Zertifizierungsrichtlinie für die T-Systems Trust Center Public Key Infrastrukturen

Certificate Policy, CP

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
T-Systems-Root-CP-V1.5_DE.doc	1.3.6.1.4.1.7879.13.18	Certificate Policy, CP

Version	Stand	Status
1.5	17.04.2009	Freigegeben

Autor	Inhaltlich geprüft von	Freigegeben von
T-Systems Enterprise Services GmbH Trust Center Services	L. Eickholt	A. Treßel
	15.04.2009	17.04.2009

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

Kurzinfo

Certificate Policy für die T-Systems Trust Center Public Key Infrastrukturen

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
1.0	14.01.2003	L. Eickholt	Ursprungsversion
1.1	01.06.2006	A. Klenk	Gliederung gemäß RFC3647 und verschiedene inhaltliche Aktualisierungen
1.2	02.03.2007	L.Eickholt	Inhaltliche Aktualisierungen
1.3	15.08.2007	L. Eickholt, M. Graf	Inhaltliche Aktualisierungen
1.4	13.09.2007	L. Eickholt, M. Ulm	Kapitel 9.13 eingefügt, Kapitel 9.14 aktualisiert, Kapitel 4.6 ergänzt, Kapitel 3.1.3 aktualisiert, Kapitel 3.3 aktualisiert, Kapitel 4.9.2 ergänzt, Kapitel 4.9.3 aktualisiert, Kapitel 5.8 aktualisiert, Kapitel 8 komplett überarbeitet, Kapitel 9.5 ergänzt, Kapitel 9.9 geändert in Kapitel 9.12, 9.12.1 und 9.12.2 hinzu gefügt
1.5	17.04.2009	L. Eickholt, S. Kölsch	Kapitel 1.1 aktualisiert, Kapitel 1.3.2.1 aktualisiert, Kapitel 1.3.3.1 ergänzt, Kapitel 1.4 Gliederung aktualisiert, Kapitel 1.5.2 aktualisiert, Kapitel 2.2 aktualisiert, Kapitel 4.1.2.1 ergänzt, Kapitel 4.9.1 aktualisiert, Kapitel 5 aktualisiert, Kapitel 6 aktualisiert, Kapitel 8 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.

Bei dem vorliegenden Dokument handelt es sich um die **Zertifizierungsrichtlinie** (engl. Certificate Policy, kurz **CP**) für die Dienstleistungen des T-Systems Trust Centers. Im Folgenden wird es als die **T-Systems Trust Center CP** bezeichnet.

Die T-Systems Trust Center CP beschreibt das hohe Sicherheitsniveau aller Trust Center Dienstleistungen und beinhaltet Sicherheitsvorgaben sowie Richtlinien hinsichtlich technischer, organisatorischer und rechtlicher Aspekte. Sie findet Anwendung auf alle Zertifikats-Dienstleistungen unter T-Systems Root-Instanzen, die vom T-Systems Trust Center angeboten werden, mit Ausnahme von Testdiensten, die dazu dienen, Kunden Testmöglichkeiten für Schnittstellen und Zertifikatsabläufe zu bieten. Diese Testdienste stehen unter explizit deklarierten Test-Zertifizierungsstellen zur Verfügung, sind daher klar identifizierbar, und werden im Folgenden nicht weiter betrachtet.

Das T-Systems Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Root-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. Die konkrete Abbildung der T-Systems Trust Center CP im Rahmen einer Zertifizierungsstelle ist jeweils in einem separaten Certification Practice Statement (CPS) niedergelegt. Ein solches 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 berücksichtigt die Anforderungen aus [RFC3647].

1.1 Überblick

Das T-Systems Trust Center ist seit 1996 nach DIN ISO 9002 und seit Januar 2001 nach DIN EN ISO 9001:2000 zertifiziert.

Im Jahr 1998 hat das T-Systems Trust Center (unter der Bezeichnung „Trust Center der Deutschen Telekom“) den Betrieb als erster Zertifizierungsdiensteanbieter aufgenommen, der über eine Akkreditierung nach dem deutschen Signaturgesetz (SigG) verfügt.

Zusätzlich zu den genau festgelegten und zertifizierten Arbeitsabläufen zeichnet sich das T-Systems Trust Center durch einen sehr hohen Sicherheitsstandard aus. Die Vertrauenswürdigkeit des eingesetzten Trust Center Personals ist durch öffentliche Stellen überprüft worden. Alle Dienste sind Gegenstand regelmäßiger Qualitäts-

kontrollen. Die eingesetzte Technologie ist Stand der Technik und wird laufend durch ausgebildete Administratoren überwacht.

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 T-TeleSec Public Key Service (PKS), der die Ausstellung qualifizierter Zertifikate gemäß dem deutschen Signaturgesetz (SigG) umfasst.

Im Einzelnen behandelt die T-Systems Trust Center CP 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:	Zertifizierungsrichtlinie für die T-Systems Trust Center Public Key Infrastrukturen
Version:	1.5
Datum	17.04.2009
Objektbezeichnung (Object Identifier)	1.3.6.1.4.1.7879.13.18

1.3 PKI Beteiligte

Die unten aufgeführten Kapitel stellen alle Dienste, die im T-Systems Trust Center betrieben werden, dar. Die nicht unter diese Policy fallenden Dienste sind explizit gekennzeichnet.

1.3.1 Zertifizierungsstellen

Das T-Systems Trust Center betreibt eine Anzahl unterschiedlicher Zertifizierungsstellen zur Ausgabe qualifizierter und fortgeschrittener Zertifikate. Darüber hinaus 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 qualifizierte Zertifikate

Die Root-CA Instanz wird von der Bundesnetzagentur (vormals „Regulierungsbehörde für Telekommunikation und Post“) als zuständiger Aufsichtsbehörde im Sinne des deutschen Signaturgesetzes (SigG) betrieben. Die Root-CA Zertifikate werden von der Bundesnetzagentur regelmäßig neu ausgegeben und veröffentlicht, und erlauben eine Gültigkeitsüberprüfung aller in dieser Hierarchie ausgestellten Zertifikate.

Im T-Systems Trust Center werden unterhalb dieser Root CA Instanz verschiedene Zertifizierungsstellen für qualifizierte Zertifikate betrieben. Die Struktur dieser Zertifizierungsstellen ist in der folgenden Abbildung schematisch dargestellt:

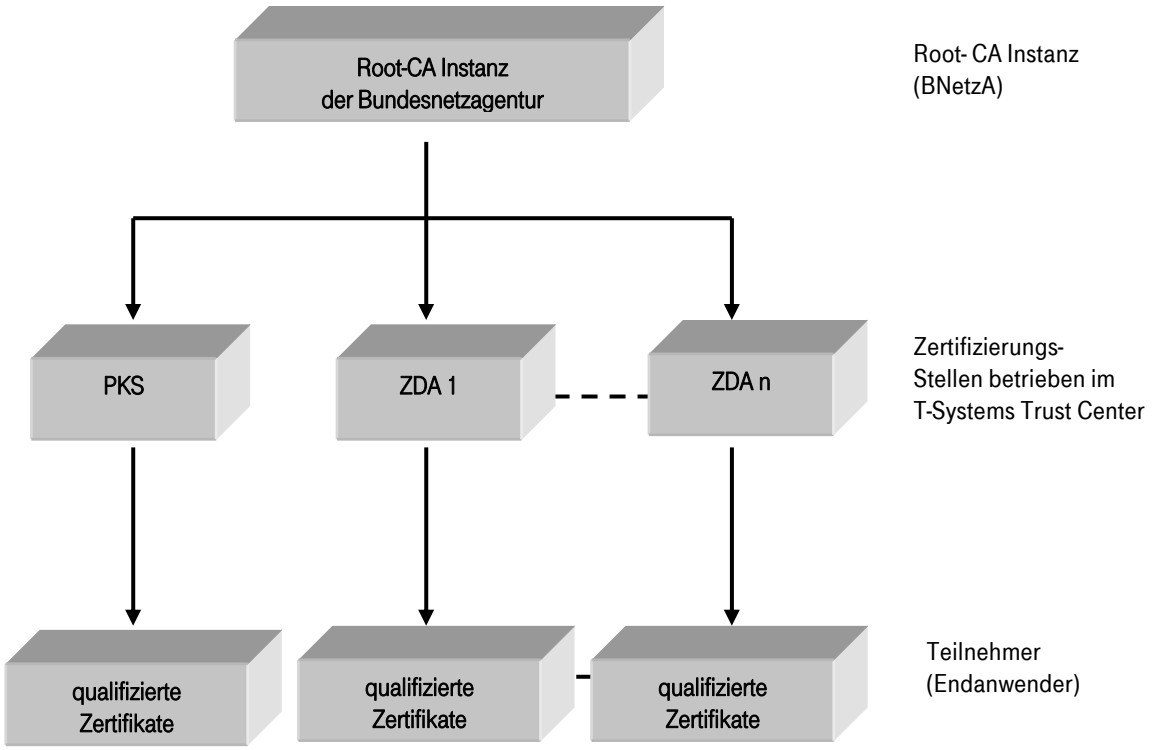

Abbildung 1: Zertifizierungsstellen für qualifizierte Zertifikate

Jede Zertifizierungsstelle verfügt über mehrere von der Bundesnetzagentur ausgestellte CA- und Dienste-Zertifikate, die in regelmäßigen Abständen neu ausgegeben werden.

Der T-TeleSec Public Key Service für qualifizierte Zertifikate, in der obigen Abbildung kurz mit PKS bezeichnet, stellt gemäß deutschem Signaturgesetz qualifizierte Zertifikate personengebunden an Endanwender aus.

Parallel dazu betreibt das T-Systems Trust Center weitere Zertifizierungsstellen für qualifizierte Zertifikate im Auftrag von Kunden, die in der Abbildung mit ZDA 1 bis ZDA n bezeichnet sind.

Die dargestellten, von T-Systems betriebenen Zertifizierungsstellen für qualifizierte Zertifikate, unterliegen nicht dieser CP.

1.3.1.2 Zertifizierungsstellen für fortgeschrittene Zertifikate

1.3.1.2.1 Zertifizierungsstellen für fortgeschrittene Zertifikate unter eigenen Root-CA Instanzen

Das T-Systems Trust Center betreibt eine Reihe von Root-CA Instanzen für fortgeschrittene Zertifikatsdienste. Die Root-CA Zertifikate sind selbst-signierte Zertifikate, und werden durch die T-Systems veröffentlicht. Die Veröffentlichung erlaubt eine Gültigkeitsüberprüfung aller in diesen Hierarchien ausgestellten Zertifikate.

Im T-Systems Trust Center werden unterhalb dieser Root-CA Instanzen verschiedene Zertifizierungsstellen für fortgeschrittene Zertifikate betrieben. Darüber hinaus stellt das T-Systems Trust Center CA-Zertifikate für andere Betreiber von Zertifizierungsstellen aus. Die Struktur ist in der folgenden Abbildung schematisch dargestellt:

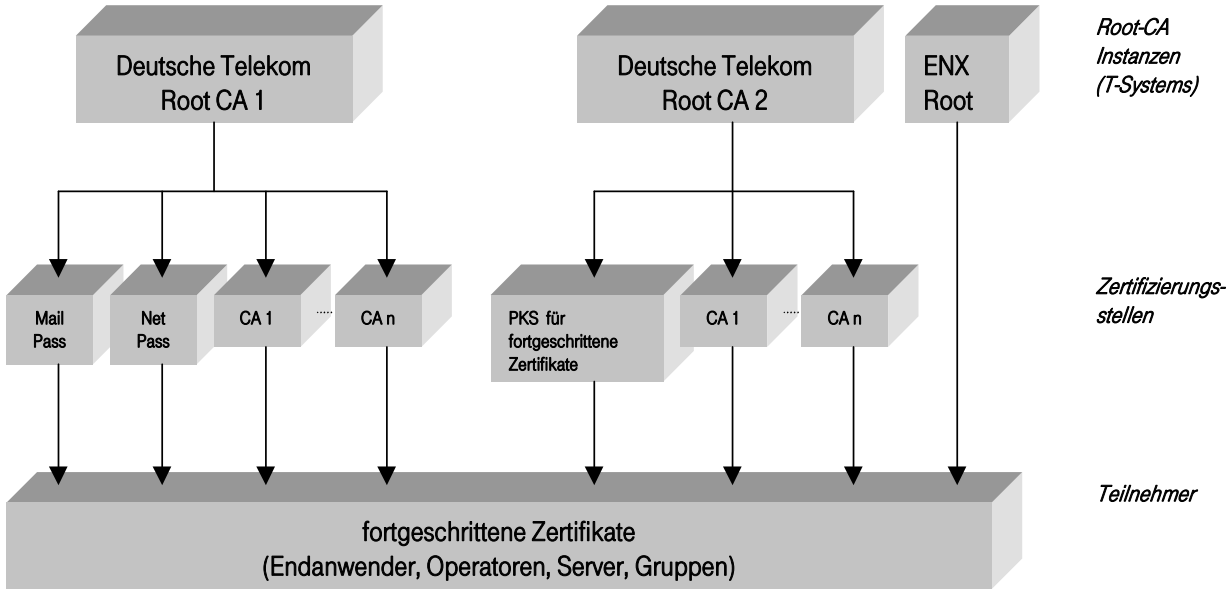

Abbildung 2: Zertifizierungsstellen für fortgeschrittene Zertifikate unter eigenen Root-CA Instanzen

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.

Die dargestellten und von T-Systems oder anderen Betreibern betriebenen Zertifizierungsstellen für fortgeschrittene Zertifikate unterliegen dieser CP.

1.3.1.2.2 Zertifizierungsstellen für fortgeschrittene Zertifikate unter der Verwaltungs-PKI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betreibt mit der "PCA-1-Verwaltung" eine Wurzelzertifizierungsstelle für die öffentliche Verwaltung. Von ihr können sich interessierte Zertifizierungsstellen von Bund, Ländern und Kommunen CA Zertifikate ausstellen lassen. Die Root-CA Zertifikate werden vom BSI regelmäßig neu ausgegeben und veröffentlicht, und erlauben eine Gültigkeitsüberprüfung aller in dieser Hierarchie ausgestellten Zertifikate. Die Root-CA Instanz zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen.

Das T-Systems Trust Center betreibt im Auftrag von Kunden eine Reihe von fortgeschrittenen Zertifikatsdiensten innerhalb dieser Hierarchie der Verwaltungs-PKI. Die Struktur ist in der folgenden Abbildung schematisch dargestellt:

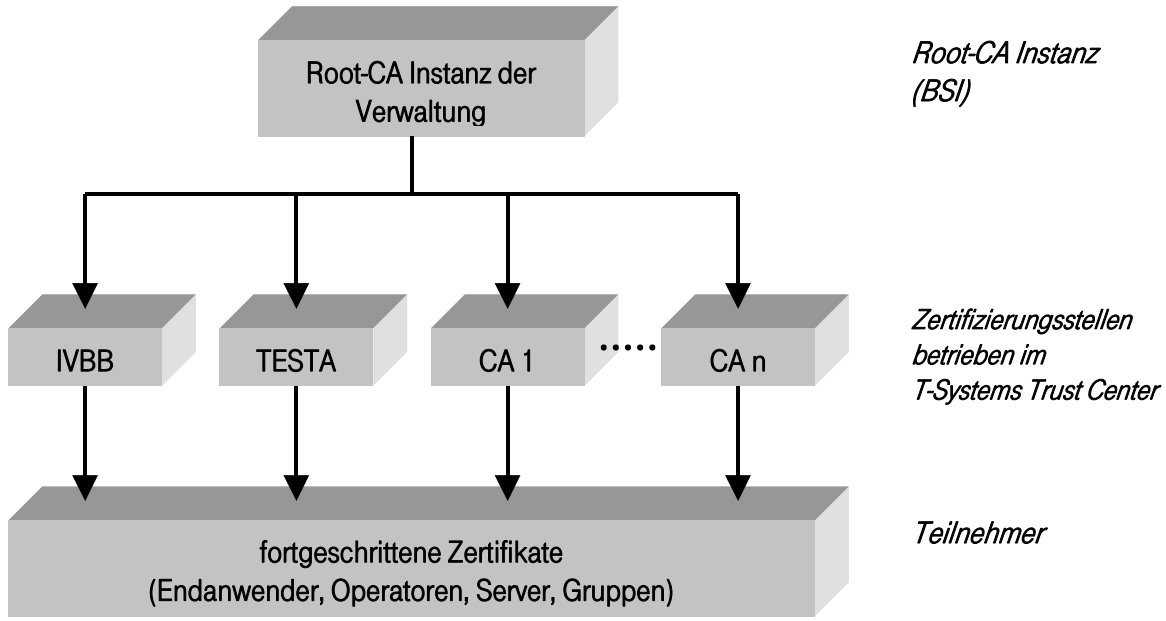

Abbildung 3: Zertifizierungsstellen für fortgeschrittene Zertifikate unter der Verwaltungs-PKI

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

Die dargestellten und von T-Systems betriebenen Zertifizierungsstellen für fortgeschrittene Zertifikate unterliegen nicht dieser CP.

1.3.1.2.3 Zertifizierungsstellen für fortgeschrittene Zertifikate unter externen Root-CA Instanzen

Im Fall der Zertifizierungsstellen für Serverzertifikate (z.B. SSL Server, Mail Server) wird aufgrund der stärkeren Verbreitung in verschiedenen Clientanwendungen derzeit unter extern betriebenen Root-CA Instanzen gearbeitet.

Die Struktur ist in der folgenden Abbildung schematisch dargestellt:

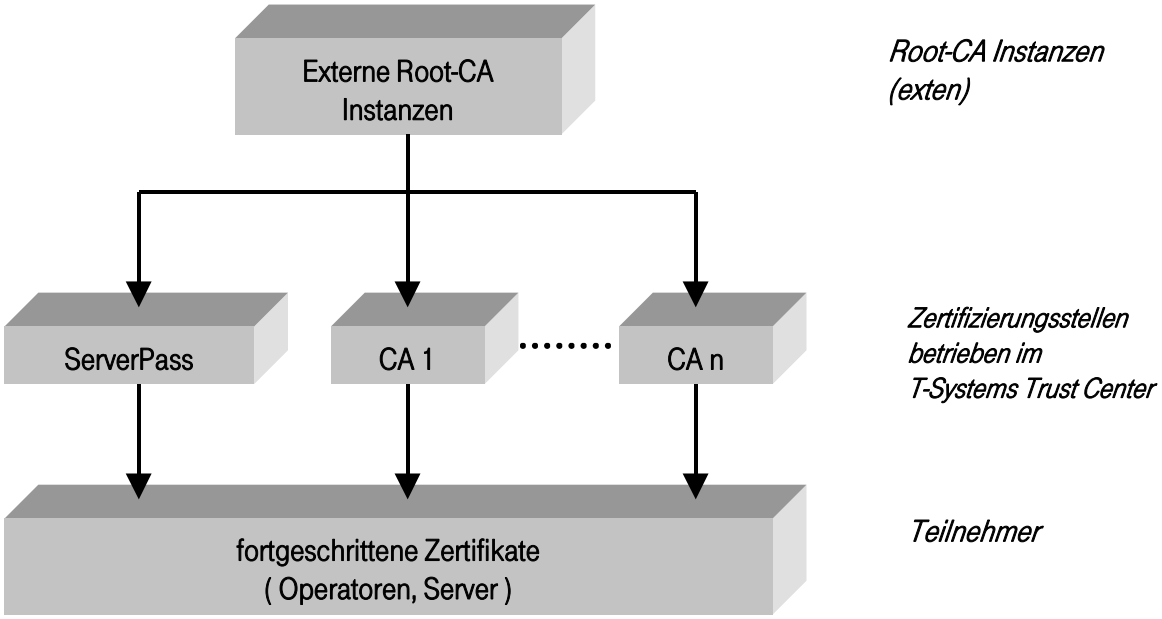

Abbildung 4: Zertifizierungsstellen für fortgeschrittene Zertifikate unter sonstigen externen Root-CA Instanzen

Jede Zertifizierungsstelle verfügt über ein oder mehrere von externe Root-CA Instanzen ausgestellte CA-Zertifikate, die in regelmäßigen Abständen neu ausgegeben werden.

Die dargestellten und von T-Systems betriebenen Zertifizierungsstellen für fortgeschrittene Zertifikate unterliegen nicht dieser CP.

1.3.1.2.4 Zertifizierungsstellen für fortgeschrittene Zertifikate unter externen Root-CA Instanzen, die im Trust Center betrieben wird

T-Systems betreibt als Dienstleister im Kundenauftrag die IT-Systeme und das Application Management für deren Root-CA.

Die dargestellten und von T-Systems betriebenen Zertifizierungsstellen für fortgeschrittene Zertifikate unterliegen nicht dieser CP.

1.3.2 Registrierungsstellen

Jeder Zertifizierungsstelle sind eine oder mehrere Registrierungsstellen zugeordnet. Es gibt keine Begrenzung hinsichtlich der Anzahl der zugeordneten Registrierungsstellen. Eine Registrierungsstelle ist der zugeordneten Zertifizierungsstelle unterstellt, und agiert als vorgelagerte Schnittstelle zu den Teilnehmern der PKI. Die Registrierungsstellen sind daher ebenso dieser Trust Center CP untergeordnet.

Bei der Mehrzahl der Zertifizierungsstellen gibt es eine Hierarchiebildung innerhalb der zugeordneten Registrierungsstellen in eine oder mehrere übergeordnete und eine oder mehrere nachgeordnete Registrierungsstellen. Jede nachgeordnete Registrierungsstelle ist genau einer übergeordneten Registrierungsstelle zugeordnet.

Aufgaben von übergeordneten Registrierungsstellen sind

- die Zulassung und der Widerruf nachgeordneter Registrierungsstellen,
- die Zuordnung des jeweiligen Verantwortungsbereiches einer nachgeordneten Registrierungsstelle (für welche Teilmenge der Teilnehmeraufträge ist die Registrierungsstelle verantwortlich?),
- die Sperrung bzw. Suspension von Teilnehmerzertifikaten über alle Verantwortungsbereiche.

Aufgaben von nachgeordneten Registrierungsstellen sind

- die Registrierung von Teilnehmern innerhalb des definierten Verantwortungsbereiches,
- Prüfung von Teilnehmeraufträgen innerhalb des definierten Verantwortungsbereiches gemäß der Richtlinien der jeweiligen Zertifizierungsstelle (ggf. unter Zuhilfenahme beglaubigter oder mit Dienstsiegeln versehener Identifikationsdokumente),
- nach erfolgreicher Prüfung die Freigabe oder andernfalls die Ablehnung dieser Teilnehmeraufträge,
- in Folge der Freigabe eines Teilnehmerauftrags der Auftrag an die Zertifizierungsstelle zur Ausstellung und Auslieferung des Teilnehmerzertifikats,
- die Entgegennahme und Prüfung von Aufträgen auf Zertifikatssperrung oder –suspension innerhalb des definierten Verantwortungsbereiches (falls Suspension im Rahmen der jeweiligen Zertifizierungsstelle vorgesehen ist),
- in Folge der Freigabe eines Sperr- oder Suspensionsauftrags der Auftrag an die Zertifizierungsstelle zur Sperrung bzw. Suspension des Teilnehmerzertifikats.

Wird keine Hierarchiebildung der Registrierungsstellen vorgenommen, erfüllen die Registrierungsstellen gleichrangig die Aufgaben der nachgeordneten Registrierungsstellen, ohne dass eine Trennung in Verantwortungsbereiche vorliegt.

Die Registrierungsstellen werden mit der notwendigen Technologie ausgestattet. Die Mitarbeiter der Registrierungsstellen authentifizieren sich sicher gegenüber der jeweiligen Zertifizierungsstelle.

Die Regelungen und Prozesse bzgl. der Registrierungsstellen sind in den jeweiligen CPS Dokumenten der Zertifizierungsstellen detailliert beschrieben.

1.3.2.1 Registrierungsstellen bei CA-Verkettung

Wird eine nicht-T-Systems-eigene CA 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, an Endanwender oder Mitarbeiter von Registrierungsstellen (RA Operatoren), an Server (Maschinen oder Programme) oder an Gruppen vergeben werden.

Der Zertifikatsnehmer

- beauftragt das Zertifikat (im Fall von juristischen Personen, Servern oder Gruppen 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.

Im Fall von natürlichen Personen als Zertifikatsnehmer wird im folgenden auch von Zertifikatsinhabern gesprochen.

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, Server, Gruppen oder Organisationen, die Zertifikate von Zertifikatsnehmern im Rahmen von Anwendungen nutzen. Im Zuge der Nutzung muss eine Gültigkeitsüberprüfung der Zertifikate durch Zugang zu Veröffentlichungsdiensten der Zertifizierungsstellen und Auswertung von Sperrinformationen erfolgen.

1.3.5 Andere Teilnehmer

Teilnehmer, die keine vertragliche Beziehung haben, die eine in Kapitel 1.3.1.2.1 dargestellte Root betreffen, werden in dieser Richtlinie nicht betrachtet.

1.4 Zertifikatsverwendung

1.4.1 Erlaubte Zertifikatsverwendung

1.4.1.1 Qualifizierte Zertifikate

Qualifizierte Zertifikate werden für qualifizierte Signaturen im Sinne des deutschen Signaturgesetzes eingesetzt. Attribut-Zertifikate beschränken den Verwendungszweck des zugehörigen Schlüsselzertifikats oder enthalten zusätzliche Informationen über den Zertifikatsinhaber des zugehörigen qualifizierten Schlüsselzertifikats.

1.4.1.2 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.

1.4.1.3 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 Richtlinie

1.5.1 Zuständigkeit für die Richtlinie

Diese CP wird von T-Systems Enterprise Services GmbH, ITO - AL Region – PSS - Security Solutions - Trust Center Services herausgegeben.

1.5.2 Kontaktperson

Adresse:

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

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

1.5.3 Pflege der Richtlinie

Diese Richtlinie 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 einer CPS

Die in Kapitel 1.5.1 benannte für diese Richtlinie zuständige Instanz ist ebenso zuständig für die Bescheinigung der Konformität der CPS einer Zertifizierungsstelle zu dieser Richtlinie.

1.6 Definitionen und Abkürzungen

Siehe Kapitel 9 (Glossar).

2 Veröffentlichung und Verantwortlichkeiten für den Verzeichnisdienst

2.1 Verzeichnisdienst

Jede dieser Richtlinie unterliegende Zertifizierungsstelle stellt ihren Zertifikatsnutzern durch den Verzeichnisdienst mindestens einen Zugriff auf die Sperrdaten zur Verfügung. Werden die Sperrdaten in Form einer Sperrliste (CRL) bereitgestellt, sind die jeweiligen Bezugsadressen dem Attribut „CRL Distribution Point" der Teilnehmerzertifikate zu entnehmen. Werden die Sperrdaten in Form eines OCSP Dienstes bereitgestellt, sind die jeweiligen Bezugsadressen dem Attribut „authority information access" der Teilnehmerzertifikate zu entnehmen.

Darüber hinaus wird per Verzeichnisdienst den Zertifikatsnehmern –und nutzern auch der Zugriff auf die Sperrdaten der herausgebenden Root-CA bereitgestellt, soweit diese Root-CA vom T-Systems Trust Center betrieben wird. Werden die Sperrdaten in Form einer Sperrliste (CRL) bereitgestellt, sind die jeweiligen Bezugsadressen dem Attribut „CRL Distribution Point" des CA Zertifikats zu entnehmen. Werden die Sperrdaten in Form eines OCSP Dienstes bereitgestellt, sind die jeweiligen Bezugsadressen dem Attribut „authority information access" des CA Zertifikats zu entnehmen.

Eine dieser Richtlinie unterliegende Zertifizierungsstelle kann darüber hinaus die Teilnehmerzertifikate im Verzeichnisdienst zugänglich machen. Falls dabei personenbezogene Daten publiziert werden, die dem Datenschutz unterliegen, geschieht dies nicht ohne Einwilligung der betroffenen Personen.

Details sind der jeweiligen CPS zu entnehmen.

2.2 Veröffentlichung von Informationen

Jede dieser Richtlinie unterliegende Zertifizierungsstelle stellt ihren Zertifikatsnehmern –und nutzern weiterhin mindestens folgende Informationen auf den Webseiten der Zertifizierungsstelle zur Verfügung:

- das jeweilige Root-CA Zertifikat (zusätzlich auch per Verzeichnisdienst) und dessen Fingerprint,
- das jeweilige CA Zertifikat (zusätzlich auch per Verzeichnisdienst) und dessen Fingerprint,
- 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,
- relevante Abschnitte der jeweiligen CPS ,

- Leistungsbeschreibung & Anforderungsprofil „T-Systems Root Signing“ zur Ausstellung von Root-Zertifikaten (CA-Verkettung),

2.3 Update der Informationen / Veröffentlichungsfrequenz

Neu ausgestellte Zertifikate, Sperrinformationen, Richtlinien und ggf. weitere Informationen werden zeitnah zur Verfügung gestellt. Es gelten die folgenden Veröffentlichungsfrequenzen:

- Falls der jeweilige Zertifizierungsdienst die Veröffentlichung von Teilnehmerzertifikaten vorsieht, werden Zertifikate umgehend nach der Ausstellung und der ggf. erforderlichen Zustimmung des Zertifikatsnehmers in den Verzeichnisdienst eingestellt.
- Sperrinformationen für Teilnehmerzertifikate werden zeitnah, mindestens jedoch täglich aktualisiert.
- Sperrinformationen für CA Zertifikate werden im Fall einer Sperrung umgehend aktualisiert.
- Richtlinien und sonstige Informationen werden nach Bedarf aktualisiert.

Details sind der jeweiligen CPS zu entnehmen.

2.4 Zugang zu den Informationsdiensten

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

Der lesende Zugriff auf die in Abschnitt 2.2 aufgeführten Informationen auf den Webseiten einer Zertifizierungsstelle ist für die Zertifikatsnehmer zu gewährleisten. Die Webseiten können einer Zugangskontrolle unterliegen, um Zugriffe unberechtigter Personen zu unterbinden.

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.

Details über verpflichtende und optionale Attribute im Subject DN und Subject Alternative Name sind der jeweiligen CPS zu entnehmen.

3.1.2 Aussagekräftigkeit von Namen

Der Name muss den Zertifikatnehmer eindeutig identifizieren.

Details sind der jeweiligen CPS zu entnehmen.

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 Pseudonym an die zuständigen Stellen soweit dies der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Auflagen der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erfor-

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

Details sind der jeweiligen CPS zu entnehmen.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Der zu verwendende Zeichensatz und die Substitutionsregelungen für Sonderzeichen sind der jeweiligen CPS zu entnehmen.

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.

Die Namen von Zertifikatsnehmern müssen innerhalb einer Zertifizierungsstelle eindeutig sein. Es ist gleichwohl möglich, dass ein Zertifikatsnehmer mehrere Zertifikate mit gleichem Namen hat (z.B. im Fall von Schlüsseltrennung Zertifikate mit verschiedenen key usages, oder im Fall von Zertifikatserneuerung).

Details sind der jeweiligen CPS zu entnehmen.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Sofern sich der DN eines Zertifikats explizit auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen nicht relevant. In allen anderen Fällen liegt es in der Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Die Zertifizierungsstellen sind 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. Details sind der jeweiligen CPS zu entnehmen.

Diese Anforderung gilt nicht, wenn die Schlüsselerzeugung bei der Zertifizierungsstelle stattfindet.

3.2.2 Authentifizierung einer Organisation

Die Authentifizierung von Organisationen ist nur für Zertifizierungsstellen für fortgeschrittene Zertifikate relevant. Sie findet nach den in der jeweiligen CPS dargelegten Anforderungen statt. Siehe hierzu auch Kapitel 3.2.5.

3.2.3 Authentifizierung einer natürlichen Person

Die Authentifizierung natürlicher Personen findet nach den in der jeweiligen CPS dargelegten Anforderungen statt. Jede Zertifizierungsstelle nimmt in geeigneter Weise eine zuverlässige Überprüfung mindestens derjenigen Auftragsdaten vor, die in das Zertifikat eingehen.

3.2.4 Nicht verifizierte Endteilnehmer Informationen

Nicht verifizierte Endteilnehmer Informationen sind Informationen, die ohne Prüfung ins Zertifikat übernommen werden. Details sind der jeweiligen CPS zu entnehmen.

3.2.5 Unterschriftenvollmacht

Die Autorisierung einer natürlichen Person als handlungsberechtigt im Namen einer Organisation oder natürlichen Person muss durch ein adäquates, in der CPS beschriebenes Verfahren erfolgen. Dies gilt insbesondere im Fall von Funktions-, Gruppen-, Maschinen- oder Serverzertifikaten, oder im Fall von Zertifikatsaufträgen, die von einer Registrierungsinstanz gestellt werden.

3.3 Identifizierung und Authentifizierung bei Folge-Beauftragungen

Rechtzeitig vor Ablauf der Gültigkeit des Zertifikats wird der Zertifikatsnehmer in geeigneter Weise unter Verwendung der beim Erstauftrag hinterlegtenKundendaten benachrichtigt.

Eine Zertifizierungsstelle kann die Möglichkeit einer automatisierten Authentifizierung eines Folgeauftrags anhand einer Signatur mit dem noch gültigen Zertifikat der gleichen Zertifizierungsstelle vorsehen. Ist dieses „Vorgänger"-Zertifikat jedoch abgelaufen oder gesperrt, muss ein Neuauftrag gestellt werden.

Details sind der jeweiligen CPS zu entnehmen.

3.4 Identifizierung und Authentifizierung bei Sperraufträgen

Zur Sperrung autorisierte Personen und Institutionen (siehe Kapitel 4.9) können die Sperrung eines Zertifikates entweder per Brief, per Fax, oder telefonisch beauftragen.

Die Authentisierung einer Sperrung geschieht in geeigneter Art und Weise. Es wird empfohlen, ein Sperrpasswort zu verwenden, das im Rahmen der Zertifikatsbeauftragung bzw. Auslieferung in geeigneter Weise festgelegt und sicher an den Zertifikatsnehmer übermittelt wird.

Die zur Sperrung zu verwendenden Telefonnummern, Faxnummern, Webseiten oder Adressen sind zu veröffentlichen.

Details sind der jeweiligen CPS zu entnehmen.

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.

Ein geeignetes Verfahren für den Nachweis der Autorisierung muss dokumentiert sein. Einzelheiten regelt die CPS der Zertifizierungsstelle.

4.1.2 Registrierungsprozess

Ein Zertifikat kann erst erzeugt werden, wenn der Registrierungsprozess bei einer der Zertifizierungsstelle zugeordneten Registrierungsstelle erfolgreich abgeschlossen wurde. Der Registrierungsprozess beinhaltet mindestens die folgenden Schritte:

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

Im Fall eines Folgeauftrags kann ein abweichender automatisierter Registrierungsprozess (siehe Kapitel 3.3) erfolgen. Der Registrierungsprozess für Erst- und Folgeaufträge muss im CPS einer Zertifizierungsstelle vollständig beschrieben sein.

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 wird im zugehörigen CPS beschrieben.

4.2 Bearbeitung des Zertifikatsauftrags

4.2.1 Durchführung der Identifikation und Authentifizierung

Die zuständige Registrierungsstelle führt die Identifizierung und Authentifizierung gemäß den Festlegungen der CPS durch. Im Fall eines Folgeauftrags kann eine automatische Identifikation und Authentifizierung anhand einer gültigen Signatur (siehe Kapitel 3.3) erfolgen.

4.2.2 Annahme oder Abweisung von Zertifikatsaufträgen

Die zuständige Registrierungsstelle führt die vollständige Überprüfung der Auftragsdaten gemäß den Festlegungen der CPS durch. Nur bei erfolgreicher Überprüfung wird ein Zertifikatsauftrag angenommen und zur Bearbeitung weitergeleitet.

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

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer variiert in Abhängigkeit von den in der jeweiligen CPS definierten Prozessen. Die CPS sollte eine Aussage zur zu erwartenden Bearbeitungsdauer machen.

4.3 Ausstellung von Zertifikaten

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

Die Zertifizierungsstelle erhält in der Regel in elektronischer Form oder im Fall qualifizierter Zertifikate auch in Schriftform geprüfte Aufträge von einer zuständigen Registrierungsstelle. Die Kommunikation mit der Registrierungsstelle wird mit geeigneten Verfahren sicher authentifiziert; diese sind in der CPS zu beschreiben.

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.

Einzelheiten sind der jeweiligen CPS zu entnehmen.

4.3.2 Benachrichtigung des Zertifikatsnehmers

Der Zertifikatsnehmer erhält eine Benachrichtigung über die Ausstellung des Zertifikats in geeigneter Weise. Falls auf Seiten der Zertifizierungsstelle nur für den Zertifikatsnehmer bestimmte vertrauliche Informationen wie Sperrpassworte oder Downloadpassworte erzeugt wurden, werden diese in geeigneter Art und Weise sicher

und vertraulich an den Zertifikatsnehmer übermittelt. Es bestehen je nach Zertifizierungsstelle verschiedene Möglichkeiten der Auslieferung des Zertifikats:

- der Zertifikatsnehmer lädt sich sein Zertifikat, ggf. unter Verwendung eines Downloadpassworts
- die zuständige Registrierungsstelle lädt das Zertifikat und leitet es in geeigneter Weise an den Zertifikatsnehmer weiter,
- das ausgestellte Zertifikat wird an den Zertifikatsnehmer per Mail gesendet,
- das ausgestellte Zertifikat wird an den Zertifikatsnehmer per Datenträger (Chipkarte) auf dem Postweg gesendet.

Einzelheiten müssen in der jeweiligen CPS festgelegt werden.

4.4 Zertifikatsannahme

4.4.1 Akzeptanz durch den Zertifikatsnehmer

Abhängig von der CPS der Zertifizierungsstelle kann eine explizite Annahmebestätigung des Zertifikatsnehmers an die Zertifizierungsstelle erforderlich sein.

Beispielsweise gelten qualifizierte Zertifikate erst als gültig gemäß dem deutschen Signaturgesetz, nachdem eine solche Bestätigung erfolgt ist, und daraufhin das Zertifikat im Verzeichnisdienst aktiviert ist.

Einzelheiten müssen in der jeweiligen CPS festgelegt werden.

4.4.2 Veröffentlichung des Zertifikats

Es gelten die Regelungen aus Kapitel 2.1.

4.4.3 Benachrichtigung weiterer Instanzen

Eine explizite Benachrichtigung weiterer Instanzen ist im Fall von Teilnehmerzertifikaten die Ausnahme. Es kann im Einzelfall entsprechende Benachrichtigungen geben, die dann in der jeweiligen CPS zu beschreiben sind.

4.5 Verwendung von Schlüsselpaar und Zertifikat

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Verantwortlichkeiten des Zertifikatsnehmers sind im CPS der Zertifizierungsstelle zu dokumentieren, und dem Zertifikatsnehmer in geeigneter Weise mitzuteilen. Dies kann insbesondere die Verpflichtung zum Schutz

des privaten Schlüssels oder zur unverzüglichen Beauftragung der Sperrung im Fall einer Kompromittierung des Schlüssels beinhalten.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Relying Parties

Jeder, der ein Zertifikat, welches im Rahmen dieser CP ausgestellt wurde, zur Überprüfung einer Signatur oder für die Zwecke der Authentifizierung oder Verschlüsselung verwendet, 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 der 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

Zulässigkeit und Bedingungen für die Zertifikatserneuerung sind im jeweiligen CPS zu regeln. In der Regel ist eine Zertifikatserneuerung nur bei Ablauf der Gültigkeit des vorhandenen Zertifikats zulässig. Rechtzeitig vor Ablauf der Gültigkeit des Zertifikats sollte der Zertifikatsnehmer in geeigneter Weise benachrichtigt werden.

4.6.2 Wer darf eine Zertifikatserneuerung beauftragen?

In der Regel wird eine Zertifikatserneuerung nur durch den Zertifikatsnehmer beauftragt.

4.6.3 Ablauf der Zertifikatserneuerung

Der Ablauf ist in der CPS zu beschreiben. 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 Identifikationsdaten oder Inhalte von Attributen des Zertifikats ändern (z. B. bei der Namensänderung in Folge einer Eheschließung) 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 führen zu einer Sperrung des Zertifikats:

- Abhandenkommen des privaten Schlüssels (z. B. Verlust oder Diebstahl einer Chipkarte).
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor.
- Die Angaben im Zertifikat sind nicht mehr korrekt.
- Der zertifizierte Schlüssel oder die damit verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.
- Es liegt ein Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen vor.
- 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.

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,
- sperrberechtigte Dritte (z.B. autorisierte Personen im Fall von Maschinenzertifikaten, siehe Kapitel 3.2.5 und 3.4),
- das T-Systems Trust Center gemäß den Allgemeinen Geschäftsbedingungen oder aus Gründen, die in der CPS der Zertifizierungsstelle benannt sein müssen.
- die Registrierungsstelle

Details sind dem jeweiligen CPS zu entnehmen.

4.9.3 Ablauf einer Sperrung

Zur Sperrung autorisierte Personen und Institutionen können die Sperrung eines Zertifikates entweder per Brief, per Fax, oder telefonisch beauftragen. Inwieweit eine Suspendierung (Sperrgrund „on-hold“) zulässig ist, regelt die CPS.

Die Authentisierung einer Sperrung geschieht in geeigneter Art und Weise. Es wird empfohlen, ein Sperrpasswort zu verwenden, das im Rahmen der Zertifikatsbeauftragung bzw. Auslieferung in geeigneter Weise festgelegt und sicher an den Zertifikatsnehmer übermittelt wurde.

Sind die Voraussetzungen zur Sperrung erfüllt, wird die Sperrung vorgenommen, und das gesperrte Zertifikat in die Sperrinformationen übernommen. Sperrinformationen müssen in standard-konformer Form (CRL und/oder OCSP) bereitgestellt werden.

Die zur Sperrung zu verwendenden Telefonnummern, Faxnummern, Webseiten oder Adressen sind zu veröffentlichen.

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

Details sind der jeweiligen CPS zu entnehmen.

4.9.4 Fristen für einen Sperrauftrag

Der Zertifikatsnehmer bzw. autorisierte Dritte sollten bei Vorliegen entsprechender Gründe unverzüglich die Sperrung initiieren. Falls es definierte Fristen gibt, sind diese in der CPS festzulegen.

4.9.5 Fristen für die Zertifizierungsstelle

Festlegungen hinsichtlich der Bearbeitung von Sperraufträgen regelt die jeweilige CPS. Nach Möglichkeit sollte die Bearbeitung unverzüglich erfolgen.

4.9.6 Methoden zur Prüfung von Sperrinformationen

Sperrinformationen werden in standardisierter Form (CRL und/oder OCSP-Abfrage) bereitgestellt und können daher mit Standard-konformen Anwendungen geprüft werden. Die genauen Festlegungen sind in der CPS zu treffen.

4.9.7 Frequenz der Veröffentlichung von Sperrinformationen

Die Frequenz der Veröffentlichung von Sperrinformationen ist in der CPS festzulegen. Eine zeitnahe Verfügbarkeit der Sperrinformationen soll gewährleistet sein.

4.9.8 Maximale Latenzzeit von Sperrlisten

Die maximale Latenzzeit für Sperrlisten ist in der CPS festzulegen.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Sperrinformationen müssen für die Zertifikatsnutzer online mit einem standard-konformen Verfahren bereitgestellt werden. Dabei müssen alle von einer Zertifizierungsstelle ausgegebenen Zertifikate erfasst sein.

Die Online Überprüfungsverfahren sollten eine möglichst hohe Verfügbarkeit aufweisen.

4.9.10 Anforderungen an Online Überprüfungsverfahren

Die für die Nutzung der Online Sperrinformationen notwendigen Informationen (z.B. URL der Sperrliste oder des OCSP Responders) müssen in geeigneter Weise bekannt gemacht werden (siehe hierzu auch Kapitel 2.1). Die genauen Festlegungen sind in der CPS zu treffen.

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 Gründe für eine Suspendierung von Zertifikaten

Ob eine Suspendierung (Sperrgrund „on-hold“) für eine Zertifizierungsstelle zulässig ist, und falls ja, aus welchen Gründen, regelt die CPS.

4.9.14 Wer kann suspendieren?

Falls eine Suspendierung für eine Zertifizierungsstelle zulässig ist, sind die genauen Festlegungen hierzu in der CPS zu treffen.

4.9.15 Ablauf einer Suspendierung

Falls eine Suspendierung für eine Zertifizierungsstelle zulässig ist, sind die genauen Festlegungen hierzu in der CPS zu treffen.

4.9.16 Begrenzung der Suspendierungsperiode

Falls eine Suspendierung für eine Zertifizierungsstelle zulässig ist, sind die genauen Festlegungen hierzu in der CPS zu treffen.

4.10 Statusauskunftsdienste für Zertifikate

4.10.1 Verfahrensmerkmale

Wenn ein Statusauskunftsdienst (z.B. OSCP) zur Verfügung steht, ist dies in der CPS zu beschreiben.

4.10.2 Verfügbarkeit

Wenn ein Statusauskunftsdienst (z.B. OSCP) zur Verfügung steht, sollte er eine möglichst hohe Verfügbarkeit aufweisen.

4.10.3 Optionale Merkmale

Wenn ein Statusauskunftsdienst (z.B. OSCP) zur Verfügung steht und dieser über optionale Merkmale verfügt, sind diese in der CPS zu beschreiben.

4.11 Kündigung durch den Zertifikatsnehmer

Im Falle der Kündigung des Vertragsverhältnisses durch den Zertifikatsnehmer muss eine Sperrung des Zertifikats erfolgen.

4.12 Schlüsselhinterlegung und Wiederherstellung

Im Fall von Zertifizierungsstellen für fortgeschrittene Zertifikate sind die Zulässigkeit der Hinterlegung und Wiederherstellung von Schlüsseln festzulegen. Falls zulässig, sind die technischen und organisatorischen Abläufe im CPS zu dokumentieren.

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).

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 und Endteilnehmer 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 und im Fall qualifizierter Zertifikate von einer unabhängigen Stelle überprüft worden. Die verwendete Netzwerk- und IT-Technologie entspricht dem aktuellen Stand der Technik. 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 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.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

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

Im Fall von CA Zertifikaten für Signaturgesetz-konforme Zertifizierungsstellen handelt es sich um einen evaluierten Schlüsselgenerator und ein evaluiertes und nach Signaturgesetz bestätigtes Speichermedium. Der private Schlüssel wird direkt nach der Generierung gespeichert, und kann nach der Speicherung nicht mehr ausgelesen werden.

Im Fall von Benutzerzertifikaten von Signaturgesetz-konformen Zertifizierungsstellen handelt es sich um einen evaluierten Schlüsselgenerator und ein evaluiertes und nach Signaturgesetz bestätigtes Speichermedium. Der private Schlüssel wird direkt nach der Generierung gespeichert, und kann nach der Speicherung nicht mehr ausgelesen werden.

Im Fall von Root-CA und CA Zertifikaten für fortgeschrittene Zertifizierungsstellen werden die privaten Schlüssel auf einem sicherheitsüberprüften Hardware Security Module (zum Beispiel FIPS oder entsprechend evaluiert) erzeugt und abgelegt.

Im Fall von Benutzerzertifikaten von fortgeschrittenen Zertifizierungsstellen können bei Bedarf die gleichen hochwertigen Generierungs- und Speichermechanismen eingesetzt werden.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Im Fall von Benutzerzertifikaten von Signaturgesetz-konformen Zertifizierungsstellen wird der private Schlüssel auf einem evaluierten und nach Signaturgesetz bestätigten Speichermedium ausgeliefert.

Im Fall von Benutzerzertifikaten von fortgeschrittenen Zertifizierungsstellen können bei Bedarf die gleichen hochwertigen Speichermedien eingesetzt und ausgeliefert werden.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Öffentliche Schlüssel werden in Form signierter PKCS#10 Requests auf einem sicheren Speichermedium an andere Zertifikatsherausgeber ausgeliefert.

6.1.4 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).

6.1.5 Schlüssellängen

Die verwendeten Schlüssellängen von Root CA-, CA- und Teilnehmerzertifikaten sind in den CPS Dokumenten der Zertifizierungsstellen festgelegt. Sie orientieren sich am aktuellen Stand der Technik.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Die Festlegung der Parameter der öffentlichen Schlüssel von Root CA-, CA- und Teilnehmerzertifikaten und ggf. anzuwendende Qualitätskontrollen sind in den CPS Dokumenten der Zertifizierungsstellen festgelegt. Sie orientieren sich am aktuellen Stand der Technik.

6.1.7 Schlüsselverwendungen

Die Schlüsselverwendungen der Root CA-, CA- und Teilnehmerzertifikate sind im Attribut „key usage“ festzulegen.

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.

Die Schlüsselverwendungen der Teilnehmerzertifikate sind in der CPS einer Zertifizierungsstelle festzulegen.

6.2 Sicherung privater Schlüssel

Im Fall von CA Zertifikaten für Signaturgesetz-konforme Zertifizierungsstellen werden die privaten Schlüssel auf einem evaluierten und nach Signaturgesetz bestätigten Speichermedium direkt nach der Schlüsselgenerierung und ohne Anfertigung einer Sicherungskopie abgelegt. Ein privater Schlüssel kann nach der Speicherung nicht mehr ausgelesen, und daher auch nicht nachträglich gesichert werden. Die Verwendung des privaten Schlüssels wird durch eine PIN geschützt. Die PINs der Speichermedien, die in einer Zertifizierungsstelle eingesetzt werden, werden in verschlüsselter Form im CA System gespeichert, so dass keine natürliche Person über das Wissen der PINs verfügt.

Im Fall von Benutzerzertifikaten von Signaturgesetz-konformen Zertifizierungsstellen werden die privaten Schlüssel auf einem evaluierten und nach Signaturgesetz bestätigten Speichermedium direkt nach der Schlüsselgenerierung und ohne Anfertigung einer Sicherungskopie abgelegt. Ein privater Schlüssel kann nach der Speicherung nicht mehr ausgelesen, und daher auch nicht nachträglich gesichert werden.

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

Im Fall von Benutzerzertifikaten von fortgeschrittenen Zertifizierungsstellen können bei Bedarf die gleichen hochwertigen Generierungs- und Speichermechanismen eingesetzt werden, die Sicherungskopien von Schlüsseln verhindern. Zugriffsschutz ist über eine persönliche PIN gegeben.

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung von öffentlichen Schlüsseln

Im Rahmen von routinemäßig durchgeführten Sicherungsverfahren werden die Daten gesichert und archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren sind in den CPS Dokumenten der Zertifizierungsstellen festgelegt.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatsprofile

7.1.1 Zertifikatsprofil der Root Zertifikate

7.1.1.1 Zertifikatsprofil Deutsche Telekom Root CA 1

Zertifikatsfeld	Inhalt		Bemerkungen
Version	v3		
SerialNumber	24		Hexadezimal (Dezimal 36)
SignatureAlgorithmIdentifier	RSA, MD5		
Issuer			
Country Name	DE		
Organization Name	Deutsche Telekom AG		
Organizational Unit Name 1	T-TeleSec Trust Center		
Common Name	Deutsche Telekom Root CA 1		
Validity			
Not Before	9.7.1999 11:34		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 1		
SubjectPublicKeyInfo			
Algorithm	<OID für RSA>		
Subject Public Key	<Schlüssel>		Schlüssellänge: 1024 Bit
Extensions			
Subject Key Identifier	non critical	1431 E27F 9CCA 1295 FBF1 7020 DB4D 2813 7142 61C6	

Zertifikatsfeld	Inhalt		Bemerkungen
Basic Constraints	non critical	CA=1	
		PathLenConstraint=5	
Key Usage	critical	keyCertSign, cRLSign	

7.1.1.2 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 critical	CA=1	
		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

Sperrlistenprofile werden in der CPS einer Zertifizierungsstelle definiert.

7.3 Profile von Online-Statusabfragen

7.3.1 Profil von Online-Statusabfragen der Root Zertifikate

Online-Statusabfragen für von T-Systems betriebene Root-CA-Zertifikate werden derzeit nicht unterstützt.

7.3.2 Profil von Online-Statusabfragen der Zertifizierungsstellen

Profile von Online-Statusabfragen für Teilnehmerzertifikate werden in der CPS einer Zertifizierungsstelle definiert, sofern diese Online-Statusabfragen unterstützt. Online-Statusabfragen für CA-Zertifikate werden derzeit nicht unterstützt.

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. Weitergehende Regelungen sind im jeweiligen CPS zu finden.

8.1 Intervall von Prüfungen

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

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

Art und Umfang der Haftungsbeschränkungen sind dem jeweils gültigem Certification Practice Statement zu entnehmen.

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 die Supportline (0800/835372 oder t-telesec@t-systems.com) möglich.

9.11 Gegenseitige Benachrichtigung und Mitteilungen von Teilnehmern

Die Teilnehmer kommunizieren untereinander.

9.12 Änderungen der CP oder 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 an CP und CPS durchzuführen. Änderungen an CP und CPS gelten von dem Moment an, in dem sie in Kraft treten. Die CP/ das

CPS tritt innerhalb von sechs Wochen nach Veröffentlichung 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 der CP oder des CPS können nur von T-Systems Change Advisory Board durchgeführt werden. Bei jeder Änderung der CP oder 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	Richtlinien 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