T-TeleSec ServerPass
Certification Practice Statement

Herausgegeben von:

T-Systems International GmbH
Business Unit ITC-Security, TeleSec

Untere Industriestraße 20
57250 Netphen

Supportline: 0800 8 3 5 3 7 3 2
0800 T e l e S e c

Telefax : (02 71) 7 08 - 16 25

E-Mail : T-TeleSec@t-systems.com

Internet : www.telekom.de/t-telesec

T · · Systems · · ·

Inhaltsverzeichnis

Versionshistorie

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	gültig	01.12.2003	EICK	Aktualisierung der Zertifikatshierarchie

Glossar und Abkürzungen

CA	Certification Authority (siehe Zertifizierungsinstanz)
CPS	Certification Practice Statement (Ergänzende Beschreibung der Zertifizierungsdienstleistung)
CRL	Certificate Revocation List (Liste der gesperrten Zertifikate)
GMT	Greenwich Mean Time
HRA	Handelsregisterauszug
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-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)
SSL	Secure Socket Layer (Standard für ein Sicherheitsprotokoll, hauptsächlich zur sicheren Online-Datenübertragung zwischen Client und Server im Internet-Umfeld eingesetzt)
TTC	Telekom Trust Center
Wurzelzertifizierungsinstanz	Oberste Zertifizierungsinstanz einer CA - Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsinstanz ausgestellt wurde, sondern selbstsigniert ist.
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

1 Vorwort

Die T-Systems International GmbH betreibt durch die Business Unit ITC-Security, Geschäftsbereich TeleSec das Trust Center der Deutschen Telekom, das 1997 nach ISO 9002 und 2000 nach ISO 9001:2000 zertifiziert wurde. 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 Trust Center der Deutschen Telekom durch einen sehr hohen Sicherheitsstandard aus. Alle im 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.
Die bauliche und organisatorische Infrastruktur erfüllt die strengen Anforderungen des Deutschen Signaturgesetzes.
Seit Bestehen des Trust Centers der Deutschen Telekom wurden weit mehr als 2,2 Mio. Zertifikate ausgegeben.

2 Bedeutung der CPS

Das Certification Practice Statement (CPS) beschreibt die Tätigkeiten von TeleSec in der Funktion als Certification Authority (CA) und Registration Authority (RA) und beschreibt in Ergänzung zu den AGB die Verfahrensweisen, wie TeleSec Server-Zertifikate im Rahmen der zertifikatsbasierten Public Key Infrastructure (PKI) ausgestellt und verwaltet werden.
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.

Besucher eines mit T-TeleSec ServerPass geschützten Webauftrittes können aufgrund des CPS entscheiden, ob Sie das TeleSec Zertifikat anerkennen und der digitalen Signatur vertrauen.

3 Allgemeines zum T-TeleSec ServerPass

Der T-TeleSec ServerPass macht einen Server 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 Zertifikats sowie der Signatur des Telekom Trust Centers.
Durch die Möglichkeit der Verschlüsselung (SSL) wird für die Sicherheit der Verbindung 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 Zertifikats für T-TeleSec ServerPass ist in einem separaten Abschnitt beschrieben (siehe Kapitel 12.55).

5 Benutzung und Zweck des T-TeleSec ServerPass

TeleSec Server Zertifikate dürfen nur zur Authentifizierung der Kommunikation des entsprechenden Servers genutzt werden. Die sichere Kommunikation erfolgt mittels SSL - Sicherheitsstandard.

6 Haftung

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

7 Pflichten

7.1 Rolle und Pflichten des Trust Centers

Das Telekom Trust Center (TTC) handelt als Certification Authority (CA) und Registration Authority (RA). Das TTC in der Rolle als CA generiert und signiert den T-TeleSec ServerPass und die dazugehörigen Sperrlisten. Ferner verwaltet und archiviert das TTC den T-TeleSec ServerPass und die Sperrlisten.
In ihrer Rolle als RA überprüft sie die Aufträge zur Ausstellung, Sperrung und Erneuerung von ServerPass Zertifikaten und autorisiert die Aufträge oder lehnt sie ab.

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 Auftrags erzeugt.
Die unterschriebene Papierversion des Auftrags, Onlinedaten sowie Identifikationspapiere vervollständigen den Auftrag.

8.2 Ablaufübersicht

Der ServerPass wird für den Zeitraum von 1 Jahr ausgestellt und im einzelnen wie folgt beauftragt:

- Server-Request wird durch den Kunden erzeugt (siehe Kapitel 8.3)
- Eingabe der Kundendaten inkl. Server-Request auf der TeleSec Webseite (Online-Auftrag) Absenden der Daten
- Ausdrucken des Auftrags und Unterzeichnen durch Zeichnungsberechtigte(n) (Es wird nur der vom Telekom 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 Telekom Trust Center senden

8.3 Hinweise zum Server-Request

Beim Erzeugen des 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 des Requests 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, wenn ja (z. B. laut HRA)
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

* bei Gewerbetreibenden steht hier entweder die gewerbetreibende Person selbst mit Vor- und Nachname oder bei einem freigewählten 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 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	|

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:

9.1.1 Bei der Erstbeauftragung unterscheiden wir folgende Fälle:

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

9.1.2 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 Server Pass 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 Auftrags 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 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 Auftrags

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 und dem Root Zertifikat bereitgestellt. Der im Auftrag genannte technische Ansprechpartner wird informiert.
Dieser kann über die TeleSec Webseite 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 Zertifikats ist endgültig und kann nicht aufgehoben werden!

11.3 Erneuerung von Zertifikaten

Der T-TeleSec ServerPass hat eine Gültigkeit von einem Jahr. 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 Zertifikats 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, jedoch behält sich das Trust Center der Deutschen Telekom das Recht auf eine erneute Identitätsfeststellung, zum Beispiel auf Grund eventuell geänderter Sicherheitsanforderungen, vor.

12 Zertifikatshierarchie und -aufbau

Für T-TeleSec ServerPass wird eine zweistufige CA Hierarchie eingesetzt.

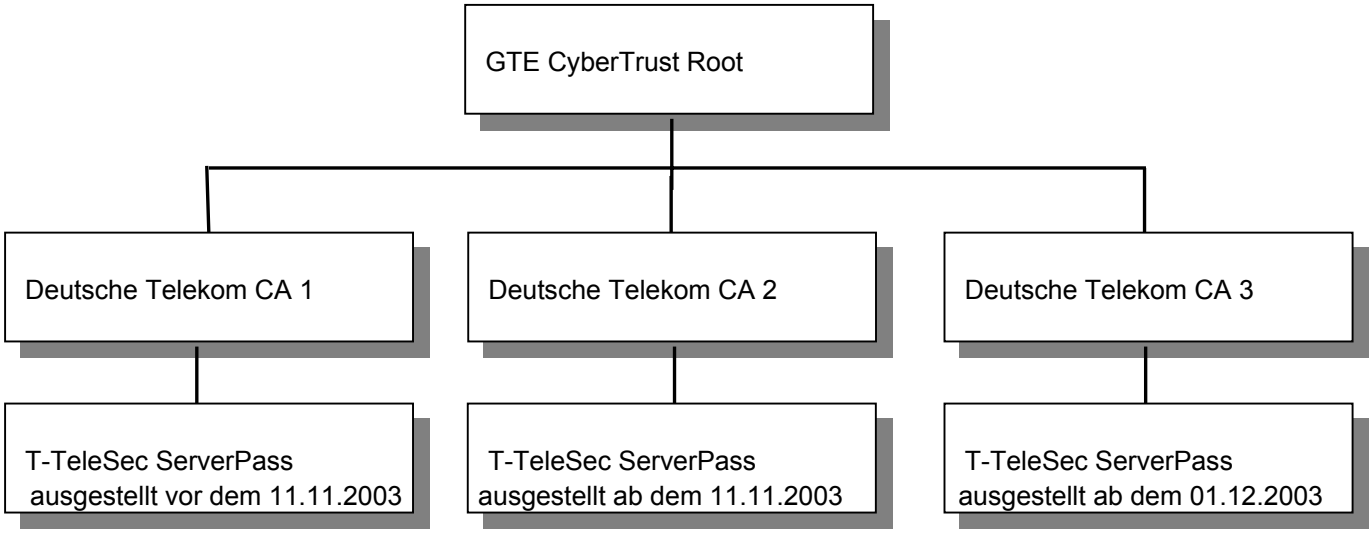

Abbildung : CA Hierarchie

Die Abbildung stellt die PKI – Struktur im Trust Center der Deutschen Telekom dar. Der vom Trust Center ausgestellte ServerPass lässt sich über die Vertrauenskette (Chain of Trust) bis zur obersten Zertifizierungsstelle prüfen.

Die Wurzelzertifizierungsstelle als oberste Zertifizierungsstelle erstellt das selbstsignierte Wurzelzertifikat (Root – Zertifikat) GTE CyberTrust Root und signiert Zertifizierungsstellen der zweiten Stufe. Das Trust Center der Deutschen Telekom als Zertifizierungsstelle der zweiten Stufe signiert mit dem (CA – Zertifikat) den T-TeleSec ServerPass.

12.1 GTE CyberTrust 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 Root Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 1
Schlüsselalgorithmus	Md5/RSA
Schlüssellänge	1024
Aussteller des Zertifikats	GTE Corporation
Eigentümer des Zertifikats	GTE Corporation
Gültigkeitsdauer	not before23-Feb-1996 not after 23-Feb-2006 (10Jahre)
Seriennummer	419 (dez) 0x000001A3 (hex)
Signatur	Digitale Signatur der GTE Cyber Trust Root

Die Root CA ist dadurch gekennzeichnet, dass ihr Zertifikat mit dem eigenen privaten Schlüssel signiert wurde (self signed root).

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

MD5: C4D7 F0B2 A3C5 7D61 67F0 04CD 43D3 BA58
SHA-1: 90DE DE9E 4C4E 9F6F D886 1757 9DD3 91BC 65A6 8964

12.2 Deutsche Telekom CA 1

Die CA der Deutschen Telekom nutzte vor dem 11.11.2003 einen Schlüssel, dessen öffentlicher Teil eine Länge von 1024 bit hat. Dieser Schlüssel wurde im Trust Center der Deutschen Telekom generiert und mit dem privaten Schlüssel der GTE CyberTrust Root signiert. Das Deutsche Telekom CA 1 Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	Md5/RSA
Schlüssellänge	1024 bit
Aussteller des Zertifikats	GTE Corporation
Eigentümer des Zertifikats	T-TeleSec
Gültigkeitsdauer	not before16-Nov-2000 not after 16-Nov-2004 (4Jahre)
Seriennummer	33554766 (dez) 0x0200014E (hex)
Signatur	Digitale Signatur der GTE Cyber Trust Root

Zur Prüfung der Authentizität des Deutsche Telekom CA 1 Zertifikats kann folgender Fingerprint des Zertifikats herangezogen werden:

MD5: 95:7E:E2:B3:82:F8:03:88:EC:F5:86:22:4D:7F:DA:78
SHA-1: 9D:AB:F4:32:76:56:A7:6B:F2:D0:65:F1:3A:66:C8:56:A2:2A:4B:2F

12.3 Deutsche Telekom CA 2

Die CA der Deutschen Telekom nutzt ab dem 11.11.2003 einen Schlüssel, dessen öffentlicher Teil eine Länge von 2048 bit hat. Dieser Schlüssel wurde im Trust Center der Deutschen Telekom generiert und mit dem privaten Schlüssel der GTE CyberTrust Root signiert. Das Deutsche Telekom CA 2 Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	SHA-1/RSA
Schlüssellänge	2048 bit
Aussteller des Zertifikats	GTE Corporation
Eigentümer des Zertifikats	TeleSec Trust Center
Gültigkeitsdauer	not before 03-Nov-2003 15:37:00 GMT not after 03-Feb-2006 23:59:00 GMT
Seriennummer	67109681 (dez) 0x4000331 (hex)
Signatur	Digitale Signatur der GTE Cyber Trust Root

Zur Prüfung der Authentizität des Deutsche Telekom CA 2 Zertifikats kann folgender Fingerprint des Zertifikats herangezogen werden:

MD5: 1F:12:76:BB:2F:CC:C8:C2:13:E8:9A:23:1B:9A:7C:3B
SHA-1: 6D:60:40:23:66:EB:AF:8D:96:E1:A0:28:A5:CA:91:4C:3B:07:11:C7

12.4 Deutsche Telekom CA 3

Die CA der Deutschen Telekom nutzt ab dem 01.12.2003 einen Schlüssel, dessen öffentlicher Teil eine Länge von 2048 bit hat. Dieser Schlüssel wurde im Trust Center der Deutschen Telekom generiert und mit dem privaten Schlüssel der GTE CyberTrust Root signiert. Das Deutsche Telekom CA 3 Zertifikat enthält folgende Informationen:

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	SHA-1/RSA
Schlüssellänge	2048 bit
Aussteller des Zertifikats	GTE Corporation
Eigentümer des Zertifikats	TeleSec Trust Center
Gültigkeitsdauer	not before: 01-Dec-2003 18:52:00 GMT not after 23-Feb-2006 23:59:00 GMT
Seriennummer	67109719 (dez) 0x4000357 (hex)
Signatur	Digitale Signatur der GTE Cyber Trust Root

Zur Prüfung der Authentizität des Deutsche Telekom CA 3 Zertifikats kann folgender Fingerprint des Zertifikats herangezogen werden:

MD5 6A:CE:88:DD:92:1F:21:60:3B:DF:BC:B4:94:F6:EF:F6
SHA1 64:39:86:93:32:0F:13:76:ED:DF:21:A5:3B:4A:D2:F2:9A:F4:BC:84

12.5 T-TeleSec ServerPass

Zertifikatsfeld	Inhalt
Version	Version 3
Schlüsselalgorithmus	Md5/RSA
Schlüssellänge	512 bis 2048
Aussteller des Zertifikats	TeleSec
Eigentümer des Zertifikats	Auftraggeber
Gültigkeitsdauer	1 Jahr ab Ausstellungstag
Seriennummer	XXXX (hex)
Signatur	Digitale Signatur Deutsche Telekom CA 1 vor 11.11.2003 Digitale Signatur Deutsche Telekom CA 2 ab 11.11.2003

13 Verwaltung der Zertifikate

13.1 Statusabfrage

Das Telekom Trust Center betreibt einen öffentlich zugänglichen Dienst, in welchem die Zertifikate der 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.

13.3 Archivierung

Das Telekom 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 Trust Center der Deutschen Telekom ist in einem besonders geschützten Gebäude realisiert und wird von speziell geschultem Personal betrieben.

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 Trust Center der Deutschen Telekom arbeitende Personal ist sicherheitsüberprüft und erfüllt die Anforderungen des Signaturgesetzes.

14.3 Erstellung und Management der CA Keys

Der öffentliche und private Schlüssel der CAs wurde direkt auf kryptografischen PCMCIA-Karten unter Aufsicht erstellt. Von dem privaten Schlüssel der CAs 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 kryptografischen Karten sind in einer gesicherten Umgebung abgelegt. Der private Schlüssel der CAs ist im Trust Center nie unverschlüsselt vorhanden.

15 Wichtige Hinweise

Änderungen:
Um auf geänderte Marktanforderungen reagieren zu können behält sich die Deutsche Telekom 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 Zertifikats werden diese Daten nicht erneut überprüft. Bei Änderungen des Zertifikatsinhaltes ist der Zertifikatsinhaber zu einer Sperrung des Zertifikats verpflichtet.

Vorbehalte:
Trotz größtmöglicher Sorgfalt bei der Erstellung dieser Dokumentation behält sich die Deutsche Telekom Irrtümer über enthaltene Aussagen vor.
Es besteht kein Rechtsanspruch auf die Ausstellung eines Zertifikats.