Public Key Service 2007

Certificate Practice Statement

Version: 2.1
Stand: 21.09.2007
Status: Freigegeben

Business flexibility T · · Systems · · ·

Business flexibility T · · Systems · · ·

Impressum

Herausgeber

T-Systems Enterprise Services GmbH

Security Solutions
Untere Industriestraße 20

57250 Netphen

Dateiname	Dokumentennummer	Dokumentenbezeichnung
CPS PKS DRAFTv2.0.QS TH.doc	[Hier Dok-Nr. eingeben]	[Hier Bezeichnung eingeben]

Version	Stand	Status
2.1	21.09.2007	Freigegeben

Autor	Inhaltlich geprüft von	Freigegeben von
Peter Schmidt	Thomas Hoof, Jörg Spitzensteder	Axel Treßel
Netphen, 20.08.2008	Netphen, Bonn,	Bad Kreunach

Ansprechpartner	Telefon / Fax	E-Mail
T-TeleSec Support Line	Tel: +49 800 8 3 5 3 7 3 2 Tel: +49 800 T e l e S e c Fax: +49 271 7 08 - 16 25	T-TeleSec@t-systems.com

Kurzinfo

Certificate Practice Statement für den T-TeleSec Public Key Service

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
1.0	14.01.2005	Jog	Ursprungsversion in Englisch
1.1	21.01.2005	Jog	Redaktionelle Änderungen
1.2	17.06.2005	Jog	Überarbeitung
1.3	10.08.2005	SB	Übersetzung ins Deutsche
1.33	07.09.2005	Jog, SB	Überarbeitung
2.0	20.09.2007	PS	Qual. und fortgeschr. Zertifikate für Netkey3.0 (RSA2048)
2.1	21.09.2007	PS	Kommentare und Anmerkungen von DD, TH, JK zur Qualitätssicherung eingearbeitet

Inhaltsverzeichnis

1 Einleitung

Bei dem vorliegenden Dokument handelt es sich um die **Zertifizierungsrichtlinie** (engl. Certification Practice Statement, kurz **CPS**) für die Dienstleistung **T-TeleSec Public Key Service ® (kurz PKS)**. Im Folgenden wird es als die **PKS CPS** bezeichnet. Die PKS CPS findet ausschließlich Anwendung auf die Ausstellung qualifizierter Public Key Zertifikate, qualifizierter Attribut-Zertifikate sowie fortgeschrittener Zertifikate im Rahmen der PKS Dienstleistung.

Hinweis:

Unter fortgeschrittenen Zertifikaten sind im Kontext der Dienstleistung PKS Zertifikate zur Erstellung fortgeschrittener Signaturen, zur Verschlüsselung und zur Authentisierung zu verstehen.

1.1 Überblick

Das Trust Center der Deutschen Telekom AG (Telekom Trust Center) wird durch die Konzerneinheit T-Systems Enterprise Services, IT Operatons betrieben. Das Telekom Trust Center ist seit 1996 nach ISO 9002 und seit Januar 2001 nach ISO 9001:2000 zertifiziert.

Im Jahr 1998 hat das Telekom Trust Center 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 Telekom 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 Qualitätskontrollen. Die eingesetzte Technologie ist hoch entwickelt 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 Telekom Trust Center mehr als 4 Millionen Zertifikate ausgestellt. Zu den vom Telekom Trust Center angebotenen Leistungen gehört der T-TeleSec Public Key Service (PKS), der die Ausstellung qualifizierter Zertifikate gemäß dem deutschen Signaturgesetz (SigG) umfasst.

Die PKS CPS beschreibt die betrieblichen Abläufe und Sicherheitsmaßnahmen des Telekom Trust Centers in der Rolle als Zertifizierungsinstanz (engl. Certification Authority, kurz CA) und Registrierungsstelle (engl. Registration Authority, kurz RA). Das vorliegende Dokument dient als Ergänzung der Allgemeinen Geschäftsbedingungen (AGB) für die Nutzung der Dienstleistungen des PKS der T-Systems Enterprise Services GmbH.. Die aktuelle Version der PKS CPS stellt den tatsächlichen Stand der Zertifizierungstätigkeit dar und gilt ausschließlich für die Dienstleistung T-TeleSec PKS.

Im Einzelnen enthält die PKS CPS die folgenden Aspekte:

- Bedeutung und Verwendung von qualifizierten Public Key Zertifikaten
- Bedeutung und Verwendung von qualifizierten Attribut-Zertifikaten

- Bedeutung und Verwendung von fortgeschrittenen Zertifikaten
- Ausstellung von Zertifikaten
- Erneuerung von Zertifikaten (Re-Zertifizierung)
- Folge-Beauftragung von Zertifikaten
- Zertifikatsmanagement
- Haftung
- Sicherheitsvorkehrungen

Mit einem PKS Public Key Zertifikat kann ein Teilnehmer nachweisen, dass ein elektronisches Dokument mit seinen (privaten) Signaturschlüssel, der auf einer sicheren Signaturerstellungseinheit (Chipkarte) gespeichert ist, elektronisch signiert wurde. Ferner kann er die Unverfälschtheit des signierten Dokumentes nachweisen. Die zugehörige qualifizierte Signatur ist der handschriftlichen Unterschrift gleichgestellt.

Teilnehmer können PKS Attribut-Zertifikate nutzen, um die Verwendung des entsprechenden Signaturschlüssels einzuschränken oder zusätzliche Informationen (z. B: Vertretungsmacht) kenntlich zumachen.

1.2 Dokumentenidentifikation

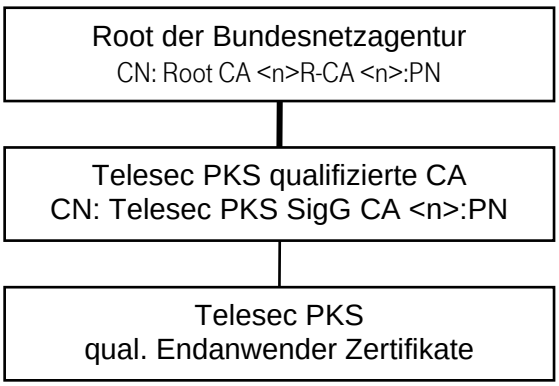
Name:	Zertifizierungsrichtlinie für T-TeleSec Public Key Service ® (PKS CPS)
Version:	2.0
Datum	20.08.2007
Objektbezeichnung (Object Identifier)	N/A

1.3 PKI Beteiligte

1.3.1 Zertifizierungsstellen

1.3.1.1 Qualifizierte Zertifikate

Der T-TeleSec Public Key Service für qualifizierte Zertifikate (sowohl Public Key als auch Attribut Zertifikate) ist in eine zweistufige Zertifizierungshierarchie eingegliedert:

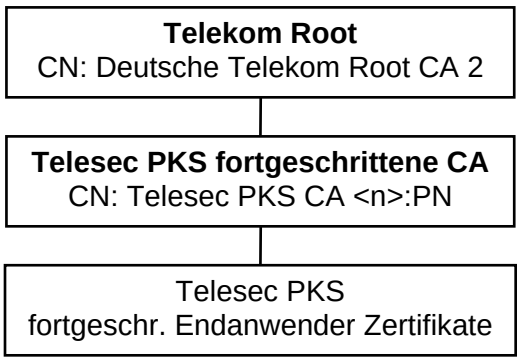


Die Wurzel-Zertifikate sowie die CA- und Dienste-Zertifikate von PKS werden von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen im Folgenden kurz BNetzA genannt) als zuständige Aufsichtsbehörde im Sinne des deutschen Signaturgesetzes (SigG) ausgestellt. Die Vertrauensbeziehung zwischen den verschiedenen Wurzel-Zertifikaten der Bundesnetzagentur wird technisch durch Cross-Zertifizierung hergestellt. Die Grafik oben veranschaulicht die Zertifizierungshierarchie anhand von beispielhaft ausgewählten Zertifikaten.

Zertifizierungsinstanz PKS CA: Gemäß dem deutschen Signaturgesetze stellt die PKS CA nur qualifizierte Zertifikate an Endanwender aus. Der Zertifizierungspfad von PKS Zertifikaten kann bis zu einem Wurzel-Zertifikat geprüft werden. Die PKS CA wird im Hochsicherheitsbereich des Telekom Trust Centers betrieben.

1.3.1.2 Fortgeschrittene Zertifikate

Der T-TeleSec Public Key Service für fortgeschrittene Zertifikate folgt einer zweistufigen Zertifizierungshierarchie:



Der öffentliche Schlüssel (Public Key) der Telekom Root CA2 ist in einem selbst signierten Zertifikat (Wurzel-Zertifikat) enthalten. Alle Teilnehmer des T-TeleSec Public Key Service erhalten das Zertifikat und können somit die Authentizität und Gültigkeit aller unterhalb dieses Wurzelzertifikates innerhalb der T-TeleSec Public Key Service ausgestellten Zertifikate überprüfen.
Die Telekom Root CA2 zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten Zertifizierungsstellen.

Die T-TeleSec PKS fortgeschrittene CA zertifiziert ausschließlich Zertifikate für Endanwender des T-TeleSec PKS.

1.3.2 Registrierungsstellen

T-TeleSec PKS angegliederte Stellen betreiben etliche Registrierungsstellen, die die PKS-Anträge entgegennehmen und die zuverlässige Identifizierung von Auftraggebern durchführen. Die Vertrauenswürdigkeit und Zuverlässigkeit der Registrierungsstellen wird durch anerkannte Prüf- und Bestätigungsstellen geprüft und bestätigt. Die aktuelle Liste der autorisierten Registrierungsstellen ist unter http://pks.telesec.de/annahmestellen/index.htm einsehbar.

1.3.3 Zertifikatsinhaber

Zertifikatsinhaber sind natürliche Personen, die ein PKS Zertifikat beantragen bzw. erhalten, nachdem eine erfolgreiche Identifizierung und Authentifizierung durchgeführt worden ist.

1.4 Zertifikatsverwendung

1.4.1 Qualifizierte Zertifikate

T-TeleSec PKS Public Key qualifizierte Zertifikate werden für qualifizierte Signaturen im Sinne des deutschen Signaturgesetztes eingesetzt. Attribut-Zertifikate beschränken den Verwendungszweck des zugehörigen Signaturschlüssels oder enthalten zusätzliche Informationen über den Zertifikatsinhaber des zugehörigen qualifizierten Schlüsselzertifikats.

1.4.2 Fortgeschrittene Zertifikate

T-TeleSec PKS Public Key fortgeschrittene Zertifikate werden zur Authentisierung, zur Verschlüsselung und für fortgeschrittene Signaturen im Sinne des deutschen Signaturgesetzes eingesetzt. Die Prozesse und das Sicherheitsniveau zur Beantragung, Produktion und Auslieferung von fortgeschrittenen PKS-Zertifikaten sind exakt identisch zu denen, der qualifizierten Zertifikate. Lediglich die Root-Hierarchie ist unterschiedlich (vgl. Kap.1.3.1, Zertifizierungsstellen. Außerdem wird für die fortgeschrittenen Zertifikate standardmäßig kein OCSP-Service angeboten (vgl. Kap. 2.1).

1.5 Organisation zur Verwaltung dieses Dokuments

Diese CPS wurde von T-Systems Enterprise Services, IT Operations herausgegeben.

Adresse:
T-Systems Enterprise Services GmbH
IT-Operations
Trust Center Applications

Untere Industriestraße 20, 57250 Netphen
Postfach 1465, 57238 Netphen

Telefon: 0800 TELESEC (8 35 37 32)

Sperrhotline: +49 (0) 1805 26 82 02

E-Mail: t-telesec@t-systems.com

WWW: www.t-systems-telesec.com

1.6 Definitionen und Abkürzungen

BNetzA	Bundesnetzagentur für für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
CA	Certification Authority, Zertifizierungsinstanz
CPS	Certification Practice Statement
CRL	Certificate Revocation List, Sperrliste
ISIS-MTT	Gemeinsame Spezifikation von TeleTrust und der T7 Gruppe für elektronische Signaturen, Verschlüsselung und Public Key Infrastrukturen
LDAP	Lightweight Access Protocol
LRA	Lokale RA
OCSP	Online Certificate Status Protocol
PKD	Public Key Directory
PKS	Public Key Service
RA	Registration Authority,
Relying Party	Bezeichnet Personen oder Organisationen, die sich auf ein Zertifikat oder eine digitale Signatur verlassen.
RS	Registrierungsstelle
SigG	Signaturgesetz
SigV	Signaturverordnung
Subscriber	Zertifikatsempfänger
TTC	Telekom Trust Center
Zertifikatsempfänger	bezeichnet eine Person, die Gegenstand eines Zertifikats ist und der ein Zertifikat erteilt worden ist.

2 Veröffentlichung und Verantwortlichkeiten für den Verzeichnisdienst

2.1 Verzeichnisdienst

Der Verzeichnisdienst den T-TeleSec PKS ist unter den folgenden Bezugsadressen online zu erreichen:

- http://pks.telesec.de/verzeichnisdienst/index.htm
- http://pks.telesec.de/ocspr
- ldap://pks-ldap.telesec.de

In dem Public Key Directory (PKD) können ausgestellte und zum **Abruf freigegebenen** Zertifikate online abgerufen werden. Ferner ermöglichen der OCSP-Service und die Sperrliste(CRL) das **Nachprüfen des Status aller ausgestellten qualifizierten Zertifikate** (gesperrt/nicht gesperrt).
Für die nichtqualifizierten Zertifikate zur Signatur, Verschlüsselung und Authentisierung wird standardmäßig eine Sperrliste (CRL) aber kein OCSP-Service angeboten

2.2 Veröffentlichung von Informationen

Die T-TeleSec PKS publiziert die folgenden Informationen über http://pks.telesec.de/index.htm:

- Informationen zum Ausfüllen des PKS-Auftrages
- Annahmestellen
- Technische Beschreibung zum Verzeichnisdienst (LDAP, OCSP Responder)
- Zertifikatsprofile
- Informationen zum Sperrservice

Die Zertifikatsinhaber und Rahmenvertragspartner (Abonee) werden zusätzlich informiert bei

- der Sperrung eines Wurzelinstanzschlüssels oder eines CA-Schlüssels,
- der Kompromittierung oder Verdacht auf Kompromittierung eines Wurzelinstanzschlüssels oder eines CA-Schlüssels,
- sicherheitsrelevanten Änderungen der CPS.

Diese Informationen werden auf der Webseite des Zertifizierungsdiensteanbieters veröffentlicht. Zusätzlich erfolgt eine direkte Benachrichtigung der Zertifikatsinhaber in schriftlicher Form oder per E-Mail.

2.3 Update der Informationen / Veröffentlichungsfrequenz

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

- Zertifikate werden umgehend nach ihrer Freischaltung in den Verzeichnisdienst eingestellt. Zertifikate werden nach Ablauf ihrer Gültigkeit mindestens noch ein Jahr im Verzeichnisdienst veröffentlicht.
- Sperrlisten werden mindestens alle sechs Stunden aktualisiert.
- Richtlinien werden nach Bedarf aktualisiert.

2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf alle in Abschnitt 2.1. und 2.2 aufgeführten Informationen unterliegt keiner Zugangskontrolle. Der schreibende Zugriff auf diese Informationen erfolgt ausschließlich durch berechtigte Mitarbeiter.

3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die Mechanismen, die beim Prozess der Identifizierung und Authentifizierung eingesetzt werden, bevor ein Zertifikat ausgestellt wird:

- Der Antragsteller wird persönlich in der RS/LRA identifiziert.
- Die erhaltenen Antragsformulare werden hinsichtlich Vollständigkeit und Plausibilität geprüft.
- Die Dokumente werden hinsichtlich der Authentizität überprüft.
- Wenn die Registrierung in einer RS/LRA durchgeführt worden ist, wird die Autorisierung der Registrierungsmitarbeiter durch Personal der CA überprüft.
- Nach der Identifizierung durch das PostIdent-Verfahren wird die Authentizität des PostIdent-Formulars durch Personal der CA überprüft.

3.1 Namensgebung

Die qualifizierten Zertifikate enthalten den Namen des Zertifikatsinhabers. Der Name des Zertifikatsinhabers wird in dem Feld subject gespeichert und kann folgende Attribute aufweisen:

- countryName (vorgeschrieben)
- organizationName (optional)
- organizationalUnitName (optional)
- commonName (vorgeschrieben)
- serialNumber (vorgeschrieben)
- pseudonym (bedingt vorgeschrieben, siehe unten)

Wenn der Antragssteller ein Pseudonym als Name wünscht, kommt zusätzlich das Attribut Pseudonym in das Zertifikat. Ein Pseudonym wird immer in beide Attribute commonName und pseudonym eingetragen. Hierbei erhält das Pseudonym die Endung „:PN“
Auf Wunsch des Antragstellers wird zusätzlich zum Namen oder zum Pseudonym die E-Mail Adresse oder weitere Daten des Antragstellers (z. B. Organisationszugehörigkeit, Geburtsdatum, etc.) in das Zertifikat aufgenommen.

3.2 Aussagekräftigkeit von Namen

Der Name muss den Zertifikatnehmer eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen. Bei der Namensvergabe gelten zusätzlich die folgenden Konventionen:

- Die Schreibweise des Namens muss mit der Schreibweise im Identifikationsdokument übereinstimmen. Diese darf nicht aufgrund von Sonderzeichen wie z.B. Umlauten geändert sein.
- Falls der gleiche Name mehr als einmal existiert, wird er durch die Ergänzung eines nummerierten Suffixes eindeutig gemacht.

3.3 Pseudonymität / Anonymität

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 SigGCA“, 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 erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.

3.4 Initiale Identitätsprüfung

Der Antragsteller weist seine Identität persönlich in der RS/LRA oder in einer Postfiliale unter Verwendung seines Personalausweises, seines Reisepasses oder einem vergleichbaren Dokument (bei ausländischen Antragstellern) nach. Wenn die Identifizierung des Kunden mit Hilfe seines Reisepasses vorgenommen wird, ist ein amtliche Meldebescheinigung zur Prüfung der Adresse des Antragstellers erforderlich.

Wenn der Antrag auf ein Zertifikat Daten über Dritte, berufsbezogene oder sonstige Angaben (z. B. Zugehörigkeit zu einer Organisation, Vertretungsmacht, berufliche Zulassung) enthält, muss der Antragsteller die Einwilligung des Dritten bzw. seine Autorisierung durch geeignete Dokumente nachweisen.

3.5 Identifizierung und Authentifizierung bei Folge-Beauftragungen

Rechtzeitig vor Ablauf der Gültigkeit der Zertifikate wird der Zertifikatsinhaber benachrichtigt. Ihm werden neue Zertifikate ausgestellt, wenn er dies vor Ablauf der Gültigkeit beantragt.

3.6 Identifizierung und Authentifizierung bei Sperranträgen

Zur Sperrung autorisierte Personen und Institutionen (siehe Kapitel 4.8) können die Sperrung von Zertifikaten entweder schriftlich, über einen formlosen Brief oder telefonisch beantragen.

Die Authentisierung einer schriftlichen Sperrung geschieht durch Vergleich der Unterschrift auf dem Brief mit der Unterschrift auf dem Original des Antragformulars.

Eine unverzügliche Sperrung des Zertifikates kann durch Anruf der Sperrhotline erreicht werden, die 7x24h betrieben wird. Für eine telefonische Sperrung ist das „Telepasswort“ des Zertifikates notwendig. Das Telepasswort wird durch den Antragsteller bzw. sperrberechtigten Dritten festgelegt und wird zur Authentisierung des Zertifikatsinhabers und / oder anderer zur Sperrung autorisierter Personen verwendet.

4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsbeantragung

Anträge im Rahmen von T-TeleSec Public Key Service sind nur schriftlich möglich. Der Antrag muss mit einer handschriftlichen Unterschrift des Antragstellers versehen sein. Die notwendigen Formulare sind auf den Webseiten des T-TeleSec Public Key Service zu finden.

Der Antrag muss durch Kopien des amtlichen Dokumentes, das zur Identifizierung herangezogen wurde, vervollständigt werden, und, falls der Antrag Daten über Dritte, berufsbezogene oder sonstige Angaben (z. B. Zugehörigkeit zu einer Organisation, Vertretungsmacht, berufliche Zulassung) enthält, weitere Dokumente, die die Autorisierung des Antragstellers zur Nutzung dieser Daten nachweisen, enthalten.

4.1.1 Beantragung eines qualifizierten Zertifikates

Neben dem vollständig und lesbar ausgefüllten Antragsformular ist nach §§ 3, 8 Abs. 2 SigV eine Kopie des Identifikationsdokumentes (z. B. Personalausweis) erforderlich, um eine qualifiziertes Zertifikat zu beantragen. Eine Liste weiterer akzeptierter Dokumente ist in den Erläuterungen zum PKS Antragsformular zu finden.

4.1.2 Beantragung eines Attribut-Zertifikates

Für die Beantragung eines Attribut-Zertifikates mit einschränkender Wirkung sind keine weiteren Dokumente über die Antragsdokumente hinaus notwendig, sofern keine Informationen über Dritte darin enthalten sind. Für Attribut-Zertifikate, die Informationen über Dritte enthalten, ist ein Nachweis der Berechtigung des Antragstellers zusätzlich zum vollständig und lesbar ausgefüllten Hauptantrag erforderlich.

Entsprechende Beispiele sind in den Erläuterungen zum Antrag für ein „Attribut-Zertifikat für die Vertretungsmacht“ und / oder für ein „Attribut-Zertifikat für berufrechtliche und andere Zulassungen“ enthalten.

4.1.3 Beantragung von fortgeschrittenen Zertifikaten

Die Beantragung von fortgeschrittenen Zertifikaten erfolgt zusammen mit der Beantragung von qualifizierten Zertifikaten.

4.2 Bearbeitung von Zertifikatsanträgen

Ein T-TeleSec PKS Zertifikat, das zu einen RSA-Schlüssel der Länge 1024 Bit ausgestellt wird, hat einen Gültigkeitszeitraum von 3 Jahren jedoch nicht länger als bis zum 31.12.2007. Ein Zertifikat, das zu einen RSA-Schlüssel der Länge 2048 Bit ausgestellt wird, hat wahlweise ein Gültigkeitszeitraum von 2, 3 oder 5 Jahren.

Die Beantragung eines qualifizierten Zertifikates geschieht in der folgenden Weise:

- Ausfüllen der notwendigen Formulare (dieser Vorgang kann durch die Webformulare, die auf den Webseiten von T-TeleSec PKS verfügbar sind, vereinfacht werden).
- Beifügen der Kopien der Identifikationsdokumente.
- Falls notwendig, Beifügen der Kopien weiterer Dokumente und Formulare (z. B. unterschrieben durch den Urheber der Vertretungsmacht etc.).
- Alle Formulare werden ordnungsgemäß unterschrieben.
- Persönliche Identifizierung des Antragstellers in einer RS/LRA der Deutschen Telekom AG oder über das PostIdent-Verfahren.

Danach werden die Dokumente zum Telekom Trust Center zur Produktion des qualifizierten Zertifikates gesendet.

4.3 Ausstellung von Zertifikaten

4.3.1 Ausstellung qualifizierter Zertifikate

Nach einer erfolgreichen Prüfung des Antrags wird das Zertifikat erzeugt. Das ausgestellte Zertifikat wird an den Antragsteller gesendet, entweder auf einer Chipkarteauf dem Postweg oder verschlüsselt per E-Mail oder Download, um es in eine geeignete Chipkarte zu importieren.

4.3.2 Ausstellung von Attribut-Zertifikaten

Attribut-Zertifikate werden nach erfolgreicher Prüfung der erhaltenen Dokumente ausgestellt und werden in jedem Fall verschlüsselt zur Auslieferung an den Antragsteller verschlüsselt. Die Auslieferung erfolgt per E-Mail oder Download.

4.3.3 Ausstellung von fortgeschrittenen Zertifikaten

Fortgeschrittene Zertifikate werden parallel zu den qualifizierten Zertifikaten erstellt. Die Prüf- und Generierungs- und Auslieferungsverfahren sind identisch.

4.4 Empfangsbestätigung von Zertifikaten

Nach Lieferung des qualifizierten Zertifikates muss der Zertifikatsinhaber den Empfang und die Korrektheit des Zertifikates gegenüber dem Telekom Trust Center bestätigen. Das Zertifikat wird erst aktiviert, wenn die Empfangsbestätigung vorliegt.

Qualifizierte Zertifikate gelten erst als gültig gemäß dem deutschen Signaturgesetz, nachdem sie im Verzeichnisdienst des Telekom Trust Centers aktiviert sind.
Fortgeschrittene Zertifikate gelten ebenfalls erst als Gültig, nachdem sie im Verzeichnisdienst des Telekom TrustCenters veröffentlicht sind.

4.5 Verwendung von Schlüsselpaar und Zertifikat

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsendanwender (Subscriber)

T-TeleSec PKS qualifizierte Zertifikate dürfen nur zur Erzeugung digitaler Signaturen (im Sinne der Nicht-Abstreitbarkeit) von Daten oder Dokumenten unter Beachtung der Sicherheitsanforderungen an die verwendeten Komponenten (Umgebung, Software, Kartenleser, etc) eingesetzt werden.
Fortgeschrittene Zertifikate werden auch für die Zwecke Authentiserung und Verschlüsselung so wie zur Erstellung fortgeschrittener Signaturen ausgestellt.

Darüber hinaus unterliegen Attribut-Zertifikate und nicht veröffentlichte Zertifikate dem Datenschutz.

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, muss

- 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 dieser CPS einsetzen.

4.6 Erneuerung von Zertifikaten (Re-Zertifizierung)

Eine automatisierte Zertifikatserneuerung wird nicht angeboten.

4.7 Änderung von Zertifikatsdaten

Wenn sich Identifikationsdaten des Zertifikatsinhabers ändern (z. B. bei der Namensänderung in Folge einer Eheschließung oder bei Ausstellung eines neuen Personalausweises) ist eine erneute Identifizierung erforderlich.

Bei einer Änderung der Anschrift oder E-Mail Adresse des Zertifikatsinhabers ist keine Neuidentifizierung erforderlich.

4.8 Zertifikatssperrung und Suspendierung

Die folgenden Gründe führen zu einer Sperrung des Zertifkats:

1. Abhandenkommen des privaten Schlüssels (z. B. Verlust oder Diebstahl des Schlüsselträgers).
2. Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor.
3. Die Angaben in den Zertifikaten sind nicht mehr korrekt.
4. Der zertifizierte Schlüssel oder die damit verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.
5. Es liegt ein Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsinhaber oder andere zur Nutzung des Schlüssels berechtigte Personen vor.
6. Gesetzliche Vorschriften

Die folgenden Personen und Institutionen sind berechtigt, die Sperrung eines qualifizierten Zertifikates zu initiieren:

- Der Zertifikatsinhaber.
- Sperrberechtigte Dritte, das sind:
  - Vertreter des Zertifikatsinhabers.
  - Personen, für die der Zertifikatsinhaber eine Vertretungsmacht hat und dieser Fakt in das qualifizierte Zertifikat bzw. in ein qualifiziertes Attribut-Zertifikat eingetragen wurde (siehe Abschnitt 4.1.2).
  - Für berufsbezogene oder sonstige Angaben zuständige Stelle, falls eine berufsbezogene oder sonstige Angabe in das qualifizierte Zertifikat bzw. in ein qualifiziertes Attribut-Zertifikat aufgenommen wurde (siehe Abschnitt 4.1.2).
- Das Telekom Trust Center kann die Sperrung eines Zertifikates gemäß den Allgemeinen Geschäftsbedingungen für den T-TeleSec Public Key Service oder aus gesetzlichen Gründen veranlassen.
- Die Bundesnetzagentur kann die Sperrung eines Zertifikates aufgrund gesetzlicher Vorschriften anweisen.

Die Sperrung von Zertifikaten kann durch einen formlosen Brief oder durch einen telefonischen Anruf initiiert werden. Ein formloser Brief wird nur akzeptiert, wenn er die handschriftliche Unterschrift einer autorisierten Person, die das Zertifikat sperren möchte, enthält.

Um eine telefonische Sperrung zu ermöglichen, betreibt T-Systems eine Sperrhotline, die 24 Stunden 7 Tage die Woche besetzt ist. Um die Sperrung auszuführen, ist das „Telepasswort" erforderlich. Das Telepasswort wird durch den Antragsteller bzw. den sperrberechtigten Dritten festgelegt und wird zur Authentisierung des Zertifikatsinhabers und / oder anderer zur Sperrung autorisierter Personen verwendet.

Telefonische Sperrungen werden unmittelbar nach ihrem Eingang durchgeführt. Schriftliche Sperrungen spätestens an dem auf den Eingang folgenden Arbeitstag.

Die Kontaktdaten für die Sperrhotline werden auf folgender Webseite veröffentlicht:
http://pks.telesec.de/sperrservice/index.htm.

Gesperrte Zertifikate erscheinen in der Sperrliste (CRL), die regelmäßig alle 6 Stunden sowie nach jedem Sperrvorgang erneuert wird. Das Erscheinen in der Sperrliste wird auch als Bestätigung für die erfolgreiche Durchführung der Sperrung verwendet. Die Sperrliste kann vom Webserver unter http://pks.telesec.de/telesec/servlet/download_crl oder vom LDAP-Server unter ldap://pks-ldap.telesec.de jederzeit abgerufen werden.

Auch im Falle von Systemdefekten, Servicearbeiten oder und anderen Faktoren, die außerhalb dem Einflußbereich von T-Systems liegen, wird T-Systems dafür sorgen, dass Sperranträge tatsächlich innerhalb o.g. Zeiten ausgeführt werden. Hierfür ist ein Notfallszenario entworfen worden, welches regelmäßig geprobt wird.

Zertifikate werden mindestens ein Jahr auch nach Ablauf deren Gültigkeit in der Sperrliste geführt.

Bemerkung: Die Sperrung eines Zertifikates ist endgültig und kann nicht rückgängig gemacht werden. Zertifikat-Suspendierungen sind durch das deutsche Signaturgesetz verboten und daher nicht möglich.

4.9 Statusauskunftsdienste für Zertifikate

4.9.1 Download von Zertifikaten

Das Telekom Trust Center betreibt einen öffentlich zugänglichen LDAP Server. Dieser Server stellt solche Zertifikate zum Download bereit, deren Inhaber explizit der Veröffentlichung zugestimmt haben. Ohne eine explizite Zustimmung des Inhabers wird ein ausgestelltes Zertifikat nicht veröffentlicht und kann nicht vom LDAP Server heruntergeladen werden.

Die Schnittstellenspezifikation für den LDAP Server ist auf den T-Telesec PKS Webseiten verfügbar.

4.9.2 Statusauskunftsdienst

Das Telekom Trust Center betreibt einen öffentlich zugänglichen OCSP-Responder, der zur Statusprüfung eines Zertifikates genutzt werden kann. Die Adresse des OCSP-Responders lautet http://pks.telesec.de/ocspr.

Die Schnittstellenspezifikation zu diesem Dienst ist auf den T-TeleSec PKS Webseiten verfügbar.

Für nichtqualifizierte Zertifikate werden standardmäßig keine OCSP-Auskünfte angeboten.

4.9.3 Sperrliste

Gesperrte Zertifikate werden in die Sperrliste (CRL) aufgenommen, die regelmäßig alle 6 Stunden sowie nach der jedem Sperrvorgang erneuert wird. Die Aufnahme in die Sperrliste wird auch als Bestätigung für die erfolgreiche Durchführung der Sperrung verwendet. Die Sperrliste kann vom Webserver unter http://pks.telesec.de/telesec/servlet/download_crl oder vom LDAP-Server unter ldap://pks-ldap.telesec.de jederzeit abgerufen werden.

Die technische Spezifikation der Sperrliste ist auf den T-TeleSec PKS Webseiten verfügbar.

4.10 Schlüsselhinterlegung und Wiederherstellung

Das deutsche Signaturgesetz verbietet ausdrücklich die Hinterlegung und Wiederherstellung von Schlüsseln. Daher bietet T-TeleSec PKS solche Dienstleistungen **nicht** an.

5 Bauliche und organisatorische Maßnahmen

Das Telekom Trust Center ist in einem speziell geschützten Gebäude untergebracht and wird von fachkundigem Personal betrieben. Alle Prozesse für die Beantragung und Erzeugung von Zertifikaten sind genau definiert und von einer unabhängigen Stelle überprüft worden.

5.1 Bauliche Sicherheitsmaßnahmen

Die bauliche Sicherheit des Telekom Trust Centers wird durch die folgenden Maßnahmen erreicht:

- Durchbruchsichere Bauweise.
- Einbruchsichere Stahltüren.
- Kugelsichere Fenster.
- Abstrahlsichere Wände.
- Alarmanlage.
- Unterbrechungsfreie Stromversorgung.
- 24x7 Wachdienst.
- Kameraüberwachung.

Der Zutritt zum Gebäude und den entsprechenden Räumen ist durch erhebliche Vorkehrungen gesichert:

- Elektronische Bewegungsmelder.
- Personenschleuse
- Organisatorische Regelungen für Besucher, Servicetechniker, Gebäudereinigung, etc.

5.2 Organisatorische Maßnahmen

Das Change Advisory Board des Telekom Trust Centers ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in der vorliegenden CPS dargestellt werden. Deshalb setzt es die relevanten Rollen, die im Sicherheitskonzept definiert sind, entsprechend ihrer Aufgaben, Expertisen und Kompetenzen ein.

5.3 Personelle Maßnahmen

Die Zuverlässigkeit des Personals, das im Telekom Trust Center arbeitet wird regelmäßig überprüft. Das Personal besucht in regelmäßigen Abständen Fortbildungen.

Alle Anforderungen des deutschen Signaturgesetzes werden vollständig erfüllt.

Eine Rollentrennung bei kritischen Prozessen wird im Sicherheitskonzept definiert. Organisationen, die als RS/LRA für das Telekom Trust Center agieren (z.B. die Registrierungsstellen der Deutschen Telekom AG und der Deutschen Post AG) haben vertragliche Vereinbarungen geschlossen, die die Zuverlässigkeit und Fachkunde ihres Personals sowie die Einhaltung bestimmter zugewiesener Aufgaben sicherstellen.

5.4 Einstellung des Betriebes

Die Einstellung des Betriebes wird sowohl der Bundesnetzagentur (als zuständige Behörde) als auch den Zertifikatsinhabern innerhalb einer Frist, die in §10 SigV festgelegt ist, bekannt gegeben. Das heißt mindestens zwei Monate vor der Einstellung des Betriebes.

Das Telekom Trust Center wird anderen Zertifizierungsdiensteanbietern die Möglichkeit geben, die qualifizierten Zertifikate und die Dokumentation zu übernehmen.

Wenn der Betrieb (insbesondere der Sperrdienst) nicht durch einen anderen Zertifizierungsdiensteanbieter übernommen wird, dann werden alle ausgestellten qualifizierten Zertifikate gesperrt.

Ein Antrag auf die Eröffnung eines Insolvenzverfahrens wird der Bundesnetzagentur als zuständige Behörde umgehend mitgeteilt.

6 Technische Sicherheitsmaßnahmen

6.1 Generierung und Installation der Schlüsselpaare

Alle Schlüsselpaare für Endanwender-Zertifikate und für CA-Zertifikate werden in einem abgeschirmten Raum auf einer sicherheitsüberprüften Hardwarekomponente erzeugt, die den Anforderungen des deutschen Signaturgesetzes genügt. Nach der Generierung werden die Schlüssel sicher auf einer Chipkarte gespeichert. Der private Schlüssel kann nach der Speicherung nicht mehr ausgelesen werden.

6.2 Schutz von privaten Schlüsseln und Sicherheitseigenschaften von kryptographischen Modulen

Die Schlüssel werden in sicherer Weise auf Chipkarten gespeichert, sodass der private Schlüssel nicht ausgelesen werden kann. Die Chipkarte und ihr Betriebssystem sind durch eine unabhängige Stelle evaluiert und zertifiziert worden. Sie erfüllt die Anforderungen des deutschen Signaturgesetzes.

Der Einsatz des privaten Schlüssels wird durch eine persönliche PIN geschützt. Die PINs der Chipkarten, die in der CA eingesetzt werden, werden in verschlüsselter Form gespeichert, sodass keine natürliche Person über das Wissen der PINs dieser Chipkarten verfügt.

6.3 Sicherheitsmaßnahmen an technischen Komponenten

Alle eingesetzten Komponenten, für die das deutsche Signaturgesetz eine Sicherheitsprüfung (Evaluierung) fordert, sind durch eine unabhängige Stelle nach ITSEC oder CC evaluiert worden.

6.4 Netzwerktechnische Sicherheitsmaßnahmen

Die verwendeten Firewalls und Computersysteme entsprechen dem aktuellen Stand der Technik. Alle Systeme sind minimal konfiguriert, nur die absolut notwendige Software ist installiert. Die Konfiguration der Systeme und Firewalls wurde durch eine unabhängige Stelle geprüft.

7 Zertifikatsprofile und Sperrlistenprofile

7.1 Zertifikatsprofil

Die Spezifikation des Zertifikatsprofils für qualifizierte Signaturen und Attribut-Zertifikate ist auf den T-TeleSec PKS Webseiten verfügbar unter
http://pks.telesec.de/support/dokumentation.

Die Spezifikation des Zertifikatsprofils für fortgeschrittene Zertifikate ist auf den T-TeleSec PKS Webseiten verfügbar unter
http://pks.telesec.de/support/dokumentation.

7.2 Sperrlistenprofil

Die Spezifikation der Sperrliste (CRL) ist auf den T-TeleSec PKS Webseiten verfügbar unter
http://pks.telesec.de/support/dokumentation.

7.3 OCSP Profil

Die Spezifikation des OCSP-Responders ist auf den T-TeleSec PKS Webseiten verfügbar unter
http://pks.telesec.de/support/dokumentation.

8 Audits und andere Bewertungskriterien

Als akkreditierter Zertifizierungsdiensteanbieter wird das Telekom Trust Center alle 3 Jahre von einer unabhängigen Organisation auditiert. Bei diesen Audits wird überprüft, ob das Telekom Trust Center die Anforderungen des SigG erfüllt.

Des Weiteren wird jede sicherheitserhebliche Änderung bei der zuständigen Behörde angezeigt und ebenfalls von einer unabhängigen Organisation überprüft und bestätigt.

Die an T-TeleSec PKS angegliederten Registrierungsstellen werden regelmäßig geschult. Zusätzlich werden dies e einem, regelmäßigen Audit unterzogen.

9 Sonstige geschäftliche und rechtliche Angelegenheiten

9.1 Preise

Die aktuelle Preisliste ist auf den T-TeleSec PKS Webseiten verfügbar unter http://pks.telesec.de/registration/preisliste.

9.2 Finanzielle Verantwortlichkeiten

Die finanziellen Verantwortlichkeiten werden in den Allgemeinen Geschäftsbedingungen (AGB) für den T-TeleSec Public Key Service beschrieben, diese sind verfügbar unter http://pks.telesec.de/registration/agb.

9.3 Datenschutz

Die personenbezogenen Daten des Zertifikatsinhabers werden in einem Umfang erhoben und verifiziert, wie es für die Ausstellung qualifizierter Zertifikate und zur Sicherstellung des Vertrauens in diese Zertifikate notwendig ist.

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

9.4 Urheberrecht

9.5 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.

Es gibt keinen gesetzlichen Anspruch auf die Ausstellung eines Zertifikates durch den T-TeleSec Public Key Service.

9.6 Haftungsbeschränkungen

Haftungsfragen sind in den Allgemeinen Geschäftsbedingungen (AGB) für den T-TeleSec Public Key Service geregelt, diese sind unter der folgenden Adresse verfügbar
http://pks.telesec.de/registration/agb.

9.7 Schadensersatz

Schadensersatzansprüche sind in den Allgemeinen Geschäftsbedingungen (AGB) für den T-TeleSec Public Key Service geregelt, dies sind unter der folgenden Adresse verfügbar
http://pks.telesec.de/registration/agb.

9.8 Fristen und Kündigung

Fristen und Kündigungen sind in den Allgemeinen Geschäftsbedingungen (AGB) für den T-TeleSec Public Key Service geregelt, dies sind unter der folgenden Adresse verfügbar
http://pks.telesec.de/registration/agb.

9.9 Änderungen der 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 dieser CPS durchzuführen. Änderungen der CPS werden auf der Internetseite (http://pks.telesec.de/index.htm) angekündigt und gelten von dem Moment an, in der die CPS in Kraft tritt. Die CPS tritt in zwei Wochen nach Veröffentlichung der Änderungen in Kraft, außer für den Fall, dass die Veröffentlichung einen anderen Zeitraum vorsieht.
Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Die aktuelle CPS wird mindestens einmal jährlich von T-TeleSec einem Review unterzogen. Zertifikatsempfänger, Relying Parties oder andere an der PKS beteiligte Personen bzw. Organisationen können Kommentare zu dem Inhalt der CPS an T-Systems melden. Die Entscheidungsbefugnis für Änderungen der CPS bleibt bei T-Systems.

Änderungen der CPS, welche nur Rechtschreibfehler beheben oder redaktioneller Natur sind, treten auch ohne vorherige Ankündigung in Kraft.

Bei jeder Änderung der CPS wird deren Versionsnummer und Datum erneuert.

9.10 Bestimmendes Recht

Das deutsche Signaturgesetz regelt generell die Ausstellung von qualifizierten Zertifikaten.

9.11 Andere Regelungen

9.11.1 CPS

Alle Zertifikate im Rahmen von PKS werden entsprechend der CPS in der Fassung ausgestellt, die zum Ausstellungszeitpunkt gültig ist.

9.11.2 Aktualität der Zertifikatsdaten

Die für den Service benötigten Daten werden zum Zeitpunkt der Registrierung verifiziert. Die Aktualität dieser Daten kann nicht für spätere Zeiten zu gesichert werden. Die Daten werden jedoch bei der Zertifikatserneuerung erneut verifiziert.

9.11.3 Beschwerden und Eskalationen

9.11.3.1 Benachrichtigung der Parteien eines Streitfalls

Bevor ein Verfahren zur Beilegung einer Streitigkeit (einschließlich Prozessführung oder Schlichtung) im Zusammenhang mit einer Streitigkeit in Bezug auf einen Aspekt dieses CPS oder eines von ausgestellten Zertifikats eingeleitet wird, müssen die sich in ihren Rechten verletzt fühlenden Personen das T-TeleSec Trust Center, die betreffende LRA/RS oder eine sonstige betroffene Partei benachrichtigen, um zu versuchen, die Streitigkeit untereinander beizulegen.

9.11.3.2 Eskalation

Falls die Streitigkeit nicht innerhalb von zehn (10) Tagen nach der anfänglichen Mitteilung gemäß CPS § 9.11.3.1 beigelegt wird, kann eine Partei den Streitfall in schriftlicher oder elektronischer Form T-Systems vorlegen und die Prüfung verlangen.

Daraufhin ruft T-Systems ein Gremium das sich aus PKI-Experten zusammensetzt, zusammen, um die jeweiligen Tatsachen mit dem Ziel, eine Beilegung der Streitigkeit zu ermöglichen, zusammenzutragen. Die beantragende Partei muss allen anderen Parteien eine Kopie des Sach- und Rechtsvortrags vorlegen. Jene Partei, die die Angelegenheit nicht vorgebracht hat, kann innerhalb von einer (1) Woche nach dem Datum, an dem die Streitigkeit dem Gremium vorgetragen wurde, entsprechende Informationen an das Gremium übermitteln. Das Gremium hat innerhalb von drei (3) Wochen (es sei denn, die Parteien vereinbaren, diese Frist um eine bestimmte zusätzliche Frist zu verlängern) nach dem Datum, an dem die Angelegenheit dem Gremium vorgetragen wurde, seine Empfehlungen zu formulieren und an die Parteien zu übermitteln. Das Gremium nimmt bei seiner Arbeit normalerweise E-Mail, Telekonferenzen, Kuriere und Briefpost in Anspruch. Die Empfehlungen des Gremium sind für die Parteien nicht verbindlich. Der Rechtsweg wird durch dieses Verfahren nicht ausgeschlossen.