T-TeleSec ServerPass

Certificate Practice Statement CPS

Version: 3.4
Status: final

Business flexibility T · · Systems · · ·

Business flexibility T · · Systems · · ·

Impressum

Herausgeber

T-Systems Enterprise Services GmbH
ITO - AL Region-PSS - Security Solutions - Trust Center Services
Untere Industriestraße 20

57250 Netphen

Ansprechpartner	Telefon	E-Mail
Support Line	Tel: 0800 8 3 5 3 7 3 2 Tel: 0800 T e l e S e c	T-TeleSec@t-systems.com

Kurzinfo

Änderungshistorie

Dok.Vers.	Status	Ersch.Datum	Autor	Bemerkungen
1.0	ungültig	28.11.2000	BREU	Initialversion
2.0	ungültig	01.09.2001	EICK	Aufnahme Erneuerung
2.1	ungültig	01.12.2001	EICK	Anpassung Kapitel 10
3.0	ungültig	11.11.2003	EICK	Aktualisierung der Zertifikatshierarchie, Überarbeitung inhaltlich, Layoutänderungen
3.1	ungültig	01.12.2003	EICK	Aktualisierung der Zertifikatshierarchie
3.2	ungültig	21.02.2005 09:00 (GMT)	EICK	Aktualisierung der Zertifikatshierarchie, Überarbeitung inhaltlich
3.3	ungültig	09.02.2006	EICK	Aktualisierung der Zertifikatshierarchie Inhalt überarbeitet
3.4	gültig	04.05.2007	EICK	Layoutanpassung, Aktualisierung Kapitel 14

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Konzerneinheit T-Systems Enterprise Services GmbH, ITO - AL Region – PSS - Security Solutions - Trust Center Services betreibt das Trust Center der Deutschen Telekom, das 1997 nach ISO 9002 und 2000 nach ISO 9001:2000 zertifiziert wurde. Es wird im Folgenden als „T-Systems Trust Center“ bezeichnet.

Bereits 1998 wurde dem Trust Center die Genehmigung zum Betrieb einer Zertifizierungsinstanz nach Signaturgesetz erteilt. Zusätzlich zu den genau festgelegten und zertifizierten Arbeitsabläufen zeichnet sich das T-Systems Trust Center durch einen sehr hohen Sicherheitsstandard aus. Alle vom T-Systems Trust Center angebotenen Dienstleistungen werden von sicherheitsüberprüftem Personal ausgeführt und unterliegen einer ständigen Qualitätskontrolle.
Die eingesetzte Technologie ist sehr leistungsfähig und wird laufend durch ausgebildete Administratoren überwacht.

2 Bedeutung der CPS

Das Certification Practice Statement (CPS) beschreibt die Tätigkeiten des Trust Center Betreibers in der Funktion als Certification Authority (CA) und Registration Authority (RA). In Ergänzung zu den AGB werden die Verfahrensweisen, wie T-TeleSec ServerPass im Rahmen der zertifikatsbasierten Public Key Infrastruktur (PKI) ausgestellt und verwaltet werden, beschrieben.
Das CPS in der vorliegenden Version spiegelt den aktuellen Status der Zertifizierungsabläufe wider und gilt ausschließlich für das Produkt T-TeleSec ServerPass.

Es beschreibt im Einzelnen:

- die Bedeutung und Verwendung von Zertifikaten,
- die Erstellung von Zertifikaten,
- das Sperren von Zertifikaten,
- das Erneuern von Zertifikaten,
- die Verwaltung von Zertifikaten,
- die Haftung,
- die Sicherheit.

Das CPS ermöglicht aufgrund der vorliegenden Beschreibungen die qualitative Einschätzung der Dienstleistung.

3 Allgemeines zum T-TeleSec ServerPass

Der T-TeleSec ServerPass macht einen Internetserver identifizierbar und bindet eine Firmenidentität daran. Er setzt sich zusammen aus den geprüften Angaben des Zertifikatsinhabers, dem öffentlichen Schlüssel des Servers, Daten zum Aussteller des Zertifikates sowie der Signatur der T-Systems Trust Center Zertifizierungsinstanz.
Durch die Möglichkeit der Verschlüsselung (SSL) wird für die Sicherheit der Kommunikation gesorgt. Die Verschlüsselungsstärke richtet sich nach den Möglichkeiten des Servers und des Browsers.

4 Technische Anforderungen für T-TeleSec ServerPass

T-TeleSec ServerPass kann von Komponenten benutzt werden, welche X.509v3 Zertifikate korrekt interpretieren und verwenden können. Das Profil des X.509 Zertifikates für T-TeleSec ServerPass ist in einem separaten Abschnitt beschrieben (siehe Kapitel 12).

5 Benutzung und Zweck des T-TeleSec ServerPass

T-TeleSec ServerPass darf nur zur Authentifizierung der Kommunikation des entsprechenden Servers genutzt werden. Die sichere Kommunikation erfolgt mittels SSL - Sicherheitsstandard.

6 Haftung

Die Haftung ist in den Allgemeinen Geschäftsbedingungen (AGB) für T-TeleSec ServerPass beschrieben.

7 Pflichten

7.1 Rolle und Pflichten des Trust Centers

Das T-Systems Trust Center handelt als Certification Authority (CA) und Registration Authority (RA). Das Trust Center in der Rolle als CA generiert und signiert den T-TeleSec ServerPass und die dazugehörigen Sperrlisten. Ferner verwaltet und archiviert das Trust Center den T-TeleSec ServerPass und die Sperrlisten.
In der Rolle als RA werden Aufträge zur Ausstellung, Sperrung und Erneuerung entgegen genommen und geprüft. Die RA kann Aufträge autorisieren oder ablehnen.

7.2 Pflichten des Kunden

Die Pflichten und Obliegenheiten des Kunden entnehmen Sie bitte den Allgemeinen Geschäftsbedingungen (AGB) für T-TeleSec ServerPass.

8 Beauftragung

8.1 Art der Beauftragung

Die Beauftragung des T-TeleSec ServerPass erfolgt ausschließlich mit dem Online-Auftrag. Während der Onlinebeauftragung wird eine Papierversion des Auftrages erzeugt.
Die unterschriebene Papierversion des Auftrages, Onlinedaten sowie Identifikationspapiere vervollständigen den Auftrag.

8.2 Ablaufübersicht

Der T-TeleSec ServerPass wird für den Zeitraum von 1 Jahr (+ 5 Tage Kulanzzeitraum) ausgestellt und wie folgt beauftragt:

- Server-Zertifikat-Request wird durch den Kunden erzeugt (siehe Kapitel 8.3)
- Eingabe der Kundendaten inkl. Server-Zertifikat-Request auf den Webseiten (Online-Auftrag)
- Absenden der Daten
- Ausdrucken des Auftrages und Unterzeichnen durch Zeichnungsberechtigte(n) (es wird nur der vom T-Systems Trust Center vorgegebene, ausgedruckte und unterschriebene Auftrag akzeptiert)
- Identifikationsdokumente beifügen (siehe Kapitel 9)
- Evtl. benötigtes Zusatzdokument (siehe Kapitel 9.2) beilegen
- Unterlagen auf dem Postweg an das Trust Center senden

8.3 Hinweise zum Server-Zertifikat-Request

Beim Server-Zertifikat-Request handelt es sich um eine Zertifizierungsanfrage deren Syntax durch den Standard PKCS#10 beschrieben wird. Die Serverapplikationen stellen für die Erstellung geeignete Tools zur Verfügung. Die produktspezifischen Eigenarten sind bei der Erstellung des Requests zu beachten.
Beim Erzeugen des Server-Zertifikat-Requests auf dem Server werden definierte Felder (Common Name, Organization Name, Organizational Unit Name 1-..., State or Province, Locality, E-Mail, Phone, ...) abgefragt. Diese Felder können je nach Webserver variieren.
Folgende Datenfelder werden anhand beigefügter Identifikationspapiere (siehe Kapitel 9) geprüft und gehen in das Zertifikat ein.

Feldname	Inhalt	Beispiel	Optionen u. Prüfung
Organization Name	Organisation, Firma	Muster GmbH	optional, wenn ja (z. B. laut HRA)*
Organizational Unit Name 1 - 5	Organisationseinheit, Abt.	Abteilung EK	optional (nicht verifiziertes Feld)
street address	Straße	Musterstraße	optional, wenn ja (z. B. laut HRA)
Locality	Ort, Stadt	Musterhausen	optional, wenn ja (z. B. laut HRA)
State or Province	Bundesland	NRW	optional, wenn ja (z. B. laut HRA)
Postal Code	Postleitzahl	57072	optional, wenn ja (z. B. laut HRA)

Country	Land (Kürzel)	DE für Deutschland	Pflichtfeld, (z. B. laut HRA)
Common Name	Domain Name bzw. IP-Adresse	www.muster.de	Pflichtfeld, z. B. laut DENIC

Abbildung 1 (Übersicht der Datenfelder)

* bei Gewerbetreibenden steht hier entweder die Gewerbe treibende Person selbst mit Vor- und Nachname oder bei einem frei gewählten Firmennamen muss der Inhaber nachgestellt werden
z.B. Musterfirma Inh.: Erwin Mustermann.

Bitte verwenden Sie nur die folgenden Zeichen in den oben genannten Feldern des Server-Zertifikat-Requests.
a bis z, A bis Z, 0 bis 9 und die Sonderzeichen in der folgenden Tabelle:

Leerzeichen	
Ausrufezeichen	!
Hash	#
Dollar	$
Prozent	%
Ampersant	&
Hochkomma	´
runde Klammer auf	(
runde Klammer zu	)
Plus	+
Colon	,
Bindestrich	-
Punkt	.
Schrägstrich	/
Doppelpunkt	:
Semicolon	;
Kleiner	<
Gleichheitszeichen	=
Grösser	>
Fragezeichen	?
at	@
eckige Klammer auf	[
eckige Klammer zu	]
Unterstrich	_
Pipe	|

Abbildung 2 (Übersicht der gültigen Zeichen)

Nicht zugelassen werden von der CA alle Zeichen außerhalb der ASCII 7 Bit Kodierung, also insbesondere Umlaute, scharfes S und alle Arten von Akzenten, da Netscape und Microsoft Produkte unterschiedliche Kodierungen für Zeichen außerhalb der genannten Zeichenmenge unterstützen und somit Interoperabilitätsprobleme entstehen.
Platzhalter (z. B. *Stern) im sub-domain Namensfeld des Domainnamens werden nicht akzeptiert. Wildcard-Zertifikate werden nicht ausgestellt.

9 Benötigte Dokumente

Um die von Ihnen und uns geforderte Qualität der Zertifikate zu gewährleisten, werden neben dem Papierauftrag weitere Dokumente benötigt.

9.1 Wir benötigen vom Auftraggeber:

Bei der Erstbeauftragung unterscheiden wir folgende Fälle:

Auftraggeber ist eine juristische Person:
Die beglaubigte Kopie (nicht älter als 30 Tage) des Handelsregisterauszuges der juristischen Person oder den Auszug eines elektronischen Handelsregisters (Abrufdatum nicht älter als 30 Tage).
Auftraggeber ist eine Behörde: Dienstsiegel und die Unterschrift eines Bevollmächtigten der Behörde auf dem Auftragsformular.
Auftraggeber ist ein Verein: Die beglaubigte Kopie (nicht älter als 30 Tage) des Vereinsregisterauszuges.
Auftraggeber ist eine natürliche Person: Die beglaubigte Kopie (nicht älter als 30 Tage) eines Dokumentes, welches die (natürliche) Person als solche ausweist (z. B. beglaubigte Kopie des Bundespersonalausweises).
Auftraggeber ist ein Gewerbetreibender: Die beglaubigte Kopie (nicht älter als 30 Tage) eines aktuellen Gewerbescheins und des Personalausweises des Gewerbetreibenden.

9.1.1 Mehrfachbeauftragung

Werden mehrere Server-Zertifikate beauftragt, so benötigen wir keine weiteren Identifikationspapiere des Auftraggebers, sofern sich seit der letzten Beauftragung keine relevanten Zertifikatsangaben geändert haben.

9.2 In Ausnahmefällen benötigtes Zusatzdokument

9.2.1 Auftraggeber und Domaininhaber sind nicht identisch

Eine Vollmacht des Domain- oder des IP-Adresseninhabers. Die Vollmacht erlaubt dem Auftraggeber die Nutzung der Domain/ IP-Adresse. Die Vollmacht des Domain- oder des IP-Adresseninhabers schließt die Beauftragung, Speicherung, Erneuerung und Sperrung des T-TeleSec ServerPass ein. Verwenden Sie Ihr Geschäftspapier und benutzen Sie dazu den Wortlaut aus dem Vordruck: <Vollmacht des Domaininhabers>. Den Vordruck finden Sie auf unseren Internetseiten http://wwwca.telesec.de/Pub_Cert/ServPass/index.html unter dem Menüpunkt ‘AGB/Dokumente/Preise’.

9.2.2 Zeichnungsberechtigte(r) bevollmächtigt einen Dritten

In großen Unternehmen kann das Unterzeichnen des T-TeleSec ServerPass Auftrages durch einen Zeichnungsberechtigten zu organisatorisch bedingten, zeitkritischen Verzögerungen führen. Um diese Verzögerungen zu minimieren, kann ein(e) Zeichnungsberechtigte(r) einer/ mehreren Person/en eine Vollmacht für diesen speziellen, definierten Einzelfall (T-TeleSec ServerPass Beauftragung) ausstellen. Nur mit dieser Vollmacht wird die Unterschrift einer(s) Nichtzeichnungsberechtigten anerkannt.
Zur Vollmachterteilung verwenden Sie bitte Ihr Geschäftspapier und benutzen Sie dazu den Wortlaut des bereitgestellten Vordrucks: <Vollmacht zur Beauftragung>. Den Vordruck finden Sie auf unseren Internetseiten http://wwwca.telesec.de/Pub_Cert/ServPass/index.html unter dem Menüpunkt 'AGB/Dokumente/Preise'.

10 Identifikation und Authentifizierung

Dieses Kapitel beschreibt, welche Authentifizierungsmechanismen durchgeführt werden, bevor Zertifikate ausgestellt werden.

- Eingegangene Dokumente auf Echtheit und Vollständigkeit prüfen.
- Auftraggeber wird z.B. anhand der beglaubigten Kopie des Handelsregisterauszuges und oder vergleichbarer Dokumente identifiziert.
- Der Domain- oder IP-Adresseninhaber der im Feld (Common Name) genannten Domain oder IP-Adresse wird anhand einer öffentlichen Registrierungsstelle identifiziert.
- Die Mittelbarkeit zwischen Auftraggeber und Domain- oder IP-Adresseninhaber wird geprüft (evtl. anhand eines erforderlichen Zusatzdokumentes (siehe Kapitel 9.2.1)).
- Die im Server-Zertifikat-Request unter den Feldnamen (Organisation, Firma), (Ort) und (Land) gemachten Angaben werden mit den eingereichten Unterlagen verglichen.
- Die notwendige Mittelbarkeit zwischen Auftraggeber und der im Zertifikat genannten juristischen oder natürlichen Person wird geprüft.
- Rückruf zur Überprüfung des Auftraggebers, zur Klärung von Unstimmigkeiten oder zur Vervollständigung des Auftrages.

11 Operationale Anforderungen

11.1 Ausstellung von Zertifikaten

Nach positiver Prüfung des Auftrages wird das Zertifikat generiert. Das Zertifikat wird zusammen mit dem CA Zertifikat bzw. den CA Zertifikaten und dem Root Zertifikat bereitgestellt. Der im Auftrag genannte technische Ansprechpartner wird informiert.
Dieser kann über die Service Webseiten für T-TeleSec ServerPass mit Referenznummer und Abholpasswort das Zertifikat abholen.

11.2 Sperrung von Zertifikaten

Das Sperren von Zertifikaten ist in den Allgemeinen Geschäftsbedingungen (AGB) für T-TeleSec ServerPass beschrieben.
Gesperrte Zertifikate erscheinen in einer CRL, die alle 24 h von der CA aktualisiert wird.
Achtung: Die Sperrung eines Zertifikates ist endgültig und kann nicht aufgehoben werden!

11.3 Erneuerung von Zertifikaten

Der T-TeleSec ServerPass hat eine Gültigkeit von einem Jahr (+5Tage Kulanz). Da ein ausgegebenes Zertifikat nachträglich nicht mehr verändert werden kann, muss die Verlängerung der Gültigkeit durch eine erneute Ausstellung (Erneuerung) mit neuem Gültigkeitszeitraum durchgeführt werden.

Um die durchgehende Funktion des T-TeleSec ServerPass zu gewährleisten, muss die Erneuerung vor Ablauf der Gültigkeit durchgeführt werden. Die bevorstehende Möglichkeit der Erneuerung wird erstmals ca. 4 Wochen vor Ablauf des Zertifikates dem technischen Ansprechpartner per E-Mail mitgeteilt. Von diesem Zeitpunkt an bis zum Ablauf der Gültigkeit ist die Erneuerung mittels vereinfachter Beauftragung online über die Funktion <Zertifikat erneuern> unserer Internetseiten möglich.
Das Erneuerungszertifikat ist ab dem Zeitpunkt der Ausstellung für ein Jahr gültig. Das Überlassungsentgelt wird am Tag der Ausstellung in Rechnung gestellt.

Die Erneuerung des T-TeleSec ServerPass wird in der Regel ohne die erneute Prüfung der Kundenangaben durchgeführt. Das T-Systems Trust Center behält sich jedoch das Recht auf eine erneute Identitätsfeststellung, zum Beispiel auf Grund eventuell geänderter Sicherheitsanforderungen, vor.

12 Zertifikatsaufbau und -hierarchie

12.1 Hierarchie der GlobalSign Root CA

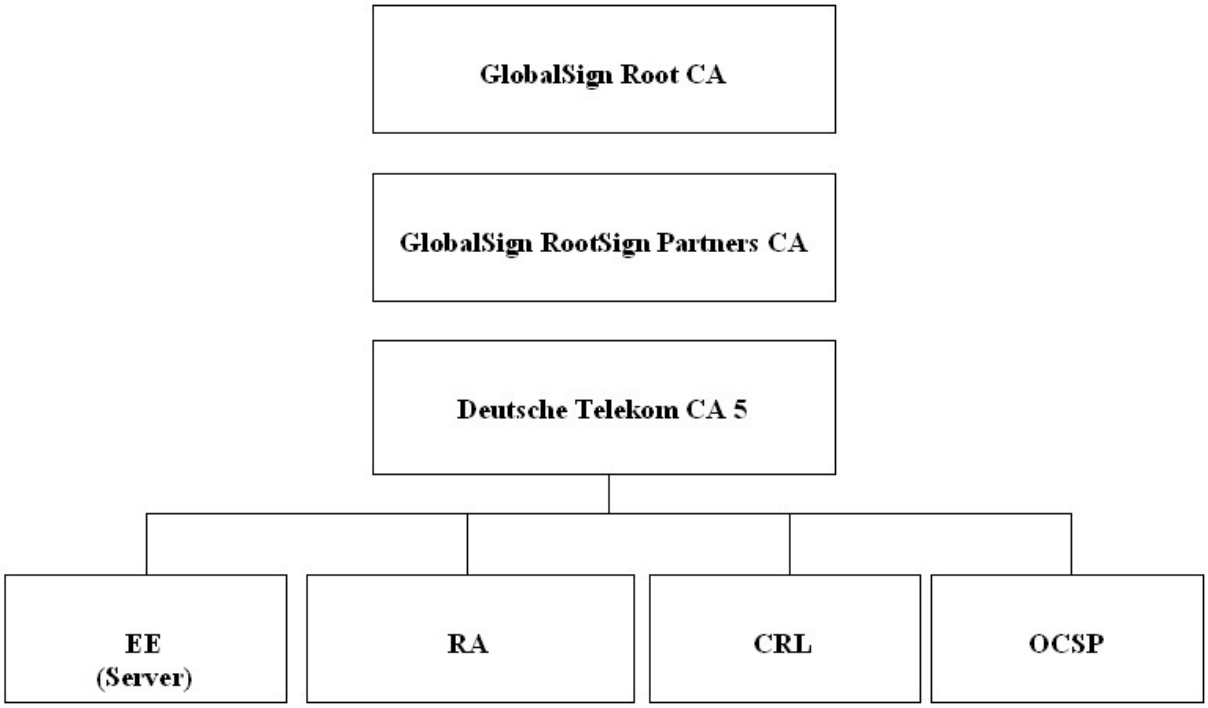

Abbildung 3 (CA Hierarchie ab 09.02.2006 unter der GlobalSign Root CA)

12.1.1 GlobalSign Root CA

Die GlobalSign Root CA nutzt einen Root Key mit einer Schlüssellänge von 2048 bit. Dieser Root Key wurde in sicherer Umgebung generiert und ist bis 2014 gültig. Das GlobalSign Root CA Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	Md5/RSA
Schlüssellänge	2048 bit
Aussteller des Zertifikates	GlobalSign nv-sa
Eigentümer des Zertifi-	GlobalSign nv-sa

kates	
Gültigkeitsdauer	not before Sep 1 12:00:00 1998 GMT not after Jan 28 12:00:00 2014 GMT
Seriennummer	2*(2^80) + 921148298245 (dez) 0x02:0000:0000:00d6:78b7:9405 (hex)
SignaturAlgorithmIdent	Md5/RSA

Zur Prüfung der Authentizität des GlobalSign Root CA Zertifikats kann folgender Fingerprint des Zertifikates herangezogen werden:

MD5: ABBF:EAE3:6B29:A6CC:A678:3599:EFAD:2B80
SHA-1: 2F17:3F7D:E996:67AF:A57A:F80A:A2D1:B12F:AC83:0338

12.1.2 GlobalSign RootSign Partners CA

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	SHA-1/RSA
Schlüssellänge	2048 bit
Aussteller des Zertifikates	GlobalSign nv-sa
Eigentümer des Zertifikates	GlobalSign nv-sa
Gültigkeitsdauer	not before 16-Dec-2003 13:00:00 GMT not after 27-Jan-2014 11:00:00 GMT
Seriennummer	4*(2^80) + 1071588716062 (dez) 04 0000 0000 00F9 7FAA 2E1E (hex)

Zur Prüfung der Authentizität des GlobalSign RootSign Partners CA Zertifikats kann folgender Fingerprint des Zertifikates herangezogen werden

MD5: A2AE:8241:90D7:3112:5354:B9FD:E243:325A
SHA-1: 0CEE:B712:AE36:104D:7719:3533:FDF9:1F15:B511:9177

12.1.2.1 Deutsche Telekom CA 5

Deutsche Telekom CA 5 signiert ab dem 09.02.2006 den T-TeleSec ServerPass. Das Zertifikat enthält folgende Informationen

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	SHA-1/RSA
Schlüssellänge	2048 bit
Aussteller des Zertifikates	GlobalSign nv-sa
Eigentümer des Zertifikates	T-Systems Enterprise Services GmbH Trust Center Deutsche Telekom

Gültigkeitsdauer	not before 07-Feb-2006 11:00:00 GMT not after 07-Feb-2013 11:00:00 GMT
Seriennummer	4*(2↑80) + 1139329266906 (dez) 04 0000 0000 0109 4550 f4da (hex)

Zur Prüfung der Authentizität des Deutsche Telekom CA 5 Zertifikats kann folgender Fingerprint des Zertifikates herangezogen werden

MD5: CC1E:29FE:4C41:5424:735B:883F:EC7C:6F31
SHA-1: 19BD:A7C0:076D:E1BE:F2B0:A4B4:CE7F:9956:71AD:2C84

12.2 GTE CyberTrust Global Root

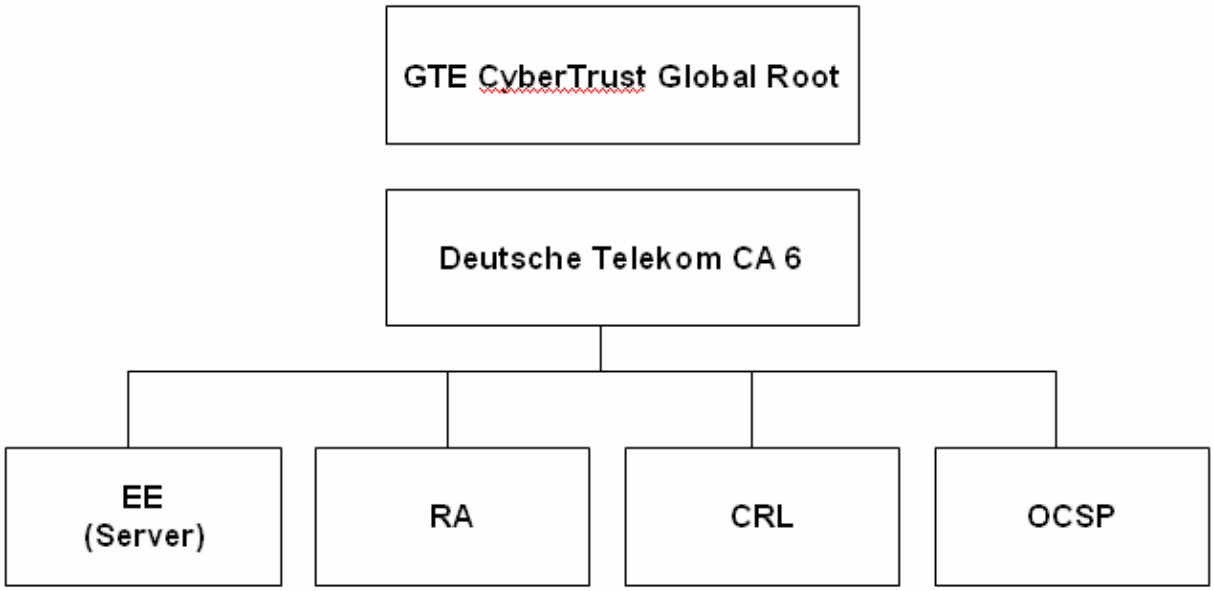

Abbildung 4 (CA Hierarchie ab 30.03.2007 unter der GTE CyberTrust Global Root)

Die Abbildungen stellen die PKI – Struktur im T-Systems Trust Center für den entsprechenden Zeitraum dar. Die Wurzelzertifizierungsstelle erstellt das selbstsignierte Wurzelzertifikat (Root – Zertifikat). Alle unter dieser Hierarchie ausgegebenen Zertifikate sind von der darüber liegenden Instanz signiert. Das vom Trust Center ausgestellte SSL-Server-Zertifikat lässt sich über die Vertrauenskette (Chain of Trust) bis zur obersten Zertifizierungsinstanz prüfen.

12.2.1 GTE CyberTrust Global Root

Die GTE CyberTrust Root nutzt einen Root Key, dessen öffentlicher Schlüssel eine Länge von 1024 bit hat. Dieser Root Key wurde in sicherer Umgebung generiert. Das GTE CyberTrust Global Root Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 1
Schlüsselalgorithmus	Md5/RSA
Schlüssellänge	1024 bit
Aussteller des Zertifikates	GTE Corporation
Eigentümer des Zertifikates	GTE Corporation
Gültigkeitsdauer	not before 13-Aug-1998 00:29:00 GMT not after 13-Aug-2018 23:59:00 GMT
Seriennummer	421 (dez) 01A5 (hex)
Signatur	Digitale Signatur der GTE Cyber Trust Root

Zur Prüfung der Authentizität des GTE CyberTrust Global Root kann folgender Fingerprint des Zertifikates herangezogen werden:

MD5: CA3D:D368:F103:5CD0:32FA:B82B:59E8:5ADB
SHA-1: 9781:7950:D81C:9670:CC34:D809:CF79:4431:367E:F474

12.2.2 Deutsche Telekom CA 6

Diese T-Systems CA signiert ab 30.03.2007 den T-TeleSec ServerPass. Die Schlüsselgenerierung erfolgte in der sicheren Umgebung des T-Systems Trust Centers. Das Deutsche Telekom CA 6 Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	SHA-1/RSA
Schlüssellänge	2048 bit
Aussteller des Zertifikates	GTE Corporation
Eigentümer des Zertifikates	T-Systems Enterprise Services GmbH
Gültigkeitsdauer	not before 29-Mar-2007 11:00:00 GMT not after 29-Mar-2014 11:00:00 GMT
Seriennummer	120001597 (dez) 0x727143d (hex)
Signatur	Digitale Signatur der GTE Cyber Trust Root

Zur Prüfung der Authentizität des Deutsche Telekom CA 6 Zertifikats kann folgender Fingerprint des Zertifikates herangezogen werden:

MD5: A1:93:98:4E:F7:05:2D:0E:8B:B4:3C:D5:9F:05:67:22
SHA1: E5:8C:7B:F4:E4:43:00:1C:7E:B2:DC:64:50:F7:D0:9F:94:23:91:78

12.3 T-TeleSec ServerPass

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	SHA-1/RSA
Schlüssellänge	512 bis 2048
Aussteller des Zertifikates	T-Systems Enterprise Services GmbH Trust Center Deutsche Telekom
Eigentümer des Zertifikates	Auftraggeber
Gültigkeitsdauer	1 Jahr ab Ausstellungstag (plus 5 Tage Kulanzzeit)
Seriennummer	XXXX (hex)
Signatur	Digitale Signatur Deutsche Telekom CA 5 ab 09.02.2006 oder Digitale Signatur Deutsche Telekom CA 6 ab 30.03.2007

13 Verwaltung der Zertifikate

13.1 Statusabfrage

Das T-Systems Trust Center betreibt einen öffentlich zugänglichen Dienst, in welchem die Zertifikate der T-TeleSec ServerPass Kunden während deren Laufzeit geführt werden und hierdurch auf ihren aktuellen Status hin überprüfbar sind. Die Möglichkeit zur Statusprüfung haben Sie auf unseren Internetseiten.

13.2 Sperrliste (Certificate Revocation List CRL)

Die gesperrten Zertifikate werden in einer CRL abgelegt und sind über das Internet abrufbar. Sobald diese Zertifikate ihre eingetragene Gültigkeitsdauer überschritten haben, werden Sie aus der CRL entfernt. Das T-Systems Trust Center stellt den Zertifikatsnutzern eine öffentliche und international 7 X 24h erreichbare CRL zur Verfügung, die sowohl per http als auch in Form eines LDAP-Verzeichnisses erreichbar ist.

13.3 Archivierung

Das T-Systems Trust Center hat Systeme und Abläufe installiert, um die Integrität der in der CA gespeicherten Daten gewährleisten zu können. Es werden täglich Sicherungskopien erstellt.
Nach Ablauf der im Zertifikat angegebenen Gültigkeitsdauer werden diese Zertifikate für einen Zeitraum von 5 Jahren archiviert. Ein Abruf von archivierten Zertifikaten ist gegen Entgelt möglich.

14 Sicherheit

Das T-Systems Trust Center ist in einem besonders geschützten Gebäude realisiert und wird von fachkundigem Personal betrieben. Alle baulichen und organisatorischen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept (nicht öffentlich verfügbar) dokumentiert.

14.1 Gebäudesicherheit

Die Gebäudesicherheit wird unter anderem durch folgende Maßnahmen erreicht:

- durchbruchhemmende Bauweise,
- einzelstehendes Gebäude,
- einbruchshemmende Stahltüren,
- durchschusssichere Fenster,
- abstrahlsichere Wände,
- Alarmanlagen,
- eigene unterbrechungsfreie Stromversorgung.

Der Zutritt zu dem Gebäude und einzelnen Räumen ist durch umfangreiche Maßnahmen gesichert:

- elektronische Zugangsschutzsicherung
- mehrere Schließkreise
- Regelungen für Besucher, Reinigung, Service etc.

14.2 Personal

Das im T-Systems Trust Center arbeitende Personal ist sicherheitsüberprüft und erfüllt die Anforderungen des Signaturgesetzes.

14.3 Erstellung und Management der CA Keys

Der öffentliche und private Schlüssel der CA wurde direkt auf kryptografischen PCMCIA-Karten unter Aufsicht erstellt. Von dem privaten Schlüssel der CA ist ein Backup angefertigt worden und zwar in der Weise, dass der private Schlüssel mittels einer weiteren kryptografischen PCMCIA Karte verschlüsselt und danach in mehrere Segmente aufgeteilt wurde. Die kryptografische Karte ist in einer gesicherten Umgebung abgelegt. Der private Schlüssel der CA ist im Trust Center nie unverschlüsselt vorhanden.

15 Wichtige Hinweise

Änderungen:
Um auf geänderte Marktanforderungen reagieren zu können, behält sich T-Systems Enterprise Services GmbH Änderungen und Anpassungen des CPS vor.

CPS:
Alle Zertifikate werden nach dem zum Zeitpunkt der Zertifikatsausstellung gültigen Certification Practice Statement (CPS) erstellt.

Identitätsdaten:
Für die Zertifikatsausstellung und um das Vertrauen in ein ausgestelltes Zertifikat zu gewährleisten, werden u.a. Identitätsdaten des Zertifikatsinhabers erfasst und geprüft. Bei diesen Prüfungen wird nur die Identität des Zertifikatsinhabers, nicht jedoch die Vertrauenswürdigkeit, Liquidität und Kreditwürdigkeit festgestellt.

Aktualität der Zertifikatsdaten:
Zum Zeitpunkt der Registrierung werden die für den Dienst erforderlichen Daten überprüft. Eine Aktualität der Daten zu einem späteren Zeitpunkt kann nicht zugesichert werden. Auch bei der Erneuerung eines Zertifikates werden diese Daten nicht erneut überprüft. Bei Änderungen des Zertifikatsinhaltes ist der Zertifikatsinhaber zu einer Sperrung des Zertifikates verpflichtet.

Vorbehalte:
Trotz größtmöglicher Sorgfalt bei der Erstellung dieser Dokumentation behält sich T-Systems Irrtümer über enthaltene Aussagen vor.
Es besteht kein Rechtsanspruch auf die Ausstellung eines Zertifikates.

16 Glossar

CA	Certification Authority (siehe Zertifizierungsinstanz)
CPS	Certification Practice Statement (Ergänzende Beschreibung der Zertifizierungsdienstleistung)
CRL	Certificate Revocation List (siehe Sperrliste)
Digitales Zertifikat	Datensatz, der den Namen einer Person oder eines Systems, deren öffentlichen Schlüssel, gegebenenfalls einige andere Angaben und eine Signatur einer Zertifizierungsinstanz enthält. Ein digitales Zertifikat ist Voraussetzung für sicheren und authentischen Datenaustausch.
DN	Distinguished Name. Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Fingerprint	Siehe Hashwert
GMT	Greenwich Mean Time
Hashwert	Ergebnis einer Hashfunktion. In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert).
HRA	Handelsregisterauszug
Kulanzzeit	Um diese Zeit (5 Tage) verlängerte Gültigkeitsdauer des Zertifikates, um bei fristgerechter Erneuerung die volle Gültigkeitsdauer nutzen zu können.
PKCS	Public Key Cryptographic Standards bezeichnet eine Reihe von kryptografischen Spezifikationen, die ab 1991 von den RSA Laboratorien und anderen entwickelt wurden.
PKI	Public Key Infrastructure. Gesamtheit der Komponenten, Prozesse und Konzepte, die zur Verwendung von Public-Key-Verfahren verwendet werden. Typischerweise besteht eine PKI aus zentralen Komponenten wie einer Zertifizierungsinstanz und einem Verzeichnisdienst und verschiedenen Client-Komponenten.
RA	Registration Authority (siehe Registrierungsinstanz)
Registrierungsinstanz	Stelle, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten.
Root	(siehe Wurzelzertifizierungsinstanz)
Server-Zertifikat-Request	Definiertes Datenformat, das mittels Softwaretool erzeugt wird und wesentlicher Bestandteil der Zertifizierungsanfrage ist. Üblicherweise ist dieses Softwaretool im Lieferumfang der meisten Server enthalten. (siehe auch FAQ der Internetseiten und Kapitel 8.3 des CPS)
Sperrliste	Liste der gesperrten Zertifikate
SSL	Secure Socket Layer (Standard für ein Sicherheitsprotokoll, hauptsächlich zur sicheren Online-Datenübertragung zwischen Client und Server im Internet-Umfeld eingesetzt)

X509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Wurzelzertifizierungsinstanz	Oberste Zertifizierungsinstanz einer CA - Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsinstanz ausgestellt wurde, sondern selbstsigniert ist.
Zertifikat	(siehe digitales Zertifikat)
Zertifizierungsinstanz	Komponente, die digitale Zertifikate ausstellt, indem sie einen Datensatz bestehend aus öffentlichem Schlüssel, Name und verschiedenen anderen Daten digital signiert. Ebenso werden von der Zertifizierungsinstanz Sperrinformationen herausgegeben