Zertifizierungserklärung für die T-Systems Trust Center Public Key Infrastruktur der Root-CA "Deutsche Telekom Root CA 2"

Certification Practice Statement, CPS

Version: 1.5
Stand: 17.04.2009
Status: Freigegeben

Business flexibility T · · Systems · · ·

Impressum

Herausgeber
T-Systems Enterprise Services GmbH Trust Center Services Untere Industriestraße 20 57250 Netphen

Dateiname	Dokumentennummer	Dokumentenbezeichnung
CPS_DT_CA_2_deutsch_v1.5.doc	1.3.6.1.4.1.7879.13.21	Certification Practice Statement, CPS

Version	Stand	Status
1.5	17.04.2009	Freigegeben

Autor	Inhaltlich geprüft von	Freigegeben von
T-Systems Enterprise Services GmbH ITO-AL Region-PSS-Security Solutions- Trust Center Services	S. Kölsch, L. Eickholt	A. Treßel

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

Kurzinfo
Certification Practice Statement für die T-Systems Trust Center Public Key Infrastruktur der Root CA DT CA 2

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
0.1	08.08.2006	L. Eickholt	Initialversion Entwurf
0.3	13.10.2006	L. Eickholt	Inhaltliche Aktualisierungen Entwurf
0.9	10.11.2006	L. Eickholt	Inhaltliche Aktualisierungen Entwurf
1.0	29.11.2006	M. Graf, W. Pietrus	Korrekturen
1.1	04.05.2007	M. Ulm, L. Eickholt	Korrekturen
1.2	15.08.2007	M. Ulm, L. Eickholt	Korrekturen
1.3	13.09.2007	L. Eickholt	Kapitel 2.2 aktualisiert, Kapitel 3.2.4 gelöscht „Endteilnehmer“, 5.4.1 Gelöscht Begriff „Endteilnehmer“, 6.3.1 Gelöscht Begriff „Endteilnehmer“, Kapitel 5.8 aktualisiert, Kapitel 9.13 eingefügt, Kapitel 9.14 aktualisiert, 9.9 geändert CP in CPS, Kapitel 6.2 aktualisiert, 4.6 ergänzt, Kapitel 3.1.3 aktualisiert, Kapitel 4.3.2 aktualisiert, Kapitel 8 komplett überarbeitet, Kapitel 4.9.3 aktualisiert, Kapitel 9.5 ergänzt, Kapitel 9.9 geändert in Kapitel 9.12, 9.12.1 und 9.12.2 hinzu gefügt
1.5	17.04.2009	L. Eickholt, S. Kölsch	Diverse Ergänzungen CA-Verkettung Kapitel 1.1 ergänzt, Kapitel 1.3.1 aktualisiert, Kapitel 1.3.2.1 hinzugefügt, Kapitel 1.3.3.1 hinzugefügt, Kapitel 1.3.5 aktualisiert, Kapitel 1.4. erweitert, Kapitel 1.5.2 aktualisiert, Kapitel 2.1 aktualisiert, Kapitel 2.2 aktualisiert, Kapitel 3.4 aktualisiert, Kapitel 4.1.2.1 hinzugefügt, Kapitel 4.9.1 erweitert, Kapitel 4.12 erweitert, Kapitel 5 erweitert, Kapitel 6 erweitert, Kapitel 8 erweitert, Kapitel 9.10.aktualisiert

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das Trust Center der Deutschen Telekom AG wird durch die Konzerneinheit T-Systems Enterprise Services GmbH, ITO - AL Region – PSS - Security Solutions - Trust Center Services betrieben. Es wird im Folgenden als **„T-Systems Trust Center"** bezeichnet.

Das T-Systems Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Root-CA 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 oder Suspendierungen, sowie der Veröffentlichung von Informationen.

Sowohl die bauliche als auch die organisatorische Infrastruktur erfüllt die strengen Anforderungen des deutschen Signaturgesetzes. Seit der Betriebsaufnahme hat das T-Systems Trust Center mehr als 4,6 Millionen Zertifikate ausgestellt. Zu den vom Trust Center angebotenen Leistungen gehört unter anderem der TeleSec Public Key Service (PKS), der die Ausstellung qualifizierter Zertifikate gemäß dem deutschen Signaturgesetz (SigG) umfasst.

1.1 Überblick

Bei dem vorliegenden Dokument handelt es sich um die **Zertifizierungserklärung** (engl. Certification Practice Statement, kurz **CPS**) für die PKI der Root-CA „Deutsche Telekom Root CA 2", die im T-Systems Trust Center betrieben wird.

Das vorliegende CPS beschreibt das für den Betrieb der PKI erforderliche Sicherheitsniveau und beinhaltet Sicherheitsvorgaben sowie Erklärungen hinsichtlich technischer, organisatorischer und rechtlicher Aspekte. Das vorliegende CPS kann die Regelungen der CP weiter ergänzen, konkretisieren und verfeinern, nicht jedoch den Regelungen der CP widersprechen oder diese in ihrer Qualität und Wirksamkeit unterschreiten.

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

Im Einzelnen behandelt das CPS die folgenden Aspekte:

- Veröffentlichungen und Verzeichnisdienst,
- Identifizierung und Authentifizierung von PKI Teilnehmern, und dabei insbesondere die Behandlung von verketteten CAs (Sub-CAs) von Dritten.
- Ausstellung von Zertifikaten,
- Erneuerung von Zertifikaten (Re-Zertifizierung),
- Sperrung und Suspendierung von Zertifikaten,

- bauliche und organisatorische Sicherheitsmaßnahmen,
- technische Sicherheitsmaßnahmen,
- Profile,
- Auditierung,
- verschiedene Rahmenbedingungen.

1.2 Dokumentenidentifikation

Name:	Zertifizierungserklärung für die T-Systems Trust Center Public Key Infrastrukturen
Version:	1.5
Datum	17.04.2009
Objektbezeichnung (Object Identifier)	1.3.6.1.4.1.7879.13.21

1.3 PKI Beteiligte

1.3.1 Zertifizierungsstellen

Neben dem Betrieb von Zertifizierungsstellen für eigene Produkte und Dienstleistungen stellt das T-Systems Trust Center CA Zertifikate für andere Betreiber von Zertifizierungsstellen für fortgeschrittene Zertifikate aus. Die Struktur der Zertifizierungsstellen wird im Folgenden erläutert.

1.3.1.1 Zertifizierungsstellen für fortgeschrittene Zertifikate

Das T-Systems Trust Center betreibt die „Deutsche Telekom Root CA 2“ Instanz für fortgeschrittene Zertifikatsdienste. Das Root-CA Zertifikat ist ein selbst-signiertes Zertifikat und wird durch T-Systems veröffentlicht. Die Veröffentlichung erlaubt eine Gültigkeitsüberprüfung aller in diesen Hierarchien ausgestellten Zertifikate. Die Root-CA Instanz zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen.

Die Struktur ist in der folgenden Abbildung schematisch dargestellt:

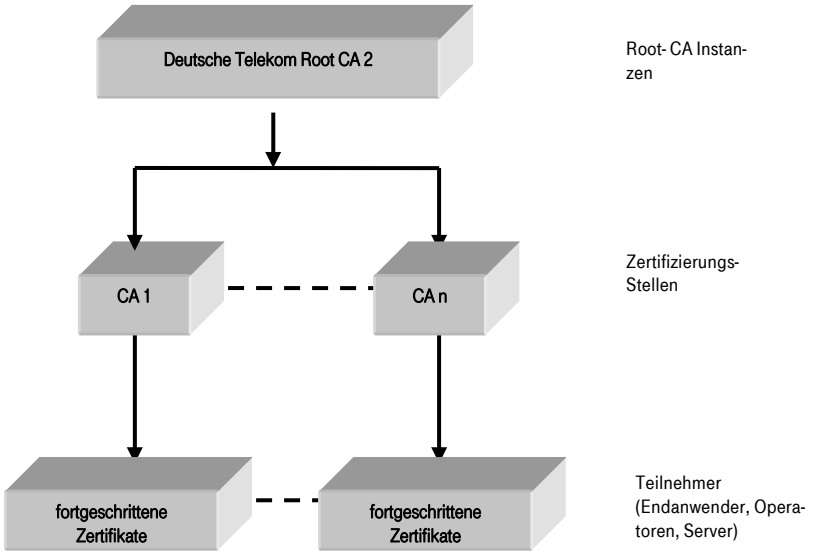

Abbildung 1: Zertifizierungsstellen für fortgeschrittene Zertifikate unter der „Deutsche Telekom Root CA 2" Instanz.

Jede Zertifizierungsstelle verfügt über ein oder mehrere von der jeweils übergeordneten Root-CA Instanz ausgestellte CA- und Dienste-Zertifikate, die in regelmäßigen Abständen neu ausgegeben werden.

Alle oben dargestellten und von der T-Systems oder anderen Betreibern betriebenen Zertifizierungsstellen für fortgeschrittene Zertifikate unterliegen der T-Systems CP.

1.3.2 Registrierungsstellen

Die Zertifizierungsstelle „Deutsche Telekom Root CA 2" betreibt nur eine zentrale Registrierungsstelle,

1.3.2.1 Registrierungsstellen bei CA-Verkettung

Wird eine CA eines externen Kunden als Sub-CA mit der „Deutschen Telekom Root CA 2" verkettet, erfolgt die Registrierung direkt durch Mitarbeiter des T-Systems Trust Centers. Als Vertrags- und Registrierungsgrundlagen gelten die Bestimmungen in der Leistungsbeschreibung „T-Systems Root Signing" [TSYSROOTSIGN]. Die Registrierung erfolgt nach einzelvertraglichen Regelungen.

1.3.3 Zertifikatsnehmer

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

Der Zertifikatsnehmer

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

1.3.3.1 Zertifikatsnehmer bei CA-Verkettung

Zertifikatsnehmer, die eine eigene CA betreiben und diese mit der „Deutsche Telekom Root CA 2“ verketten wollen, müssen spezielle Voraussetzungen erfüllen. Die genauen Voraussetzungen um als Sub-CA hierarchisch unter der „Deutsche Telekom Root CA 2“ aufgenommen zu werden sind in der Leistungsbeschreibung „T-Systems Root Signing“ [TSYSROOTSIGN] aufgeführt.

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

Teilnehmer, die keine Verpflichtung gegenüber Deutsche Telekom Root CA 2 eingegangen sind, werden in der Richtlinie nicht betrachtet.

1.4 Zertifikatsverwendung

1.4.1 Erlaubte Zertifikatsverwendung

1.4.1.1 Fortgeschrittene Zertifikate

Fortgeschrittene Zertifikate werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der Attribute zur Key Usage und den Festlegungen der CPS der jeweiligen Zertifizierungsstelle eingesetzt. Einige Beispiele sind:

- fortgeschrittene Signaturen im Sinne des deutschen Signaturgesetzes,
- Authentifizierung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPSec, S/MIME, XML-SIG, SOAP),
- Authentifizierung im Rahmen von Prozessen (Windows Log-On),
- Verschlüsselung im Rahmen von Kommunikationsprotokollen (z.B. SSL, IPSec, S/MIME, XML-ENC, SOAP),
- Festplattenverschlüsselung.

1.4.1.2 Zertifikate bei CA-Verkettung

Die im Rahmen der Dienstleistung „T-Systems Root Signing“ [TSYSROOTSIGN] signierten Root-Zertifikate dürfen nur zur Austellung von digitalen -Zertifikaten verwendet werden, die zum einen den Anforderungen

dieses und aller mitgeltenden Dokumente genügen, zum anderen die jeweils vertraglich definierten Bezugsbereiche einhalten.

1.4.2 Untersagte Zertifikatsnutzung

Der kommerzielle Einsatz von Zertifikatsdiensten, die unter die Bedingung des Abschnitts 1.4.1.3 fallen, ist nicht gestattet.

1.5 Verwaltung der Erklärung

1.5.1 Zuständigkeit für die Richtlinie

Dieses CPS wird von T-Systems Enterprise Services GmbH, ITO - AL Region – PSS - Security Solutions - Trust Center Services heraus gegeben.

1.5.2 Kontaktperson

Adresse:
T-Systems Enterprise Services GmbH
Trust Center Services
Untere Industriestraße 20
57250 Netphen

Telefon: Tel: +49 1805 268 204
E-Mail: telesec_support@t-systems.com
WWW: www.telesec.de

1.5.3 Pflege der Erklärung

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

1.5.4 Zuständigkeit für die Anerkennung eines CPS

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

1.6 Definitionen und Abkürzungen

Siehe Kapitel 10 (Glossar).

2 Veröffentlichung und Verantwortlichkeiten für den Verzeichnisdienst

2.1 Verzeichnisdienst

Das T-Systems Trust Center stellt den Zertifikatsnutzern der PKI eine öffentliche und international 7 X 24h erreichbare ARL in Form eines LDAP-Verzeichnisses unter:

ldap://pki.telesec.de/CN=Deutsche%20Telekom%20Root%20CA%202,OU=T-TeleSec%20Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?AuthorityRevocationList

und im Internet unter

http://pki.telesec.de/rl/DT_ROOT_CA_2.crl

zur Verfügung.

2.2 Veröffentlichung von Informationen

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

- das Root-CA Zertifikat und dessen Fingerprint (SHA1),
- Dokumentation über den Wechsel eines Root-CA oder eines CA-Zertifikats,
- Informationen über eine Kompromittierung oder den Verdacht auf Kompromittierung oder die Sperrung eines Root-CA oder eines CA- Zertifikats,
- CPS im Status Freigegeben,
- Leistungsbeschreibung & Anforderungsprofil „T-Systems Root Signing“ zur Ausstellung von Root-Zertifikaten (CA-Verkettung),

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

2.3 Update der Informationen / Veröffentlichungsfrequenz

Sperrinformationen für Root-CA- und CA-Zertifikate werden im Fall einer Sperrung umgehend aktualisiert. CPS und ggf. weitere Informationen werden auf den Internetseiten zur Verfügung gestellt.

2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf die in Abschnitt 2.1 und 2.2 aufgeführten Informationen unterliegt für die Zertifikatsnehmer und -nutzer einer Zertifizierungsstelle keiner Zugangskontrolle.

Der schreibende Zugriff auf alle in Abschnitt 2.1 und 2.2 genannten Informationen erfolgt ausschließlich durch berechtigte Mitarbeiter bzw. autorisierte Systeme.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Namensform

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

Die Anforderungen an die Nutzung von Namensattributen im Subject DN und Subject Alternative Name hängen konkret vom Anwendungskontext einer Zertifizierungsstelle ab. Beispielsweise muss für Zertifikate, die für sichere E-Mail genutzt werden, die E-Mail Adresse des Zertifikatsnehmers eingetragen sein.

Allgemein sollte im Subject DN das Attribut „CommonName“ (CN) enthalten sein. Im Issuer DN muss das Attribut „CommonName“ (CN) enthalten sein.

3.1.2 Aussagekräftigkeit von Namen

Der Name muss den Zertifikatnehmer eindeutig identifizieren.

3.1.3 Pseudonymität / Anonymität

Wenn Zertifikate mit Pseudonymen erstellt werden, muss die Zertifizierungsstelle die reale Identität des Zertifikatsnehmers in ihren Unterlagen festhalten.

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

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

3.1.4 Regeln zur Interpretation verschiedener Namensformen

3.1.5 Eindeutigkeit von Namen

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

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Es liegt in der Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Die Zertifizierungsstelle ist nicht verpflichtet, solche Rechte zu überprüfen.

Allein der Zertifikatnehmer ist für solche Überprüfungen verantwortlich. Falls eine Zertifizierungsstelle über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat widerrufen.

3.2 Identitätsprüfung bei Neuauftrag

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

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

3.2.2 Authentifizierung eines externen Kunden

Grundvoraussetzung für einen Neuauftrag ist ein bestehendes Vertragsverhältnis. Dieses Vertragsverhältnis wird durch T-Systems Vertriebseinheiten unter Zuhilfenahme juristischer Abteilungen generiert. Damit ist die ausreichende Authentifizierung des externen Kunden gewährleistet.

3.2.3 Authentifizierung eines internen Kunden

Die Zertifizierungsstelle nimmt in geeigneter Weise eine zuverlässige Überprüfung mindestens derjenigen Auftragsdaten vor, die in das Zertifikat eingehen.

3.2.4 Nicht verifizierte Informationen

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

- Organisationseinheit (OU)

- sonstige Informationen, die im Zertifikat als nicht verifiziert gekennzeichnet sind

3.2.5 Unterschriftenvollmacht

Die Autorisierung einer natürlichen Person als handlungsberechtigt im Namen einer Organisation oder natürlichen Person ist durch den Vertragsabschluss und die damit im Vorfeld einhergehende Zuordnung der Verantwortlichkeiten gewährleistet.

3.3 Identifizierung und Authentifizierung bei Folge-Beauftragungen

Zur Folge-Beauftragung muss die Identitätsprüfung bei Neuauftrag (siehe Kapitel 3.2) durchlaufen werden.

3.4 Identifizierung und Authentifizierung bei Sperraufträgen

Das T-Systems Trust Center bietet einen zentralen Sperrservice, um im Falle des Verlustes oder bei Missbrauchsverdacht das eigene Zertifikat sperren zu können. Im Falle der Sperrung wird das Zertifikat in eine Sperrliste aufgenommen. Zur Sperrung autorisierte Personen und Institutionen (siehe Kapitel 4.9) können die Sperrung eines Zertifikates entweder per E-Mail oder telefonisch beauftragen.

Die Authentisierung einer Sperrung geschieht durch die Angabe der Grunddaten (Name, Firma, Rückrufnummer, E-Mailadresse). Der Sperrwunsch wird durch die Angabe des Sperrpasswortes autorisiert.

Für die Sperrung sind die folgenden Eingangskanäle zu verwenden:
Telefonisch: 01805 268204
E-Mail: TeleSec_Support@t-systems.com

4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsbeauftragung

4.1.1 Wer kann ein Zertifikat beauftragen?

Der Zertifikatsnehmer bzw. eine im Sinn von Kapitel 3.2.2 und 3.2.5 autorisierte Person kann Zertifikate beauftragen.

4.1.2 Registrierungsprozess

Ein Zertifikat für Zertifizierungsstellen kann erst erzeugt werden, wenn der Registrierungsprozess beim Auftragsmanagement erfolgreich abgeschlossen und dokumentiert wurde.

Telefon Auftragsmanagement: +49 271 708-1500
Telefax: +49 1805 3344900091
PC-Fax.: +49 521 98840091
E-Mail: telesec-auftrag@t-systems.com

Der Registrierungsprozess beinhaltet mindestens die folgenden Schritte:

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

4.1.2.1 Registrierungsprozess bei CA-Verkettung

Um als Sub-CA der „Deutsche Telekom Root CA 2“ fungieren zu können, ist die Beantragung eines Root-Zertifikats zur CA-Verkettung notwendig,

Der Registrierungsprozess beinhaltet mindestens die in 4.1.2 genannten Schritte. Zusätzlich müssen die in [TSYSROOTSIGN] genannten Anforderungen erfüllt werden.

4.2 Bearbeitung des Zertifikatsauftrags

4.2.1 Durchführung der Identifikation und Authentifizierung

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

4.2.2 Annahme oder Abweisung von Zertifikatsaufträgen

Nur bei erfolgreicher Überprüfung wird ein Zertifikatsauftrag angenommen und zur Bearbeitung weitergeleitet. Dies ist gegeben, wenn die Identifikation und Authentifikation aller erforderlichen Kundendaten erfolgreich war. (siehe Kapitel 3.2)

Im Falle einer Abweisung des Auftrags wird der Zertifikatsnehmer in geeigneter Weise unter Angabe von Gründen benachrichtigt.

4.2.3 Bearbeitungsdauer

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

4.3 Ausstellung von Zertifikaten

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

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

4.3.2 Benachrichtigung des Zertifikatsnehmers

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

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

4.4 Zertifikatsannahme

4.4.1 Akzeptanz durch den Zertifikatsnehmer

Das erhaltene Zertifikat wird durch die Rücksendung der Akzeptanzbestätigung (Akzeptanzbestätigung CA Zertifikat.rtf) an die Zertifizierungsstelle, innerhalb von 14 Tagen nach Erhalt des Zertifikats, entsprechend der im Vertrag vereinbarten Leistungen, akzeptiert.

4.4.2 Veröffentlichung des Zertifikats

Es gelten die Regelungen aus Kapitel 2.1.

4.4.3 Benachrichtigung weiterer Instanzen

Es erfolgt keine Benachrichtigung weiterer Instanzen.

4.5 Verwendung von Schlüsselpaar und Zertifikat

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

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

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Relying Parties

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

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

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Bei einer Re-Zertifizierung wird dem Zertifikatsnehmer ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaares ausgestellt, sofern die im Zertifikat enthaltenen Informationen sich nicht geändert haben. Dies setzt voraus, dass die eindeutige Zuordnung von Zertifikatsnehmer und Schlüssel erhalten bleibt, keine Kompromittierung des Schlüssels vorliegt, und die kryptographischen Verfahren (z.B. Schlüssellänge) für die Gültigkeitsdauer des neuen Zertifikats noch ausreichend sind. Eine Zertifikatserneuerung von CA-Zertifikaten ist nicht vorgesehen.

4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung ist nur vor Ablauf der Gültigkeit des vorhandenen Zertifikats zulässig.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

Die Zertifikatserneuerung kann nur durch den Zertifikatsnehmer beauftragt werden.

4.6.3 Ablauf der Zertifikatserneuerung

Es gelten die Regelungen von Kapitel 3.3.

4.6.4 Benachrichtigung des Zertifikatsnehmers

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.6.5 Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.6.6 Veröffentlichung einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.7 Erneuerung von Zertifikaten (Re-Key)

Beim Re-Key wird ein neues Schlüsselpaar verwendet. Ansonsten gelten sinngemäß alle Aussagen aus Kapitel 4.6.

4.8 Änderung von Zertifikatsdaten

Wenn sich Inhalte von Attributen des Zertifikats ändern, ist eine erneute Identifizierung wie im Falle der Erst-Beauftragung erforderlich.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Gründe für eine Sperrung

Die folgenden Gründe des Zertifikatsnehmers führen zu einer Sperrung des Zertifikats:

- Abhandenkommen des privaten Schlüssels (z.B. Verlust oder Diebstahl).
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor.
- Die Angaben im Zertifikat sind nicht mehr korrekt.
- Verwendung und Handhabung des Zertifikats im Widerspruch zu vertraglichen Regelungen oder der CP/CPS des Zertifikatsnehmers oder Zertifikatsgebers
- Der zertifizierte Schlüssel oder die damit verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.
- Ein Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen.
- Der Zertifikatsnehmer benötigt kein Zertifikat mehr und kündigt daher das Vertragsverhältnis.
- Gesetzliche Vorschriften
- Bei CA-Verkettung: Es wird von den vertraglich geregelten und in [TSYSROOTSIGN] dargelegten Regelungen abgewichen.

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

- 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
- Es liegt ein Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen vor.
- Der zertifizierte Schlüssel oder die damit verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.

4.9.2 Wer kann eine Sperrung beauftragen?

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

- der Zertifikatsnehmer,
- das T-Systems Trust Center

4.9.3 Ablauf einer Sperrung

Zur Sperrung autorisierte Personen und Institutionen können die Sperrung eines Zertifikates entweder per E-Mail oder telefonisch beauftragen. Die Authentisierung einer Sperrung geschieht in geeigneter Art und Weise.

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

Die autorisierte Person oder Institution wird über die Durchführung der Sperrung in geeigneter Weise informiert.

4.9.4 Fristen für einen Sperrauftrag

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

4.9.5 Fristen für die Zertifizierungsstelle

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

4.9.6 Methoden zur Prüfung von Sperrinformationen

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

4.9.7 Frequenz der Veröffentlichung von Sperrinformationen

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

4.9.8 Maximale Latenzzeit von Sperrlisten

Die Latenzzeit für Sperrlisten beträgt mindestens 12 Stunden.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Sperrinformationen, werden für die Zertifikatsnutzer online, siehe Kapitel 2.1, mit einem standard-konformen Verfahren bereitgestellt werden. Es sind alle von dieser Zertifizierungsstelle gesperrten Zertifikate enthalten.

4.9.10 Anforderungen an Online Überprüfungsverfahren

nicht definiert.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Derzeit werden keine anderen Formen der Bekanntmachung eingesetzt.

4.9.12 Kompromittierung privater Schlüssel

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

4.9.13 Suspendierung von Zertifikaten

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

4.9.14 Wer kann suspendieren?

nicht definiert.

4.9.15 Ablauf einer Suspendierung

nicht definiert.

4.9.16 Begrenzung der Suspendierungsperiode

nicht definiert.

4.10 Statusauskunftsdienste für Zertifikate

Ein Statusauskunftsdienst steht nicht zur Verfügung.

4.11 Kündigung durch den Zertifikatsnehmer

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

4.12 Schlüsselhinterlegung und Wiederherstellung

Für im T-Systems Trust Center betriebene Zertifizierungsstellen werden die Schlüsselpaare auf einem sicherheitsüberprüften Hardware Security Module HSM verschlüsselt hinterlegt und in sicherer Umgebung abgelegt.

Schlüsselpaare für extern betriebene Zertifizierungsstellen (externe Sub-CAs bei CA-Verkettung) müssen nach den Regelungen in [TSYSROOTSIGN] behandelt werden.

5 Bauliche und organisatorische Maßnahmen

Das T-Systems Trust Center ist in einem speziell geschützten Gebäude untergebracht und wird von fachkundigem Personal betrieben. Alle Prozesse für die Beauftragung und Erzeugung von Zertifikaten der dort betriebenen Zertifizierungsstellen sind genau definiert und im Fall qualifizierter Zertifikate von einer unabhängigen Stelle überprüft worden. Alle baulichen und organisatorischen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept (nicht öffentlich verfügbar) dokumentiert.

Die folgenden Aussagen gelten für die vom T-Systems Trust Center betriebenen Zertifizierungsstellen. Zertifizierungsstellen, die in der Hierarchie von Root-CAs des T-Systems Trust Center stehen, aber extern betrieben werden, müssen Regelungen wie die im folgenden beschriebenen in adäquater Weise umsetzen und in ihrer CPS beschreiben. Bei Bedarf muss ergänzend auch das Sicherheitskonzept der externen Zertifizierungsstellen zur Prüfung auf Konformität mit dieser Richtlinie der T-Systems vorgelegt werden. Die Mindestanforderungen an extern betriebene CAs sind in [TSYSROOTSIGN] dargelegt und müssen vor Inbetriebnahme der Sub-CA durch den externen Kunden umgesetzt sein.

5.1 Trust Center Sicherheitsmaßnahmen

5.1.1 Standort und bauliche Maßnahmen

T-Systems betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Hälften, zwei getrennt arbeitenden Energietrakten (Elektro, Klima, Wasser) mit Gebäudemanagementsystem und Notstromaggregaten sowie einem Verwaltungstrakt verfügt. Je nach Kundenanforderung kann im Trust Center ein abgestuftes Ausfallsicherungskonzept mit definierten Sicherungsstufen realisiert werden.

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

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

5.1.2 Zutritt

Im Trust Center gilt eine Zutrittsregelung die die Zutrittsrechte für Mitarbeiter, Mitarbeiter von Fremdfirmen und Gästen in den einzelnen Sicherheitszonen regelt. Der Zutritt ist zwischen den Sicherheitsbereichen nur über

Personenvereinzelungsanlagen möglich. Der kontrollierte Zutritt zu den verschiedenen Sicherheitsbereichen ist weiter mit einem rechnergesteuerten Zutrittskontrollsystem geschützt. Gäste werden nur in Ausnahmefälle und nach vorheriger Anmeldung empfangen. Hier gelten besondere Sicherheitsvorschriften.

5.1.3 Stromversorgung und Klimatisierung

Die Ansaugöffnungen für die Außenluft sind so angeordnet, dass keine Schadstoffe wie Staub und Schmutz, ätzende, giftige oder leicht brennbare Gase eindringen können. Die Systeme werden mit einem sehr geringen Außenluftanteil betrieben. Die erforderlichen Zuluftöffnungen sind zugangsgeschützt. Zum Schutz gegen Luftverunreinigung durch schwebende Partikel sind Filter installiert. Die Frischluftansaugung wird ständig auf aggressive Gase überwacht. Im Notfall (z.B. Brand in der Umgebung) wird die Außenluftansaugung automatisch durch Luftklappen verschlossen.

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

5.1.4 Wasserschäden

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

5.1.5 Brandschutz

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

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

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

In alle Systemräume, Systemoperatorräume, Archivräume, USV-Räume sowie weitere ausgewählte Raume sind Brandfrühesterkennungssystemen (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut.

5.2 Organisatorische Maßnahmen

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 (nicht öffentlich verfüg-

bar) und CPS Dokumenten der vom T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.3 Personelle Maßnahmen

Die Zuverlässigkeit des Personals, das im T-Systems Trust Center arbeitet, wird durch eine unabhängige Organisation überprüft. Das Personal besucht in regelmäßigen Abständen Fortbildungen.

Alle Anforderungen des deutschen Signaturgesetzes werden vollständig erfüllt. Die gleichen hohen Anforderungen werden in analoger Weise von qualifizierten und fortgeschrittenen Zertifizierungsstellen erfüllt.

Eine Rollentrennung bei kritischen Prozessen wird im jeweiligen Sicherheitskonzept (nicht öffentlich verfügbar) definiert. Organisationen, die als RA für das T-Systems Trust Center agieren, haben vertragliche Vereinbarungen geschlossen, die die Zuverlässigkeit und Fachkunde ihres Personals sowie die Einhaltung bestimmter zugewiesener Aufgaben sicherstellen.

5.4 Protokollereignisse

5.4.1 Aufgezeichnete Ereignisse

Veränderungen im Lebenszyklus des CA Schlüssels werden protokolliert, dies bezieht sich im Einzelnen auf die folgenden Ereignisse:

Erzeugung

Sicherung

Speicherung

Wiederherstellung

Archivierung

Vernichtung

Änderungen von Hardware und Software

Protokollierungen von Ereignissen im Lebenszyklus von CA Zertifikaten:

Zertifikatsauftrag (erfolgreich / fehlgeschlagene Bearbeitung und beiliegende Dokumente)

Zertifikatserneuerung

Schlüsselerneuerung

Zertifikatssperrung

Erstellung von Zertifikaten

Sperrlisten

Protokollierung von Internen und Externen Audits.

5.5 Sicherung der Aufzeichnungen

Alle Aufzeichnungen innerhalb des T-Systems Trust Centers werden zehn (10) Jahre nach Serviceende aufbewahrt .

5.6 Schlüsselwechsel bei Root-CA und CA

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

5.7 Kompromittierung privater Schlüssel von Root-CA und CA

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

5.8 Einstellung des Betriebes

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

Ein Beendigungsplan kann die folgenden Regelungen enthalten:

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

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

6 Technische Sicherheitsmaßnahmen

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

Die folgenden Aussagen gelten für die vom T-Systems Trust Center betriebenen Zertifizierungsstellen. Zertifizierungsstellen, die in der Hierarchie von „Deutsche Telekom Root CA 2“ des T-Systems Trust Center stehen, aber extern betrieben werden, müssen Regelungen wie die im folgenden beschriebenen in adäquater Weise umsetzen und in ihrer CPS beschreiben. Bei Bedarf muss ergänzend auch das Sicherheitskonzept der externen Zertifizierungsstellen zur Prüfung auf Konformität mit diesem CPS der T-Systems vorgelegt werden. Die Mindestanforderungen an extern betriebene CAs sind in [TSYSROOTSIGN] dargelegt und müssen vor Inbetriebnahme der Sub-CA durch den externen Kunden umgesetzt sein.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Alle Schlüsselpaare für Root-CA- und CA-Zertifikate werden in einem abgeschirmten Raum auf einer sicherheitsüberprüften Hardwarekomponente erzeugt und auf einer Hardwarekomponente gespeichert.

Im Fall von Root-CA und CA Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140-1/ Lev2 evaluiert) erzeugt und abgelegt.

6.1.2 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

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

6.1.3 Lieferung öffentlicher Schlüssel des Zertifizierungsdiensteanbieters an Zertifikatsnutzer

Öffentliche Schlüssel einer Zertifizierungsstelle können sowohl aus dem jeweiligen Verzeichnis als auch von den Webseiten der Zertifizierungsstelle (dort finden sich auch die entsprechenden Fingerprints veröffentlicht) bezogen werden (siehe hierzu auch Kapitel 2).

6.1.4 Lieferung öffentlicher Schlüssel an Dritte

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

6.1.5 Schlüssellängen

Die Schlüssellänge für CA-Zertifikate muss mindestens 1024-Bit betragen. Die Schlüssellängen der T-Systems Root-CA- und CA-Zertifikate beträgt 2048-Bit. Sie orientieren sich am aktuellen Stand der Technik.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

6.1.7 Schlüsselverwendungen

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

6.2 Sicherung privater Schlüssel

Im Fall von Root-CA und CA Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140 – 2 evaluiert) abgelegt. Das Backup der Schlüssel wird unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken durchgeführt. Die Verwendung des privaten Schlüssels wird durch eine PIN geschützt, die nur hierfür zuständigen Personen bekannt ist. Details regelt das Sicherheitskonzept.

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung von öffentlichen Schlüsseln

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

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Das „Deutsche Telekom Root CA 2“ Zertifikat hat eine Gültigkeit von 20 Jahren. CA- Zertifikate können bis zur maximalen Gültigkeit der Root-CA ausgestellt werden (siehe hierzu Kapitel 7.1.1).

7 Profile für Zertifikate und Sperrlisten

7.1 Zertifikatsprofil

7.1.1 Zertifikatsprofil des Root Zertifikats

7.1.1.1 Zertifikatsprofil „Deutsche Telekom Root CA 2“

Zertifikatsfeld	Inhalt		Bemerkungen
Version	v3		
SerialNumber	26		Hexadezimal (Dezimal 38)
SignatureAlgorithmIdentifier	RSA, SHA-1		
Issuer			
Country Name	DE		
Organization Name	Deutsche Telekom AG		
Organizational Unit Name 1	T-TeleSec Trust Center		
Common Name	Deutsche Telekom Root CA 2		
Validity			
Not Before	9.7.1999 12:11		GMT
Not After	9.7.2019 23:59		GMT; Gültigkeit 20 Jahre
Subject			
Country Name	DE		
Organization Name	Deutsche Telekom AG		
Organizational Unit Name 1	T-TeleSec Trust Center		
Common Name	Deutsche Telekom Root CA 2		
SubjectPublicKeyInfo			
Algorithm	<OID für RSA>		
Subject Public Key	<Schlüssel>		Schlüssellänge: 2048 Bit
Extensions			
Subject Key Identifier	non critical	31 c3 79 1b ba f5 53 d7 17 e0 89 7a 2d 17 6c 0a b3 2b 9d 33	
Basic Constraints	non	CA=1	

Zertifikatsfeld	Inhalt		Bemerkungen
	critical	PathLenConstraint=5	
Key Usage	critical	keyCertSign, cRLSign	

7.1.2 Zertifikatsprofile der Zertifizierungsstellen

Zertifikatsprofile für CA- und Teilnehmerzertifikate werden in der CPS einer Zertifizierungsstelle definiert.

7.2 Sperrlistenprofile

7.2.1 Sperrlistenprofile der Zertifizierungsstellen

Authority Revocation List (ARL) Deutsche Telekom Root CA 2:

Version		2 (0x1)
Signature Algorithm		sha1WithRSAEncryption
Issuer		/C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2
Last Update		Sep 12 09:46:56 2006 GMT
Next Update		Mar 13 21:46:56 2007 GMT (Last Update + 6 Monate)
CRL extensions		
	X509v3 Authority Key Identifier	DirName:/C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2 Serial:26
	X509v3 CRL Number	10
Revoked Certificates		
	Serial Number	25
	Revocation Date	Jul 9 12:07:00 1999 GMT
CRL entry extensions		
	X509v3 CRL Reason Code	Cessation Of Operation
Signature Algorithm		sha1WithRSAEncryption

8 Audits und andere Bewertungskriterien

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

8.1 Intervall von Prüfungen

Entsprechend der Anforderungen findet mindest einmal jährlich eine Überprüfung statt, wenn nicht besondere Ereignisse eine

8.2 Identität/Qualifikation des Prüfers

Für die Feststellung der Webtrust Program for Certification Authorities Konformität wird eine anerkannte, renommierte Wirtschaftsprüfergesellschaft beauftragt.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Für die Feststellung der Webtrust Program for Certification Authorities Konformität wird eine anerkannte, renommierte und unabhängige Wirtschaftsprüfergesellschaft beauftragt.

8.4 Abgedeckte Bereiche der Prüfung

Der Ausprägung der jährlichen Webtrust Überprüfung für Zertifizierungsstellen (Webtrust Program for Certification Authorities) oder einer äquivalenten Überprüfung umfasst Schlüssel-Lebenszyklus, Kontrolle der Schlüsselverwaltung, Offenlegung Infrastruktur, Verwaltung und Geschäftspraktiken.

8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Werden bei einem Audit von T-Systems Mängel oder Fehler festgestellt, wird entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer geeignete Maßnahmen. Der Leiter Trust Center ist verantwortlich für die Entwicklung eine Maßnahmenplans. Die Umsetzung der Maßnahmen ist in einem wirtschaftlich angemessenen Zeitraum durch zu führen. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 30 Tagen ein Korrekturplan erstellt und die Abweichung innerhalb eines wirtschaftlich angemessen Zeitraums behoben werden. Bei weniger schwerwiegenden Defiziten entscheiden der Leiter Trust Center über den Zeitrahmen der Behebung.

9 Sonstige geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

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

9.2 Finanzielle Verantwortlichkeiten

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

9.3 Vertraulichkeit von Geschäftsdaten

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

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

9.4 Datenschutz von Personendaten

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

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

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

9.5 Urheberrecht

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

9.6 Haftungsausschluss

Trotz größter Sorgfalt bei der Erstellung dieser Dokumentation können die Deutsche Telekom AG oder die T-Systems Enterprise Services GmbH die Möglichkeit nicht vollständig ausschließen, dass Fehler in den hier beschriebenen Richtlinien enthalten sind. Für diesen Fall lehnen die Deutsche Telekom AG sowie die T-Systems Enterprise Services GmbH jegliche Haftung ab.

9.7 Haftungsbeschränkungen

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf eine vorsätzliche Pflichtverletzungen zurückführen sind, wird gegenüber der Zertifizierungsstelle unbegrenzt gehaftet.

Im Übrigen wird im Rahmen der gesetzlichen Möglichkeiten die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen einzelvertraglich gegenüber der Zertifizierungsstelle begrenzt oder ausgeschlossen.

9.8 Schadensersatz

9.9 Inkrafttreten und Aufhebung

9.10 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Für individuelle Mitteilungen und Absprachen mit den Zertifizierungsstellen werden die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben. Außerdem ist eine Kontaktaufnahme über das Servicedesk (+49 1805 268 204 oder telesec_support@t-systems.com) möglich.

9.11 Gegenseitige Benachrichtigung und Mitteilungen von Teilnehmern

Die Teilnehmer kommunizieren untereinander.

9.12 Änderungen des CPS

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich die T-Systems Enterprise Services GmbH das Recht vor, Änderungen und Anpassungen dieses CPS durchzuführen. Änderungen des CPS gelten von dem Moment an, in dem sie in Kraft tritt. Das CPS tritt innerhalb von sechs Wochen nach Veröffentlichung (siehe Kapitel 2.2) der Änderungen in Kraft, außer für den Fall, dass die Veröffentlichung einen anderen Zeitraum vorsieht.

Falls das T-Systems Change Advisory Board der Ansicht ist, dass gravierende z.B. sicherheitsrelevante Änderungen unverzüglich erforderlich sind, dann tritt die neue Dokumentversion unverzüglich mit der Veröffentlichung in Kraft.

9.12.1 Verfahren für Änderungen

Änderungen des CPS können nur von T-Systems Change Advisory Board durchgeführt werden. Bei jeder Änderung des CPS wird deren Versionsnummer und Datum erneuert.

9.12.2 Benachrichtigungen

Nachgelagerte Zertifizierungsstellen werden über Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch ein zu legen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion nach Ablauf der Frist in Kraft. Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Im Fall von Unstimmigkeiten ist von den Parteien ein Eskalationsverfahren durchzuführen.

9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist Frankfurt /Main.

10 Glossar

ARL	Siehe Authority Revocation List.
Authority Revocation List	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
CA	Certification Authority. Siehe Zertifizierungsstelle.
Certificate Policy	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Revocation List	Siehe Sperrliste.
Certification Authority	Siehe Zertifizierungsstelle.
Certification Practice Statement	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um .
Chipkarte	Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.
CP	Siehe Certificate Policy.
CPS	Siehe Certification Practice Statement.
CRL	Certificate Revocation List. Siehe Sperrliste.
CV Zertifikat	card verifiable Zertifikat: Zertifikat in einem Tag/Value Format (kein X.509 Format)
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Digitales Zertifikat	Datensatz, der den Namen einer Person oder eines Systems, deren öffentlichen Schlüssel, gegebenenfalls einige andere Angaben und eine Signatur einer Zertifizierungsinstanz enthält.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
DN	Siehe Distinguished Name.
DMZ	Demilitarisierte Zone: dabei handelt es sich um einen geschützten Rechnerverbund, der sich zwischen 2 Netzwerken befindet. Der Rechnerverbund wird jeweils durch einen Paketfilter gegen das dahinterstehende Netz abgeschirmt.
Dual Key	Variante, bei der für Verschlüsselung und Signatur getrennte Schlüsselpaare verwendet werden, das heißt, ein Benutzer besitzt zwei entsprechende Zertifikate.
Elektronische Signatur	Siehe digitale Signatur.
Hardware Security Modul	Hardwarebox zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hash-Wert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.

HSM	Siehe Hardware Security Modul.
ISIS-MTT	Gemeinsame Spezifikation von TeleTrust und T7 Gruppe für elektronische Signaturen, Verschlüsselung und Public Key Infrastrukturen
Key Recovery	Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert.
Kompromittierung	Ein geheimer Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
LDAP	Siehe Lightweight Directory Access Protocol.
LDAP-Server	Server, der Informationen speichert, die über LDAP abrufbar sind.
Lightweight Directory Access Protocol	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Mail-Request	Variante eines Zertifikatsauftrags, bei dem die Daten per E-Mail an die Zertifizierungsinstanz übermittelt werden.
OCSP	Das Online Certificate Status Protocol ermöglicht die Online-Abfrage der Gültigkeit von Zertifikaten.
PIN	Personal Identification Number. Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.
PKI	Siehe Public-Key-Infrastruktur.
PKIX	Public Key Infrastructure X.509. Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
PKS	Public Key Service. Service des T-Systems Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Policy	Richtlinien, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
PSE	Personal Security Environment. In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Public-Key-Infrastruktur	Gesamtheit der Komponenten, Prozesse und Konzepte, die zur Verwendung von Public-Key-Verfahren verwendet werden. Typischerweise besteht eine Public-Key-Infrastruktur aus zentralen Komponenten wie einer Zertifizierungsinstanz und einem Verzeichnisdienst und verschiedenen Client-Komponenten.
RA	Registration Authority. Siehe Registrierungsstelle.
Registration Authority	Siehe Registrierungsstelle.
Registrierungsstelle	Komponente, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten.
Root CA	Siehe Wurzelzertifizierungsstelle.

RSA	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
SCEP	Simple Certificate Enrollment Protocol. Protokoll zur Beauftragung und zum Laden von Zertifikaten in IPSec Devices.
S/MIME	Secure Multipurpose Internet Mail Extension. Erweiterung des E-Mail-Formats MIME, die Zusätze für kryptografische Dienste beschreibt, welche Authentizität, Integrität und Vertraulichkeit von Nachrichten sicherstellen.
Schlüssel	Ein Schlüssel bezeichnet in der Kryptografie eine geheime Information (geheimer Schlüssel) oder ein öffentliches Gegenstück dazu (öffentlicher Schlüssel). Es gibt Verfahren, bei denen jeweils mit dem gleichen geheimen Schlüssel ver- und entschlüsselt wird sowie Verfahren bei denen ein öffentlicher Schlüssel zum Ver- und ein geheimer zum Entschlüsseln verwendet wird.
Secure Socket Layer	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet. Kann ihn vielen Fällen statt dem komplexeren IPSec verwendet werden.
SigG	Signaturgesetz
SigV	Signaturverordnung
Signatur	Siehe digitale Signatur.
Single Key	Variante, bei der für Verschlüsselung und Signatur das selbe Schlüsselpaar verwendet wird, das heißt, ein Benutzer besitzt ein Zertifikat.
Smart Card	Chipkarte mit Rechenfunktionalität, die für kryptografische Zwecke verwendet werden kann.
SOAP	Simple Object Access Protocol: SOAP stellt einen einfachen Mechanismus zum Austausch von strukturierter Information zwischen Anwendungen in einer dezentralisierten, verteilten Umgebung zur Verfügung.
Software-PSE	Durch Verschlüsselung geschützte Datei zur Speicherung des privaten Schlüssels eines Benutzers.
Sperrinstanz	Komponente, die Zertifikatssperrungen durchführt.
Sperrliste	Liste, in der gesperrte digitale Zertifikate aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats sollte anhand einer Sperrliste überprüft werden, ob dieses noch verwendet werden darf. Wird auch als Certificate Revocation List (CRL) bezeichnet.
SSL	Siehe Secure Socket Layer.
Verzeichnisdienst	Datenspeicher, der den Abruf von Zertifikaten und Informationen über Zertifikate (insbesondere Sperrlisten) ermöglicht.
Web-Request	Variante eines Zertifikatsauftrags, bei dem die Daten über ein Web-Formular an die Zertifizierungsinstanz übermittelt werden.
Wurzelzertifizierungsstelle	Oberste Zertifizierungsinstanz einer CA-Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsinstanz ausgestellt wurde, sondern selbstsigniert ist.
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zertifikat	Siehe digitales Zertifikat.
Zertifizierungsstelle	Komponente, die digitale Zertifikate ausstellt, indem sie einen Datensatz bestehend aus öffentlichem Schlüssel, Name und verschiedenen anderen Daten digital signiert. Ebenso werden von der Zertifizierungsstelle Sperrinformationen herausgegeben.

Zertifikatsnehmer	Instanz, die ein Zertifikat und den dazu gehörenden privaten Schlüssel verwendet.
Zuständigkeitsbereich	Teilbereich in der CA Administrationshierarchie, der von einem RA Operator verwaltet wird.

11 Referenzen

BDSG]	Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66.
[EU-RL]	Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 1999/93/EG, EU, 1999
[PKCS]	RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“, http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC2527]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 1999
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften, Bundesgesetzblatt I 2001, S. 876
[SigV]	Signaturgesetzverordnung, „Verordnung zur elektronischen Signatur“, BGBl. I S. 3074, 21.November 2001
[TSYSROOTSIGN]	Leistungsbeschreibung T-Systems Root Signing
[X.509]	Information technology - Open Systems Interconnection - The Directory:authentication framework, Version 3, ITU, 1997