrung in den Bereichen Public-Key-Infrastructure-Technologie, Sicherheits-Auditing und Verfahren und Hilfsmittel der Informationssicherheit vorweisen können.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer handelt es sich um einen Mitarbeiter der T-Systems oder von einem T-Systems unabhängigen Dritten.

8.4 Abgedeckte Bereiche der Prüfung

Den Umfang der Prüfung legt der Prüfer selbst fest. Zielsetzung der Überprüfung ist die Umsetzung dieser Erklärung zum Zertifizierungsbetrieb. Hier sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung.

- Ausstellung von Sub-Registrator-Zertifikaten und deren Derivate,
- Identitätsprüfungen der Endteilnehmer,

- Zertifikatsbeantragungsverfahren,
- Registrierung durch Sub-Registratoren
- Bearbeitung von Zertifikatsanträgen,
- Verteilung von Schlüsseln und Geheimnissen (Passwort, PIN),
- Zertifikatsannahmen,
- Zertifikatserneuerung (Re-Zertifizierung),
- Schlüsselerneuerung (Re-Key),
- Zertifikatssperrungen,
- Zutrittsschutz,
- Zugriff auf Registrator-Arbeitsplätze,
- Schlüsselsicherung und -archivierung.

8.5 Maßnahmen zur Mängelbeseitigung

Werden bei einem Compliance-Audit von einem Prüfer bei einem Domänen-Betreiber Mängel festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durch zu führen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheiden der Leiter Trust Center über den Zeitrahmen der Behebung.

8.6 Mitteilung der Ergebnisse

Die Ergebnisse der Prüfung werden in einem vom Prüfer erstellen 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.

9 Sonstige geschäftliche und rechtliche Bestimmungen

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 Endteilnehmer- und Registrator-Zertifikaten Entgelte zu berechnen. Dies gilt insbesondere für die Bereitstellung und Überlassung des Dienstes Shared-Business-CA.

9.1.2 Entgelte für den Zugriff auf Zertifikate

T-Systems berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst der Shared-Business-CA keine Entgelte.
T-Systems gestattet Dritten, die selbst Produkte und Dienstleistungen vermarkten, nur nach vorheriger ausdrücklicher schriftlicher Genehmigung den Zugriff und Abruf von Zertifikaten.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

T-Systems berechnet für den Zugriff auf Sperrungs- oder Statusinformationen für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile keine Entgelte.
T-Systems gestattet Dritten, die selbst Produkte und Dienstleistungen vermarkten, nur nach vorheriger ausdrücklicher schriftlicher Genehmigung den Zugriff auf Sperr- und Statusinformationen von Zertifikaten.

9.1.4 Entgelte für andere Leistungen

T-Systems berechnet keine Entgelte auf den Abruf und der damit verbundenen Betrachtung dieses Dokuments „Erklärung zum Zertifizierungsbetrieb“. Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1), die das Urheberrecht des Dokuments (Kapitel 9.5.2) besitzt.
Ebenfalls ist die Nutzung dieser CPS entgeltfrei, sofern Sie als mit geltende Vertragsunterlage für die Vertragsbeziehung zwischen Domänen-Betreiber und T-Systems dient.

9.1.5 Entgelterstattung

Die Erstattung von Entgelten durch T-Systems erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts.

9.2 Finanzielle Verantwortlichkeiten

9.2.1 Versicherungsschutz

Dem Domänen-Betreiber obliegt die Pflicht sich im Rahmen seiner Betriebshaftpflichtversicherung bei einem Versicherungsträger oder mittels einer eigenen Deckungsvorsorge für einen wirtschaftlich angemessenen Versicherungsschutz abzusichern. Diese Versicherungsklausel findet ggf. keine Anwendung bei kommunalen, Landes- oder Staats-Behörden.
T-Systems verfügt über einen entsprechenden Betriebs- und Vermögenshaftpflichtversicherungsschutz.

9.2.2 Sonstige finanzielle Mittel

Dem Domänen-Betreiber wird empfohlen, selbst über ausreichend finanzielle Mittel zu verfügen, um damit die Aufrechterhaltung ihres PKI-Betriebes als auch zur Erfüllung ihrer aus diesem Dokument beschriebenen und abgeleitenden Pflichten nachkommen zu können. Darüber hinaus muss der Domänen-Betreiber in der Lage

sein, das Haftungsrisiko gegenüber den Endteilnehmern zu tragen, sofern dieses Risiko nicht übertragen werden kann.
T-Systems wird nicht grundsätzlich den Nachweis über finanzielle Mittel fordern. Eine Ausnahme bilden jedoch Compliance-Audits wie in Kapitel 8 beschrieben.

9.2.3 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 1.3.2 und 1.3.3) der Shared-Business-CA eingestuft, die nicht unter Kapitel 9.3.2 fallen.

9.3.2 Umfang von nicht vertraulichen Informationen

Unter nicht vertraulichen Informationen werden alle impliziten und expliziten Informationen der Shared-Business-CA eingestuft, die in ausgegebenen Zertifikaten (z.B. E-Mail-Adresse), Sperrlisten, 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.

Der Domänen-Betreiber hat die einschlägigen gesetzlichen Bestimmungen sowie ggf. weiteren Regelungen zum Datenschutz zu beachten.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

9.4.1 Datenschutzkonzept

Innerhalb der Shared-Business-CA müssen die Registrierungsstellen zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten.

Die T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 BDSG sicher.
Entsprechend den Konzernvorgaben der Deutschen Telekom AG wurde für Shared-Business-CA ein Datenschutzkonzept erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte um PKI-Dienst zusammen.
Das Datenschutzkonzept kann in Auszügen auf Anforderung bereitgestellt werden.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.1.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.2.

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

Ferner dürfen alle Informationen veröffentlicht werden, die nach Kapitel 9.4.3 als nicht vertraulich behandelt werden und deren Veröffentlichung durch den Domänen-Betreiber nicht widersprochen wurde.

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 Gründe zur Offenlegung von Daten

Keine Bestimmungen.

9.5 Rechte des geistigen Eigentums (Urheberrecht)

Die nachfolgenden Kapitel 9.5.1 bis 9.5.4 gelten für geistige Eigentumsrechte von Endteilnehmern und Vertrauenden Dritten.

9.5.1 Eigentumsrechte an Zertifikaten und Sperrinformationen

T-Systems behält sich jede geistigen Eigentumsrechte vor an Sperr- oder Statusinformationen, öffentlich zugängliche Verzeichnisdiensten und Datenbanken mit den ihnen enthaltenen Informationen, die die Shared-Business-CA ausstellt bzw. verwaltet. Die Eigentumsrechte von Zertifikaten obliegen dem Domänen-Betreiber, innerhalb dessen Master-Domäne die Zertifikate ausgestellt wurden.
Sofern Zertifikate und deren Inhalte, die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilen T-Systems und der Domänen-Betreiber ihre Zustimmung, Zertifikate auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren.
Unter Vorraussetzung, dass die Nutzung von Sperr- oder Statusinformationen und deren Inhalte, die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt T-Systems ihre Zustimmung, Sperrlisten und Statusinformationen auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren, insbesondere an Vertrauenden Dritte.

9.5.2 Eigentumsrechte dieser Erklärung zum Zertifizierungsbetrieb (CPS)

Dieses Dokument ist urheberrechtlich geschützt, alle geistigen Eigentumsrechte obliegen der T-Systems. Jegliche andere Nutzung (z.B. Vervielfältigung, Verwendung von Texten und Bildern, Änderung oder Erzeugung eines vergleichbaren oder abgeleiteten Dokuments, Weitergabe an Personen ohne Interesse an dem in diesem Dokument beschriebenem Dienst), auch auszugsweise, bedarf der vorherige ausdrücklichen schriftliche Genehmigung des Herausgebers dieses Dokuments „Erklärung zum Zertifizierungsbetrieb“ (siehe Kapitel 1.5.1).

9.5.3 Eigentumsrechte an Namen

Der Endteilnehmer behält, sofern zutreffend, alle Rechte an Namen oder Marken, die im Zertifikat enthalten sind, sofern das Zertifikat einen eindeutigen Namen beinhaltet.

9.5.4 Eigentumsrechte an Schlüsseln und Schlüsselmaterial

Die geistigen Eigentumsrechte von Schlüsselmaterial von CA- und Root-CA verbleiben bei T-Systems, ungeachtet des Mediums, auf denen sie gespeichert sind. Kopien von CA- und Root-CA-Zertifikate dürfen vervielfältigt werden um diese in vertrauenswürdige Hardware- und Software-Komponenten zu integrieren.

Schlüsselmaterial, das der Domänen-Betreiber bzw. Endteilnehmer selbst erzeugte oder über Shared-Business-CA erzeugte (z.B. Bulk), verbleibt sein Eigentumsrecht. Dies gilt auch für Schlüsselmaterial auf Smartcards, das er erworben hat.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle

T-Systems verpflichtet sich,

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

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

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle

Registrierungsstellen verpflichten sich,

- das Master- bzw. Sub-Registrator-Zertifikat (und deren Derivate, Kapitel 1.3.2.2.2) nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- ihren privaten Schlüssel geheim zu halten vor unberechtigtem Zugriff durch Dritte zu schützen,
- keine wesentlich unrichtigen Angaben im Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- das keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsantrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- dass das von ihnen eingesetzte Zertifikat ausschließlich für autorisierte und legale Zwecke verwendet wird, die der Domänen-Betreiber vorgibt, und nicht den Regelungen dieser Erklärung zum Zertifizierungsbetrieb widersprechen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der vorliegenden Erklärung zum Zertifizierungsbetrieb beschriebenen Pflichten entstehen,

- bei Verlust oder Verdacht der Kompromittierung des geheimen Schlüssels eine Sperrung des entsprechenden Master- bzw. Sub-Registrator-Zertifikat (und deren Derivate) zu veranlassen,
- auf Anforderung eines Endteilnehmers oder autorisierten Vertreters bei Verlust oder Verdacht der Kompromittierung des geheimen Schlüssels eine Sperrung durchzuführen,
- das alle Zertifikate den wesentlichen Anforderungen dieser Erklärung zum Zertifizierungsbetrieb genügen, und
- das die Sperrfunktionalitäten durch Master- und Sub-Registratoren und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) in allen wesentlichen Anforderungen der geltenden Erklärung zum Zertifizierungsbetrieb erfüllen.

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

9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Endteilnehmer verpflichten sich,

- das Endteilnehmer-Zertifikat nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- ihren privaten Schlüssel geheim zu halten vor unberechtigtem Zugriff durch Dritte zu schützen. Im Falle von privaten Schlüsseln von juristischen Personen, Infrastruktur-Komponenten erfolgt der Schutz durch autorisierte Personen,
- das jede digitale Signatur mit dem privaten Schlüssel erstellt wird, die zum im Zertifikat zugehörigen öffentlichen Schlüssel passt und dem Endteilnehmer eindeutig zugeordnet werden kann,
- dass jede digitale Signatur mit dem Schlüsselmaterial eines gültigen und nicht gesperrten Zertifikats erfolgt,
- dass die in seinem Endteilnehmer-Zertifikat aufgenommenen Zertifikatsinhalte des Subject-DN der Wahrheit entsprechen. Im Falle von juristischen Personen, Infrastruktur-Komponenten erfolgt die Prüfung der Zertifikatsinhalte durch autorisierte Personen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der vorliegenden Erklärung zum Zertifizierungsbetrieb beschriebenen Pflichten entstehen,
- bei Verlust oder Verdacht der Kompromittierung des geheimen Schlüssels eine Sperrung des entsprechenden Endteilnehmer-Zertifikat zu veranlassen bzw. selbst durchzuführen,
- dass das von ihnen eingesetzte Zertifikat ausschließlich für autorisierte und legale Zwecke die der Domänen-Betreiber vorgibt verwendet wird und nicht den Regelungen dieser Erklärung zum Zertifizierungsbetrieb widersprechen, und
- das der Endteilnehmer tatsächlich ein Endteilnehmer ist und mit seinem privaten Schlüssel, dem der im Zertifikat enthaltene öffentliche Schlüssel zugeordnet ist, keine CA-Funktionalitäten durchführt wie z.B. Signatur von Zertifikaten oder Sperrlisten.

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

9.6.4 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

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

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Keine Bestimmungen.

9.7 Haftungsausschluss

Der Anbieter haftet nur im vertraglich vereinbarten Umfang.

9.8 Haftungsbeschränkungen

Der Anbieter haftet nur im vertraglich vereinbarten Umfang.

9.9 Schadenersatz

Schadenersatzansprüche sind im Dokument „Allgemeinen Geschäftsbedingungen TeleSec Shared-Business-CA" (AGB SB-CA) geregelt.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Die Erstveröffentlichung dieses Dokuments „Erklärung zum Zertifizierungsbetrieb" als auch dessen Änderungen treten mit der Veröffentlichung auf öffentlichen Webseiten der T-Systems (siehe Kapitel 2.3) in Kraft.

9.10.2 Beendigung

Diese Erklärung zum Zertifizierungsbetrieb bleibt in der jeweils gültigen Version in Kraft, bis sie durch eine neue Version ersetzt wird.

9.10.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung des Dienstes Shared-Business-CA bleiben alle Domänen-Betreiber (Teilnehmer der Master-Domänen) als auch die Benutzer der daraus erzeugten Endteilnehmer-Zertifikaten an die in der Erklärung zum Zertifizierungsbetrieb enthaltenen Regelungen gebunden, bis das letzte Zertifikat ungültig oder gesperrt ist.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Für individuelle Mitteilungen und Kommunikation mit der Zertifizierungsstelle Shared-Business-CA werden die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben (siehe auch Dokument „Zertifikats- und Konfigurationsdatenblatt").

9.12 Änderungen

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich die T-Systems das Recht vor, Änderungen und Anpassungen dieser Erklärung zum Zertifizierungsbetrieb durchzuführen.

9.12.1 Verfahren für Änderungen

Änderungen dieser Erklärung zum Zertifizierungsbetrieb können nur von T-Systems Change Advisory Board durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und Veröffentlichungsdatum.
Änderungen der Erklärung zum Zertifizierungsbetrieb treten unverzüglich mit der Veröffentlichung in Kraft (siehe auch Kapitel 2.3).

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

Innerhalb bestehender Verträge sind Änderungen dieser Erklärung zum Zertifizierungsbetrieb mindestens sechs Wochen vor Wirksamwerden schriftlich dem Kunden mitzuteilen. Bei Änderungen zu Ungunsten des Kunden steht dem Kunden ein Sonderkündigungsrecht zum Zeitpunkt des Wirksamwerdens der Änderung zu. Erfolgt seitens des Kunden innerhalb von sechs Wochen nach Zugang der Änderungsmitteilung keine schriftliche Kündigung, werden die Änderungen zum Zeitpunkt des Wirksamwerdens Vertragsbestandteil.

9.12.2 Benachrichtigungsverfahren und -zeitraum

Domänen-Betreiber werden über Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch ein zu legen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion wie unter Kapitel 9.12.1 in Kraft. Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.
Falls das T-Systems Change Advisory Board der Ansicht ist, dass gravierende z.B. sicherheitsrelevante Änderungen unverzüglich erforderlich sind, dann tritt die neue Erklärung zum Zertifizierungsbetrieb unverzüglich mit der Freigabe (siehe Kapitel 9.12.1) in Kraft.

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

T-Systems Change Advisory Board entscheidet darüber, ob Änderungen der Objekt-ID der Erklärung zum Zertifizierungsbetrieb notwendig werden. Andernfalls erfordern Änderungen keine Änderungen der Objekt-ID der Zertifikatsrichtlinie.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

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

9.14 Geltendes Recht

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

9.15 Einhaltung geltenden Rechts

Die vorliegende Erklärung zum Zertifizierungsbetrieb 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 der vorliegenden Erklärung zum Zertifizierungsbetrieb 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 dieser Erklärung zum Zertifizierungsbetrieb unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser CPS im Übrigen nicht. Statt der unwirksamen und undurchführbaren Bestimmung gilt eine solche Bestimmung als vereinbart, die dem wirtschaftlichen Zweck dieser Erklärung zum Zertifizierungsbetrieb 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

Innerhalb des gesetzlich zulässigen Rahmens müssen Verträge mit Domänen-Betreibern, Vertrauende Dritte oder Endteilnehmer Schutzklauseln über Höhere Gewalt enthalten, um T-Systems schützen zu können.

9.17 Sonstige Bestimmungen

Nicht anwendbar.

A Ergänzende Literatur

A.1 Rollenspezifische Handbücher

- Master-Registrator-Handbuch
- Sub-Registrator-Handbuch
- Benutzer-Handbuch
- Leistungsbeschreibung (LB)
- Service Level Agreement (SLA)
- Allgemeine Geschäftsbedingungen (AGB)

B Legende

✓ Leistungsmerkmal vorhanden
✗ Leistungsmerkmal nicht vorhanden

C Akronyme und Begriffsdefinition

C.1 Akronyme

AGB	Allgemeine Geschäftsbedingungen
AICPA	American Institute of Certified Public Accountants
ASP	Application Service Provider
ARL	Authority Revcation List
DK	Dual Key
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
DIN	Deutsches Institut für Normung eV
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Systems
FQDN	Fully Qualified Domain Name
GR	Kennzeichner für Gruppen, Funktions-, Rollenzertifikat
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
LB	Leistungsbeschreibung
LDAP	Lightweight Directory Access Protocol
n.v.	nicht vorhanden
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudunym
PSE	Personal Security Environmen
RA	Registration Authority
RFC	Requests for Comments
SAS	Statement of Auditing Standards
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key
SLA	Service Level Agreement
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SigG	Signaturgesetz
SigV	Signaturverordnung
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TK	Triple Key
UPN	User Principal Name
URL	Uniform Resource Locator

UTC Universal Time Coordinated
XML Extensible Markup Language

C.2 Begriffsdefinition

Abkürzung	Beschreibung
Authority Revocation List (ARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (außer Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
Betreiber-Domäne	Siehe Master-Domäne.
Bulk	Funktion der Shared-Business-CA mit der der Sub-Registrator Soft-PSE per Massengerierung erzeugen kann.
Certificate Policy (CP)	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Revocation List (CRL)	Siehe Sperrliste.
Certification Authority (CA)	Siehe Zertifizierungsstelle.
Certification Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
Chipkarte	Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Domänen-Betreiber	Kunde der T-Systems, der Shared-Business-CA beauftragt hat und diesen Dienst innerhalb seiner Master-Domäne(n) nutzt.
Dual-Key-Zertifikat	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	Siehe auch Zertifikatsnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Hardware Security Modul (HSM)	Hardware zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hashwert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
Infrastrukturkomponente	Hard-Komponente wie beispielsweise Router, Server, Gateway, Applikation, die zertifikatsbasierende Funktionen unterstützen, selbst aber nicht oder nur begrenzt

	selbst Zertifikate beantragen können. Häufig werden Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.
Interface	Schnittstelle als Teil eines Systems, dass zur Kommunikation (Ein- und Ausgabe) dient.
key back-up	Mechanismus zur Schlüsselsicherung. Um beispielsweise verschlüsselte E-Mails bei Schlüsselverlust wieder herstellen zu können empfiehlt sich das key back-up des Schlüsselmaterials des Verschlüsselungsschlüssels.
Key-Recovery	Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert.
Kompromittierung	Ein privater Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
Latenzzeit	Zeitraum zwischen einer Aktion und dem Eintreten einer verzögerten Reaktion (Verzögerungszeitraum). Bei der Latenzzeit erfolgt die Aktion im Verborgenen und wird erst durch die Reaktion festgestellt.
LDAP-Server	Server, der Informationen speichert, die über LDAP abrufbar sind.
Lightweight Directory Access Protocol (LDAP)	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Mail-Security	Security-Funktionen wie Digitale Signatur und Verschlüsselung, die Standrad-Mail-Anwendungen unterstützen.
Mandantenfähigkeit	Als Mandantenfähigkeit bezeichnet man in der Informationstechnik (IT) die Eigenschaft einer Software bzw. Server, auf einer Installation mehrere voneinander vollständig getrennte Mandanten abzubilden. Die jeweiligen Mandanten, etwa unterschiedliche rechtliche Einheiten oder Firmen, haben dabei keinerlei gegenseitigen Einblick in die Daten, Benutzerverwaltung oder Ähnliches der anderen Parteien/Mandanten.
Master-Domäne	Getrennter Bereich, in dem ein Kunde die Dienstleistung Shared-Business-CA einsetzt. Die Master-Domain ist durch einen eindeutig festzulegenden Namen gekennzeichnet, der in den Endteilnehmer-Zertifikaten aufgeführt ist.
Master-Registrator	Natürliche Person der die Master-Domäne verwaltet.
Online Certificate Status Protocol (OCSP)	Das Online Certificate Status Protocol ermöglicht die Online-Abfrage der Gültigkeit von Zertifikaten.
Personal Identification Number (PIN)	Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.
Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
Public Key Service (PKS)	Service des T-Systems Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Policy	Richtlinien bzw. Erklärung, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
Personal Security	In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen

Environment (PSE)	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.
Registration Authority (RA)	Siehe Registrierungsstelle.
Registrierungsstelle	Komponente, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten.
Request	Engl. Begriff für Antrag. In diesem Zusammenhang ist der Zertifikatsantrag zu verstehen.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
Root-CA	Siehe Wurzelzertifizierungsstelle.
Statement of Auditing Standards (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.
Simple Certificate Enrollment Protocol (SCEP)	Simple Certificate Enrollment Protocol. Protokoll zur Beauftragung und zum Laden von Zertifikaten in IPSec Devices.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Erweiterung des E-Mail-Formats MIME, die Zusätze für kryptografische Dienste beschreibt, welche Authentizität, Integrität und Vertraulichkeit von Nachrichten sicherstellen.
Schlüssel	Ein Schlüssel bezeichnet in der Kryptografie eine geheime Information (privater Schlüssel) oder ein öffentliches Gegenstück dazu (öffentlicher Schlüssel). Es gibt Verfahren, bei denen jeweils mit dem gleichen privaten Schlüssel ver- und entschlüsselt wird sowie Verfahren bei denen ein öffentlicher Schlüssel zum Verschlüsseln und ein privater zum Entschlüsseln verwendet wird.
Schlüsselmaterial	Das Schlüsselmaterial beinhaltet den privaten und korrespondierenden öffentlichen Schlüssel. Eien kryptografische Aktion (z.B. Verschlüsselung) und deren Inversion (z.B. Entschlüsselung) ist nur mit beiden Schlüsselteilen möglich.
Schlüsselverantwortlicher	Eine durch den Domänen-Betreiber autorisiert natürliche Person, die verantwortlich ist für die ordnungsgemäße Verwendung (Verteilung, Nutzung und ggf. Sperrung) von Zertifikaten für Personen- und Funktionsgruppe, juristische Person als auch Infrastrukturkomponente.
Secure Socket Layer (SSL)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet. Kann ihn vielen Fällen statt dem komplexeren IPSec verwendet werden.
Service Desk	Das Service Desk ist eine organisatorische Einheit innerhalb eines Unternehmens, das für den Kunden als zentrale Anlaufstelle für alle Service- und Supportanfragen dient und diese innerhalb des Unternehmens entsprechend den vereinbarten Geschäftsprozessen vermittelt.
Signatur	Siehe digitale Signatur.
Single-Key-Zertifikat	Variante, bei der für Verschlüsselung und Signatur das selbe Schlüsselpaar verwendet wird, das heißt, ein Benutzer besitzt ein Zertifikat.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP stellt einen einfachen Mechanismus zum Austausch von strukturierter Information zwischen Anwendungen in einer dezentralisierten, verteilten Umgebung zur Verfügung.

Smartcard	Chipkarte mit Rechenfunktionalität, die für kryptografische Zwecke verwendet werden kann.
Software-PSE (Soft-PSE)	Durch Verschlüsselung geschützte Datei zur Speicherung des privaten Schlüssels eines Benutzers.
Sperrberechtigter	Person, die von einem Schlüsselverantwortlichen autorisiert ist, ein Zertifikat für Personen- und Funktionsgruppen, juristische Personen und Infrastrukturkomponenten sperren zu dürfen.
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.
Sub-Domäne	Hierarchisch untergeordneter Bereich der Master-Domäne.
Sub-Registrator	Natürliche Person der die Sub-Domäne verwaltet.
Subject- Distinguished Name (Subject-DN)	Subject = engl. Subject (Person oder Maschine). Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Subject-DN bezeichnet eindeutig den Zertifikatsinhaber.
Suspension	Im Zusammenhang von PKI ist unter Suspendierung die vorläufige bzw. temporäre Sperrung zu verstehen. Das Zertifikat erscheint zunächst in der Zertifikatssperrliste kann aber durch den Sub-Registrator wieder aktiv geschaltet werden.
Triple-Key-Zertifikat	Variante, bei der für Verschlüsselung, Signatur und Microsoft Smartcard-LogOn getrennte Schlüsselpaare verwendet werden, das heißt, ein Benutzer besitzt drei entsprechende Zertifikate.
T-Systems Advisory Board	Gremium innerhalb der T-Systems das über PKI-Funktionalitäten entscheidet.
Validierung	Im Zusammenhang von PKI ist unter Validierung die Gültigkeitsprüfung von Zertifikaten zu verstehen. Im Allgemeinen wird der Gültigkeitszeitraum auf Basis der PC-Systemszeit, der Sperrstatus (auf Basis Sperrliste oder OCSP und die Zertifikats-Hierarchie (ausstellende CA-Instanz) geprüft.
Vertrauende Dritte (Relying Parties)	Eine natürliche oder juristische Person (z.B. Firma, Organisation) die im Vertrauen auf die Funktion eines Zertifikats handelt.
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.
Webtrust	Überprüfung und Bestätigung für Zertifizierungsstellen (WebTrust for Certification Authorities) durch ein unabhängiges Wirtschaftsprüferunternehmens das die PKI nach den Webtrust-Kriterien „American Institut of Certified Public Accountants“ (AICPA) betrieben werden. Ziel der WebTrust-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken.
Wurzelzertifizierungsstelle	Oberste Zertifizierungsinstanz einer CA-Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsinstanz ausgestellt wurde, sondern selbstsigniert ist. Dieses Zertifikat stellt den „vertrauenswürdigen Anker“ innerhalb der Anwendung dar.
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	Strukturierter Datensatz, indem der Eigentümer (natürlichen Person, Personen- und Funktionsgruppe, juristische Person oder Infrastrukturkomponente) sowie

	weitere Eigenschaften einem öffentlichen Schlüssels zuordnet ist, der durch eine Zertifizierungsinstanz (CA) elektronische signiert ist.
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 (natürliche oder juristische Person, Personen – und Funktionsgruppe, Infrastruktur-Komponente), die ein Zertifikat und den dazu gehörenden privaten Schlüssel verwendet.
Zuständigkeitsbereich	Hierarchisch untergeordneter Teilbereich der Master-Domäne, der von einem Sub-Registrator verwaltet wird.

Quellenverzeichnis

[BDSG] Datenschutzgesetz und BDSG-Novelle 2009

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

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

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

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

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

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