Public Key Service

Certificate Practice Statement

Version: 3.2
Stand: 21.04.2015
Status: Freigegeben

Business flexibility T · · Systems · · ·

Impressum

Herausgeber

T-Systems International GmbH
Trust Center
Untere Industriestraße 20

57250 Netphen

Ansprechpartner	Telefon / Fax	E-Mail
TeleSec Support Line	Tel: +49 1805 268204	TeleSec_Support@t-systems.com

Kurzinfo

Certificate Practice Statement für den 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
3.0	19.04.2013	TH	Anpassung an aktualisierte ETSI TS 102 042 Anforderungen
3.1	19.05.2014	JS	Anpassungen Online Sperrungen und Änderungen nach ETSI Audit
3.2	21.04.2015	TH	Review 2015

Inhaltsverzeichnis

1 Einleitung

Bei dem vorliegenden Dokument handelt es sich um die **Zertifizierungsrichtlinie** (engl. Certification Practice Statement, kurz **CPS**) für die Dienstleistung **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 International GmbH 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 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 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 zu machen.

1.2 Dokumentenidentifikation

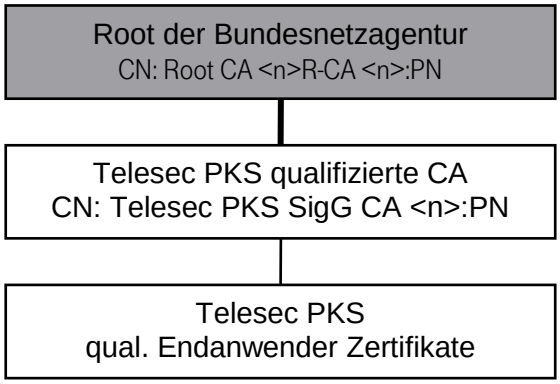
Name:	Zertifizierungsrichtlinie für TeleSec Public Key Service ® (PKS CPS)
Version:	3.2
Datum	21.04.2015
Objektbezeichnung (Object Identifier)	N/A

1.3 PKI Beteiligte

1.3.1 Zertifizierungsstellen

1.3.1.1 Qualifizierte Zertifikate

Der 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[1]-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.

Gemäß dem deutschen Signaturgesetz 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.

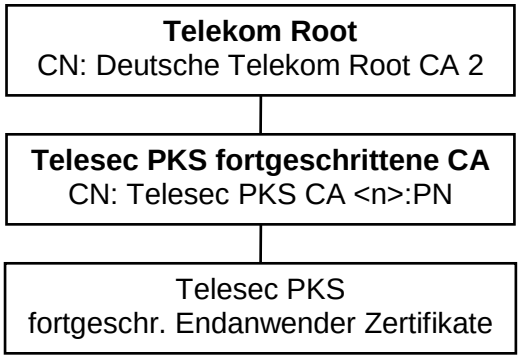
Für qualifizierte Zertifikate gelten die Bestimmungen des deutschen Signaturgesetzes (SigG), der Signaturverordnung (SigV) und die Festlegungen der Bundesnetzagentur.

1.3.1.2 Fortgeschrittene Zertifikate

Die Ausstellung fortgeschrittener Zertifikate, zusätzlich zu einem qualifizierten Zertifikat ist optional. Das für jedermann zugängliche Standardprodukt des Public Key Service enthält zusätzliche fortgeschrittene Zertifikate. Diese werden teilweise auch als nicht qualifizierte Zertifikate Bezeichnet. Kunden, die speziellen geschlossenen Benutzergruppen angehören erhalten möglicherweise keine fortgeschrittenen Zertifikate. Dies ist abhängig von den Vereinbarungen mit dem Leiter der Benutzergruppe, Eine nachträgliche Erstellung fortgeschrittener Zertifikate ist nicht möglich.

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

[1] Zertifikate zur Signatur von Verzeichnisdienst-Auskünften (OCSP), Sperrlisten und von qualifizierten Zeitstempeln



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

Die TeleSec PKS fortgeschrittene CA zertifiziert ausschließlich Zertifikate für Endanwender des TeleSec Public Key Service. Diese Zertifikate unterliegenden den Anforderungen von ETSI TS 102 042, Policy NCP+..

1.3.2 Registrierungsstellen

TeleSec PKS angegliederte Stellen betreiben etliche Registrierungsstellen, die die PKS-Aufträge entgegennehmen und die zuverlässige Identifizierung von Auftraggebern durchführen. Die Vertrauenswürdigkeit und Zuverlässigkeit der Registrierungsstellen wird durch anerkannte Prüf- und Bestätigungsstellen gemäß den Anforderungen des deutschen Signaturgesetzes geprüft und bestätigt. Die Identifizierung ist für jedermann mittels des PostIdent Verfahrens der Deutschen Post AG oder durch Notarident bei jedem Notar zugänglich. Zusätzlich existieren verschiedene Registrierungsstellen, die jedoch teilweise nur für bestimmte Benutzergruppen zuständig sind.

1.3.3 Zertifikatsinhaber

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

1.4 Zertifikatsverwendung

1.4.1 Allgemeine Grundlagen

Bei Verlust oder Missbrauch der Chipkarte/des Zertifikates ist unverzüglich eine Sperrung durch den Zertifikatsinhaber zu veranlassen. Dies gilt auch für den Verdacht des Missbrauches oder einem Verdacht auf Kompromittierung des verwendeten Schlüsselmaterials. Die betroffenen Zertifikate dürfen nicht mehr verwendet werden.

1.4.2 Qualifizierte Zertifikate

TeleSec PKS Public Key Service 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.
Bei Verlust oder Missbrauch der Chipkarte/des Zertifikates ist unverzüglich eine Sperrung des durch den Zertifikatsinhaber zu veranlassen. Dies gilt auch für den Verdacht des Missbrauches oder einem Verdacht auf Kompromitierung des verwendeten Schlüsselmaterials.

1.4.3 Fortgeschrittene Zertifikate

TeleSec PKS Public Key Service fortgeschrittene Zertifikate werden zur Authentisierung, zur Verschlüsselung und für fortgeschrittene Signaturen im Sinne des deutschen Signaturgesetzes eingesetzt. Die Prozesse und das Sicherheitsniveau zur Beauftragung, 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 Gültigkeitsmodell

Zur Prüfung der Gültigkeit einer Signatur bzw. eines Zertifikates existieren zwei unterschiedliche Gültigkeitsmodelle. Bedingt durch die Festlegung durch das deutsche Signaturgesetz gelten für alle Endanwender Zertifikate, die im Rahmen der PKS Dienstleistung ausgestellt wurden das Kettenmodell.
Das Kettenmodell besagt, dass die jedes Zertifikat zum Zeitpunkt seiner Anwendung gültig gewesen sein muss. Das bedeutet, zum Signaturzeitpunkt eines Dokumentes muss das signierende Zertifikat gültig gewesen sein. Dessen Ausstellerzertifikat muss gültig gewesen sein, als es das ausgestellte Zertifikat signiert hat usw. Die nachfolgende Abbildung veranschaulicht diesen Sachverhalt.

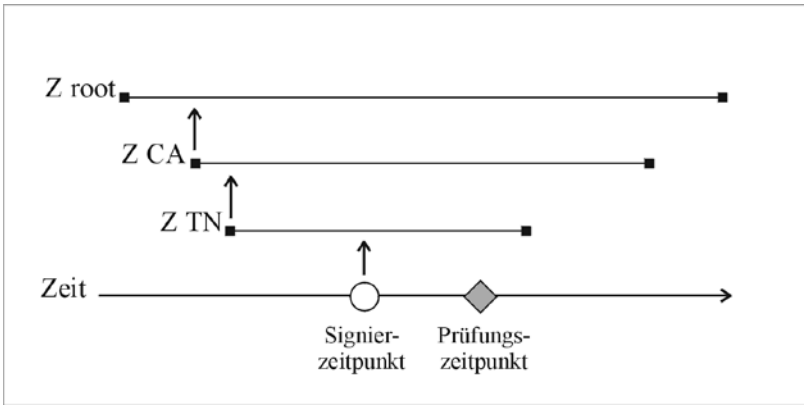


Abbildung 1: Kettenmodell

1.6 Organisation zur Verwaltung dieses Dokuments

Diese CPS wurde von T-Systems International GmbH herausgegeben.

Adresse:
T-Systems International GmbH
Trust Center Applications

Untere Industriestraße 20, 57250 Netphen
Postfach 1465, 57238 Netphen

Telefon: +49 (0) 1805 268 204 [2]

Sperrhotline:

Aus Deutschland	116 116
Aus dem Ausland	+49 30 4050 4050
Alternativ	+49 (0) 1805 26 82 02 [2]

E-Mail: telesec_support@t-systems.com

WWW: http://www.telesec.de

[2] 14 Ct/Minute aus dem deutschen Festnetz, max. 42 Ct/Minute aus dem Mobilfunk

1.7 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
Common-PKI	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 der TeleSec PKS Dienstleistung ist unter den folgenden Adressen jederzeit (7x24 entsprechend den Anforderungen des SigG) zu erreichen:

- http://www.telesec.de/pks/ → Verzeichnisdienst
- 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 nicht qualifizierten Zertifikate zur Signatur, Verschlüsselung und Authentisierung wird standardmäßig eine Sperrliste (CRL) aber kein OCSP-Service angeboten

2.2 Veröffentlichung von Informationen

Die TeleSec PKS publiziert die folgenden Informationen über http://www.telesec.de/pks:

- Informationen zum Ausfüllen des PKS-Auftrages
- 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 Auftraggeber wird persönlich in der RS/LRA identifiziert.
- Die erhaltenen Auftragsformulare 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 ausgestellten Public Key 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 Auftraggeber 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 Auftraggebers wird zusätzlich zum Namen oder zum Pseudonym die E-Mail Adresse oder weitere Daten des Auftraggebers (z. B. Organisationszugehörigkeit etc.) in das Zertifikat aufgenommen.

3.2 Aussagekräftigkeit von Namen

Der Name muss den Zertifikatsinhaber 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 (serialNumber) eindeutig gemacht.

3.3 Pseudonymität / Anonymität

Auf expliziten Wunsch kann dem Auftraggeber auch ein anonymes Zertifikat ausgestellt werden. In diesem Fall kann der Auftraggeber 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 Auftraggeber weist seine Identität persönlich in der RS/LRA oder in einer Postfiliale unter Verwendung seines Personalausweises, seines Reisepasses oder einem vergleichbaren Dokument (bei ausländischen Auftraggebern) nach.

Wenn der Auftrag auf ein Zertifikat Daten über Dritte, berufsbezogene oder sonstige Angaben (z. B. Zugehörigkeit zu einer Organisation, Vertretungsmacht, berufliche Zulassung) enthält, muss der Auftraggeber 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 beauftragt. Die Folge-Beauftragung kann mittels einer qualifizierten Signatur mit dem noch gültigen Zertifikat erfolgen.

3.6 Identifizierung und Authentifizierung bei Sperranträgen

Zur Sperrung autorisierte Personen und Institutionen (siehe Kapitel 4.9) können die Sperrung von Zertifikaten entweder schriftlich oder über einen formlosen Brief beauftragen.

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

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 Auftraggeber festgelegt und wird zur Authentisierung des Zertifikatsinhabers verwendet.

4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsbeauftragung

Aufträge im Rahmen von TeleSec Public Key Service sind nur schriftlich möglich. Der Auftrag muss mit einer handschriftlichen Unterschrift des Auftraggebers versehen sein. Die notwendigen Formulare sind auf den Webseiten des TeleSec Public Key Service zu finden.

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

4.1.1 Beauftragung eines qualifizierten Zertifikates

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

4.1.2 Beauftragung eines Attribut-Zertifikates

Für die Beauftragung eines Attribut-Zertifikates mit einschränkender Wirkung sind keine weiteren Dokumente über die Auftragsdokumente hinaus notwendig, sofern keine Informationen über Dritte darin enthalten sind. Für Attribut-Zertifikate, die Informationen über Dritte enthalten, ist ein Nachweis der Berechtigung des Auftraggebers zusätzlich zum vollständig ausgefüllten Hauptauftrag erforderlich.

Entsprechende Beispiele sind in der Information zum Public Key Service enthalten.

4.1.3 Beauftragung von fortgeschrittenen Zertifikaten

Die Beauftragung von fortgeschrittenen Zertifikaten erfolgt zusammen mit der Beauftragung von qualifizierten Zertifikaten. Eine einzelne Beauftragung von fortgeschrittenen Zertifikaten ohne ein qualifiziertes Zertifikat ist nicht möglich.

4.2 Bearbeitung von Zertifikatsaufträgen

Ein TeleSec PKS Zertifikat, das zu einen RSA-Schlüssel der Länge 1024 Bit ausgestellt wird, hat einen Gültigkeitszeitraum nicht länger als bis zum 31.12.2007. Ein Zertifikat, das zu einen RSA-Schlüssel der Länge 2048 Bit ausgestellt wird, hat einen maximalen Gültigkeitszeitraum nicht länger als bis zum 30.06.2016. Zu den RSA-Schlüsseln der Länge 2048 werden maximal bis zum 31.12. 2014 Zertifikate erstellt. Ab dem 15.01.2013 wer-

den Zertifikate mit Schlüsseln basierend auf elliptischen Kurven verwendet. Bei allen Zertifikaten gilt das diese nicht länger gültig sind wie der von der Bundesnetzagentur und dem BSI herausgegebene Algorithmenkatalog die verwendeten Algorithmen als geeignet für qualifizierte Signaturen einstuft. Die Angaben aus dem Algorthmenkatalog ergänzen die hier getätigten Angaben zu der maximalen Gültigkeitsdauer und haben den hier getätigten Angaben Vorrang.

Fortgeschrittene Endanwenderzertifikate haben den gleichen Gültigkeitszeitraum wie das qualifizierte Zertifikat der gleichen Chipkarte. Fortgeschrittene Zertifikate, die den Einschränkungen des deutschen Algorithmenkatalogs eigentlich nicht unterliegen, werden vom Trust Center so behandelt als würden sie diesen Einschränkungen unterliegen.

Die Beauftragung eines qualifizierten Zertifikates geschieht in der folgenden Weise:

- Ausfüllen der notwendigen Formulare mittels der auf der Webseite http://www.telesec.de verfügbaren Online-Formularen. Handschriftlich ausgefüllte Formulare werden nicht anerkannt. Das gleiche gilt für handschriftlich durchgeführte Änderungen auf den ausgedruckten Formularen.
- Beifügen der Kopien der Identifikationsdokumente.
- Falls notwendig, Beifügen der Kopien weiterer Dokumente und Formulare (z. B. unterschrieben durch den Urheber der Vertretungsmacht etc.).
- Falls der Auftraggeber einen Organisationseintrag in seine Zertifikate aufgenommen haben möchte, einen Nachweis darüber das er diesen Eintrag führen darf.
- Alle Formulare werden ordnungsgemäß unterschrieben.
- Persönliche Identifizierung des Auftraggebers in einer RS/LRA der Deutschen Telekom AG, über das PostIdent-Verfahren das BehördenIdent-Verfahren oder bei einem Notar.
- Alle Formulare (Auftragsformulare, Urkunden von Notaren, Attributbestätigungen von Dritten, usw.) müssen auf Papier ausgedruckt und ausschließlich im Original oder für Folgeaufträge vom Zertifikatsinhaber qualifiziert elektronisch signiert vorliegen. Handschriftliche Änderungen sind auch zur Vermeidung von Manipulationen nicht zulässig. Aus dem gleichen Grund werden Auftragsformulare, die nicht in einem verschlossenen Umschlag im Trust Center ankommen zurückgewiesen.

Danach werden die Dokumente zum Telekom Trust Center zur Produktion des qualifizierten Zertifikates gesendet. Im Telekom Trust Center wird die Authentizität der Aufträge auf Basis der im Sicherheitskonzept festgelegten Prozesse überprüft. Diese Prozesse werden in regelmäßigen Abständen durch eine anerkannte Prüf- und Bestätigungsstelle kontrolliert.

Alle Auftragsunterlagen werden im Trust Center gemäß den Anforderungen des deutschen Signaturgesetz 30 Jahre nach Ablauf des letzten Zertifikates, das auf Basis eines Auftrages ausgestellt wurde, archiviert. Die rein digitale Übermittlung eines Auftrags zur Erstellung qualifizierter Zertifikate ist gemäß den Bestimmungen des Signaturgesetz ausgeschlossen und wird somit nicht angeboten.

4.3 Ausstellung von Zertifikaten

Zertifikate werden erst ausgestellt wenn alle notwendigen Unterlagen vollständig und in der erforderlichen Form (im Original, kein Fax) vorhanden sind. Die Zuordnung der ausgestellten Zertifikate zu den vorliegenden Aufträgen und Personen erfolgt in der Kundendatenbank des Trust Centers.

4.3.1 Ausstellung qualifizierter Zertifikate

Nach einer erfolgreichen Prüfung des Auftrags wird das Zertifikat erzeugt. Auf Basis der in der Datenbank abgelegten Daten ist eine sichere und eindeutige Zuordnung zu den Auftragsunterlagen im Archiv sicher gestellt. Das ausgestellte Zertifikat wird entweder sofort auf der persönlichen Chipkarte des Zertifikatsinhabers und in der Kundendatenbank des Trust Centers gespeichert um später per Email an den Zertifikatsinhaber gesendet zu werden.

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 Auftraggeber 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 Auslieferung von Zertifikaten

Die Auslieferung der Zertifikate, mit Ausnahme von Attribut-Zertifikaten, erfolgt im Regelfall durch den Versand der persönlichen Chipkarte des Zertifikatsinhabers im verschlossenen Umschlag an die von ihm im Auftrag angegebene Lieferanschrift.

Attributzertifikate und (für spezielle Kundenprojekte) auch Public Key Zertifikate können per Email versendet werden. In diesem Fall enthält die Email eine verschlüsselte Datei im Anhang oder sie verweist auf eine URL unter der sich der Kunde die verschlüsselte Datei downloaden kann. Für die Entschlüsselung benötigt der Kunde sein im Auftrag angegebenes Telepasswort und ggf. seine persönliche Chipkarte, deren Kartennummer er ebenfalls im Auftrag angegeben hat. Für ihn verschlüsselte Public Key Zertifikate kann er nach der Entschlüsselung auf seiner Chipkarte abspeichern.

Ebenfalls Teil des Auslieferungsverfahrens ist die Empfangsbestätigung des Kunden. Siehe nachfolgendes Kapitel.

4.5 Empfangsbestätigung von Zertifikaten

Nach Lieferung des qualifizierten Zertifikates muss der Zertifikatsinhaber den Empfang und die Korrektheit des Zertifikates gegenüber dem Telekom Trust Center bestätigen. Durch die Empfangsbestätigung wird sichergestellt das die Chipkarte beim Zertifikatsinhaber ohne Manipulation angekommen ist. Das Zertifikat wird erst aktiviert, wenn die Empfangsbestätigung vorliegt in der der Kunde den Korrekten Empfang der Chipkarte und deren Unversehrtheit so wie den korrekten Zertifikatsinhalt bestätigt hat.

Die Chipkarte ist mit einem integrierten Schutzmechanismus versehen. Das als NullPIN-Verfahren patentierte Verfahren schützt vor missbräuchlicher Nutzung der Chipkarte durch einen Dritten auf dem Versandweg. Bei der NullPIN handelt es sich um eine spezielle Transport-PIN (beispielsweise „00000“), die vom Trust Center voreingestellt ist mit der sich die Sicherheitsfunktionen der Chipkarte aber nicht nutzen lassen. Nach der erst-

maligen Aktivierung lässt sich die PIN nicht mehr in den NullPIN-Status zurück versetzen. Dadurch können sicherheitskritische Manipulationen an der erhaltenen Chipkarte erkannt werden.

Qualifizierte Zertifikate gelten erst als gültig gemäß dem deutschen Signaturgesetz, nachdem sie im Verzeichnisdienst des Telekom Trust Centers aktiviert sind.
Fortgeschrittene Zertifikate gelten ab dem Ausstellungszeitpunkt als gültig. Sendet ein Zertifikatsinhaber seine Empfangsbestätigung zurück und fordert er darin die Sperrung werden die Zertifikate gesperrt.

4.6 Verwendung von Schlüsselpaar und Zertifikat

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

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. Der Zertifikatsinhaber sollte seine Chipkarte ausschließlich mit Software nutzen, die über eine Bestätigung oder Herstellererklärung nach dem deutschen Signaturgesetz verfügt. Die Liste der bestätigten oder herstellererklärten Software kann auf der Webseite der Bundesnetzagentur[3] eingesehen werden.
Fortgeschrittene Zertifikate werden auch für die Zwecke Authentisierung und Verschlüsselung so wie zur Erstellung fortgeschrittener Signaturen ausgestellt.
Der Endanwender muss die Voraussetzungen zur Nutzung der Signaturkarte, Beispielsweise den Umgang mit seinen PIN's, welche in der Information zum Public Key Service beschrieben sind, beachten. Dieses Dokument kann über die Webseite des Trust Centers unter https://www.telesec.de/pks/ → Support → Downloadbereich → Hinweise heruntergeladen werden.

Darüber hinaus unterliegen Attribut-Zertifikate und nicht veröffentlichte Zertifikate dem Datenschutz.
Erhält der Zertifikatsendanwender Kenntniss von der Kompromittierung seines privaten Schlüssels, oder hegt den Verdacht, dass sein privater Schlüssel kompromittiert wurde, so ist der Zertifikatsendanwender verpflichtet unverzüglich die Sperrung seines Zertifikates zu veranlassen.

4.6.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Relying Parties

Jeder, der ein Zertifikat, welches im Rahmen dieser CPS 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

[3] http://www.bundesnetzagentur.de/cln_1911/DE/Sachgebiete/QES/Veroeffentlichungen/Produkte/Produkte_node.html (Stand Mai 2013)

- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit dieser CPS einsetzen.

4.7 Erneuerung von Zertifikaten (Re-Zertifizierung)

Eine automatisierte Zertifikatserneuerung wird nicht angeboten. Kunden, die wie in Kapitel 3.5 beschrieben einen Folgeauftrag stellen, erhalten neues Schlüsselmaterial. Eine Rezertifizierung des vorhandenen Schlüsselmaterials ist im derzeitigen Prozess nicht vorgesehen.

4.8 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.

4.9 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).
  - Rechnungsempfänger
- Das Telekom Trust Center kann die Sperrung eines Zertifikates gemäß den Allgemeinen Geschäftsbedingungen für den 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, über das online Sperrformular (Web-Seite) 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. Erfolgt die Sperrung durch einen sperrberechtigten Dritten so ist zusätzlich die Verwendung von Geschäftspapier des Dritten erforderlich.

Um eine Sperrung zu ermöglichen, betreibt das Trust Center ein online Sperrformular sowie eine telefonische Sperrhotline, die 24 Stunden 7 Tage die Woche erreichbar ist. Um die Sperrung auszuführen, ist das „Telepasswort" erforderlich. Das Telepasswort wird durch den Auftraggeber bzw. den sperrberechtigten Dritten festgelegt und wird zur Authentisierung des Zertifikatsinhabers und / oder anderer zur Sperrung autorisierter Personen verwendet.

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

Die Kontaktdaten für die Sperrhotline und das online Sperrformular werden auf folgender Webseite veröffentlicht:
http://www.telesec.de/pks/ → Sperrservice.

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 für qualifizierte Zertifikate kann vom Webserver unter http://pks.telesec.de/telesec/servlet/download_crl oder vom LDAP-Server unter ldap://pks-ldap.telesec.de/o=Deutsche Telekom AG,c=de jederzeit abgerufen werden. Die Sperrlisten für fortgeschrittene Zertifikate können vom LDAP Server unter ldap://pks-ldap.telesec.de/o=T-Systems International GmbH,c=de oder ldap://pks-ldap.telesec.de/o=T-Systems Enterprise Services GmbH,c=de jederzeit abgerufen werden.

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

Nach Durchführung einer Sperrung erhält der Zertifikatsinhaber eine Email in der er über die erfolgte Sperrung benachrichtigt wird. In dieser Email wird ihm auch der genaue Sperrzeitpunkt mitgeteilt.

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.

4.10 Statusauskunftsdienste für Zertifikate

4.10.1 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 Telesec PKS Webseiten verfügbar.

4.10.2 Statusauskunftsdienst

Das Telekom Trust Center betreibt einen öffentlich zugänglichen OCSP-Responder, der jederzeit (7x24 entsprechend den Anforderungen des SigG) 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 TeleSec PKS Webseiten verfügbar.

Für nichtqualifizierte Zertifikate werden keine OCSP-Auskünfte angeboten.

4.10.3 Sperrliste

Gesperrte Zertifikate werden in die Sperrliste (CRL) aufgenommen, die regelmäßig mindestens alle 6 Stunden sowie nach jedem Sperrvorgang erneuert wird. Die Ankündigung der Erneuerung nach spätestens 6 Stunden ist in der Sperrliste für die qualifizierten Zertifikate, nicht enthalten, Das optionale Feld nextUpdateTime wird auf Grund einer Anforderung der BNetzA nicht verwendet.
Die Aufnahme eines Zertifikats in die Sperrliste wird auch als Bestätigung für die erfolgreiche Durchführung der Sperrung verwendet. Die Sperrliste für qualifizierte Zertifikate kann vom Webserver unter http://pks.telesec.de/telesec/servlet/download_crl oder vom LDAP-Server unter ldap://pks-ldap.telesec.de/o=Deutsche Telekom AG,c=de jederzeit abgerufen werden. Die Sperrlisten für fortgeschrittene Zertifikate können vom LDAP Server unter ldap://pks-ldap.telesec.de/o=T-Systems International GmbH,c=de oder ldap://pks-ldap.telesec.de/o=T-Systems Enterprise Services GmbH,c=de jederzeit abgerufen werden.

Die Web- und LDAP-Server sind, entsprechend den Anforderungen des deutschen Signaturgesetzes (7x24) verfügbar.

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

4.11 Schlüsselhinterlegung und Wiederherstellung

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

5 Bauliche und organisatorische Maßnahmen

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

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Standort und bauliche Maßnahmen

T-Systems betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Hälften, zwei getrennt arbeitenden Energietrakten (Elektro, Klima, Wasser) mit Gebäudemanagementsystem und Notstromaggregaten sowie einem Verwaltungstrakt verfügt. Je nach Kundenanforderung kann im Trust Center ein abgestuftes Ausfallsicherungskonzept mit definierten Sicherungsstufen realisiert werden.
Die Errichtung und der Betrieb des Trust Centers erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Verbandes der Schadenversicherer e.V. (VdS) / neu: Gesamtverband der Deutschen Versicherungswirtschaft (GDV), der einschlägigen DIN-Normen zu Brandschutz, Rauchschutz und Angriffhemmung. Das Trust Center ist sicherheitstechnisch vom VdS / GDV abgenommen.
Die technischen Maßnahmen werden durch organisatorische Elemente ergänzt, die die Handhabung der sicherheitsrelevanten Techniken und Regelungen über den Zutritt zu Sicherheitszonen für Mitarbeiter und Dritte (Besucher, Fremd- und Putzkräfte), die Anlieferung von Material (Hardware, Zubehör, Betriebsmittel) und Ordnung am Arbeitsplatz sowie in Rechnerräumen beinhalten.

5.1.2 Zutritt

Im Trust Center gilt eine Zutrittsregelung die die Zutrittsrechte für Mitarbeiter, Mitarbeiter von Fremdfirmen und Gästen in den einzelnen Sicherheitszonen regelt. Der Zutritt ist zwischen den Sicherheitsbereichen nur über Personenvereinzelungsanlagen möglich. Der kontrollierte Zutritt zu den verschiedenen Sicherheitsbereichen ist weiter mit einem rechnergesteuerten Zutrittskontrollsystem geschützt. Gäste werden nur in Ausnahmefällen und nach vorheriger Anmeldung empfangen. Hier gelten besondere Sicherheitsvorschriften.

5.1.3 Stromversorgung und Klimatisierung

Die Ansaugöffnungen für die Außenluft sind so angeordnet, dass keine Schadstoffe wie Staub und Schmutz, ätzende, giftige oder leicht brennbare Gase eindringen können. Die Systeme werden mit einem sehr geringen Außenluftanteil betrieben. Die erforderlichen Zuluftöffnungen sind zugangsgeschützt. Zum Schutz gegen Luftverunreinigung durch schwebende Partikel sind Filter installiert. Die Frischluftansaugung wird ständig auf aggressive Gase überwacht. Im Notfall (z.B. Brand in der Umgebung) wird die Außenluftansaugung automatisch durch Luftklappen verschlossen.
Zum Ausfallschutz der Energieversorgung ist eine unabhängige Wechselspannungsversorgung entsprechend VDE-Vorschriften installiert. Sie bietet Schutz gegen Spannungsschwankungen, unterbrechungsfreie Kurzzeitüberbrückung, eine Langzeitüberbrückung mit zwei getrennten, ortsfeste Notstromaggregate mit einer Leistung die der Volllast des Rechenzentrums entspricht.

5.1.4 Wasserschäden

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

5.1.5 Brandschutz

Die geltenden Brandschutzbestimmungen (z.B. DIN 4102, Auflagen der örtlichen Feuerwehr, Vorschriften über Feuerresistenz, VDE-gerechte Elektroinstallation) werden eingehalten. Alle Brandschutztüren besitzen automatische Schließeinrichtungen. In Absprache mit der Feuerwehr wird nur in äußersten Notfällen mit Wasser gelöscht.
Brandabschnitte sind durch feuerbeständige Bauteile gesichert. Durchgänge durch Brandschutzwände sind mit selbsttätig schließenden Brandschutztüren ausgestattet
In Bereichen mit Doppelböden sowie abgehängten Decken sind Brandschutzwände durchgehend bis zum Geschoßboden bzw. zur Geschoßdecke ausgeführt.
In alle Systemräume, Systemoperatorräume, Archivräume, USV-Räume sowie weitere ausgewählte Raume sind Brandfrühesterkennungssystemen (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut.

5.2 Organisatorische Sicherheitsmaßnahmen

Die organisatorischen Maßnahmen der sind im Sicherheitskonzept des Public Key Service niedergelegt welches nicht öffentlich verfügbar ist. Das Sicherheitskonzept und die darin beschriebenen Maßnahmen werden regelmäßig von einer für Bestätigungen nach dem deutschen Signaturgesetz zugelassenen Bestätigungsstelle überprüft.

Die nachfolgende Aufzählung nennt einen Teil der organisatorischen Maßnahmen, aus unterschiedlichen Quellen, die zur Wahrung der Sicherheit getroffen wurden :

- Maßnahmen zur Ermittlung, Bewertung und regelmäßigen Überprüfung von Restrisiken sind im Sicherheitskonzept des Public Key Service enthalten. (7.4.1 a)
- Die Bestimmungen zur Einbindung von externen Dienstleistern stammen aus Festlegungen des Signaturgesetzes und sind in den Verträgen umgesetzt so dass deren Umsetzung von Sicherheitsmaßnahmen jederzeit vom Trust Center oder von externen Auditoren überprüft werden kann. (7.4.1 b, 7.4.1 g)
- Alle Mitarbeiter des Trust Centers sind verpflichtet die strengen internen Datenschutz- und Sicherheitsrichtlinien des Konzerns Deutsche Telekom AG einzuhalten. (7.4.1 c)
- Die Systeme des Trust Centers werden regelmäßig auf sicherheitsrelevante Veränderungen untersucht. (7.4.1 d) Alle sicherheitsrelevanten Veränderungen müssen vor Inbetriebnahme durch das Change Advisory Board des Trust Centers freigegeben werden. Sicherheitserhebliche Veränderungen müssen zusätzlich vor der Inbetriebnahme durch eine Bestätigungsstelle für SigG überprüft werden. (7.4.1 e)
- Alle sicherheitsrelevanten Prozesse sind im Sicherheitskonzept dokumentiert und geprüft. (7.4.1 f)

5.2.1 Sicherheitsmaßnahmen bei der Softwareentwicklung

Softwareentwicklung durch Mitarbeiter des Trust Centers findet in der geschützten Umgebung des Trust Centers statt. Dabei kommt ein Versionskontrollsystem zum Einsatz. Vor Beginn der Entwicklung wird das Projekt auf einzuhaltende Sicherheitsaspekte untersucht.

Bei der Auswahl externer Software wird auf vertrauenswürdige Hersteller Wert gelegt. In Bereichen in denen dies möglich ist kommen Open Source Komponenten zum Einsatz. Bei Software, die speziell für das Trust Center entwickelt wird muss der Hersteller nach Projektabschluss den Source Code im Trust Center hinterlegen.

5.3 Personelle Maßnahmen

Die Zuverlässigkeit des Personals, das im Telekom Trust Center arbeitet wird durch unabhängige Informationen regelmäßig überprüft. Das Personal besucht in regelmäßigen Abständen sowie nach der Einführung neuer Produkteigenschaften oder Prozesse Fortbildungen.

Das Personal unterliegt keinem Kostendruck oder Mengengerüst deren Einhaltung möglicherweise mit den Qualitätsanforderungen bei der Prüfung von Auftragsunterlagen konkurrieren würde. Im Sicherheitskonzept sind genaue Rollenbeschreibungen enthalten. Bei der täglichen Arbeit wird das Personal von genauen Arbeitsanweisungen unterstützt.

Alle Anforderungen des deutschen Signaturgesetzes werden vollständig erfüllt.

Eine Rollentrennung bei kritischen Prozessen wird im Sicherheitskonzept definiert. Es sind nur die minimal erforderlichen Berechtigungen zur Ausübung einer bestimmten Rolle zugewiesen. 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.

Gäste oder nicht dem Trust Center zugehöriges Personal (beispielsweise Reinigungspersonal) wird in den Räumen des Trust Centers immer durch einen Mitarbeiter des Trust Centers begleitet.

5.4 Protokollereignisse

Veränderungen im Lebenszyklus der Zertifikate (CA und Endbenutzer) werden protokolliert, dies bezieht sich im Einzelnen auf die folgenden Ereignisse:
Erzeugung
Sicherung
Speicherung
Wiederherstellung
Vernichtung
Änderungen von Hardware und Software
Protokollierungen von Ereignissen im Lebenszyklus von CA Zertifikaten:
Zertifikatsauftrag (erfolgreich / fehlgeschlagene Bearbeitung und beiliegende Dokumente)
Zertifikatserneuerung
Zertifikatssperrung
Erstellung von Zertifikaten
Sperrlisten
Protokollierung von Internen und Externen Audits.

5.5 Sicherung der Aufzeichnungen

Alle Aufzeichnungen innerhalb des T-Systems Trust Centers werden, wenn sie sich auf qualifizierte Zertifikate beziehen, gemäß den Anforderungen des deutschen Signaturgesetzes 30 Jahre lang aufbewahrt. Andere Aufzeichnungen werden zehn (10) Jahre aufbewahrt.

5.6 Schlüsselwechsel bei CA Zertifikaten

Bei Schlüsselwechseln von CA Zertifikaten ist die Generierung neuer Schlüssel und Zertifikate zu dokumentieren, und gemäß der Auflagen des jeweiligen Sicherheitskonzepts zu überwachen.

5.7 Kompromittierung privater Schlüssel von CA Zertifikaten

Bei Kompromittierung privater Schlüssel von CA Zertifikaten ist dies unverzüglich mitzuteilen. Handelt es sich um CA Zertifikate zur Ausstellung qualifizierter Zertifikate wird die Bundesnetzagentur als Zertifikatsherausgeber informiert. CA Zertifikate werden daraufhin unverzüglich gesperrt.

5.8 Einstellung des Betriebes

5.8.1 Zertifizierungsdiensteanbieter gemäß SigG

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.

5.8.2 Nicht qualifizierte Zertifikate

Eine Betriebsbeendigung kann nur durch die T-Systems Geschäftsleitung ausgesprochen werden.
Ein Beendigungsplan kann die folgenden Regelungen enthalten:

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

Wenn der Betrieb (insbesondere der Sperrdienst) nicht durch eine andere Zertifizierungsstelle übernommen wird, dann werden alle ausgestellten Zertifikate gesperrt. Für die Weiterführung des Betriebs des Sperrdienstes sind die notwendigen Vorsorgemaßnahmen getroffen.

6 Technische Sicherheitsmaßnahmen

6.1 Generierung und Installation der Schlüsselpaare

Alle Schlüsselpaare für Endanwender-Zertifikate werden in einem abgeschirmten Raum ohne externe Netzwerkanbindung auf einer sicherheitsüberprüften Hardwarekomponente oder auf der Signaturkarte des Zertifikatsinhabers selbst 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. Schlüsselgenerierung (Vorproduktion) und die Generierung und Speicherung des Zertifikats des Endanwenders erfolgen in getrennten Produktionsschritten.

Für die Schlüsselgenerierung und Schlüsselverwendung gelten die Anforderungen des Algorithmenkatalogs, der jährlich von Bundesnetzagentur und BSI aktualisiert wird. Bei Endanwender – Zertifikaten so wie bei qualifizierten CA- oder Dienste-Zertifikaten gilt der Algorithmenkatalog für die gesamte Laufzeit des Zertifikates und alle Einsatzszenarien. Bei nicht qualifizierten CA-Zertifikaten wird der Algorithmenkatalog nur zum Zeitpunkt der Schlüsselerstellung und Zertifikatsgenerierung als Entscheidungsgrundlage zur Auswahl der Algorithmen verwendet. Dies ist der Tatsache geschuldet das nicht qualifizierte CA-Zertifikate eine wesentlich längere Laufzeit haben als der Algorithmenkatalog abdeckt.

6.1.1 Generierung und Installation der Schlüsselpaare für die qualifizierte CA

Als Schlüsselträger kommen die gleichen Chipkarten zum Einsatz, die auch die Zertifikate für die Endanwender aufnehmen. Es werden Chipkarten nach dem Produktionsschritt Vorproduktion verwendet. Diese enthalten bereits die nötigen Schlüsselpaare und Zertifikate mit denen die Qualität dieser Schlüsselpaare überprüft wird.

Die Generierung von CA- und Dienste-Zertifikaten erfolgt durch die Bundesnetzagentur. Dafür wird von den Administratoren des Trust Centers und dem zukünftigen Zertifikatsinhaber des CA- oder Dienste-Zertifikats(Leiter Zertifizierungsdiensteanbieter oder eine von ihm bestimmte Person), im Vier-Augen-Prinzip ein PKCS#10-Request erzeugt. Die Generierung des PKCS#10 Requests erfolgt unter Verwendung einer nach ITSEC evaluierten und gemäß SigG bestätigten Signaturanwendungskomponente. Die Request-Generierung erfolgt auf einem gesonderten Laptop der nur für diesen Zweck betrieben wird.

6.1.2 Generierung und Installation der Schlüsselpaare für die nicht qualifizierte CA

Als Schlüsselträger kommen für nicht die qualifizierte CA Chipkarten-Rohlinge zum Einsatz aus denen im Laufe dieses Prozesses Signaturkarten erzeugt werden, deren Funktionalität den Signaturkarten der Endanwender oder der qualifizierten CA entsprechen.
Dazu wird im abgeschirmten Bereich des Trust Centers durch zwei Mitarbeiter ein Signaturschlüssel-Paar, bestehend aus privatem und öffentlichen Schlüssel erzeugt, und auf einer Schlüsselgenerator-Backup-Chipkarte abgelegt. Der private Schlüssel ist auf dieser Chipkarte so gespeichert das er nur nach Eingabe von

zwei PIN's im Vier-Augen-Prinzip ausgelesen werden kann. Mit dieser Chipkarte wird der Schlüsselgenerator gestartet. Danach gibt er für jede Abfrage eines neuen Schlüsselpaares immer den gleichen Schlüssel heraus. Auf diese Weise wird die Produktion von Vorprodukten gestartet und es werden somit mehrere Chipkarten mit dem gleichen Schlüsselpaar erzeugt.
Die Generierung des CA-Zertifikates erfolgt auf Basis eines PKCS#10 Requests, der mittels des gleichen Prozesses erzeugt wird wie ein PKCS#10 Request für eine qualifizierte CA.

6.2 Generierung und Erneuerung von CA-Zertifikaten

Das Trust Center sorgt dafür das so lange der Dienst betrieben wird, jederzeit gültige CA- und Dienste-Zertifikate vorhanden sind. Rechtzeitig vor Ablauf werden neue Zertifikate erzeugt bzw. bei der BNetzA beantragt. Nach Erhalt dieser Zertifikate werden diese auf die zugehörigen Chipkarten gespeichert und auf der Webseite http://www.telesec.de/pks im Bereich Support -> FAQ veröffentlicht. Zusätzlich erhalten alle Personen und Organisationen, die sich beim PKS Support als Interessenten für den Newsletter registriert haben, eine Email das ein CA-Wechsel bevorsteht.
So lange die neu erstellten CA- oder Dienste-Zertifikate nicht benötigt werden sind diese in versiegelten Umschlägen in Tresoren gelagert auf die nur die Zertifikatsinhaber Zugriff haben.
Jeder Interessierte kann sich mit einer Email an PKS-Support@t-systems.com als Empfänger für den Newsletter registrieren. Kurz vor dem Ablauf des CA- oder Dienste-Zertifikates wird dieses dann im Betrieb durch ein neu generiertes Zertifikat ersetzt. Nicht mehr benötigte CA- oder Dienste-Zertifikate (so wie bei nicht qualifizierten CA-Zertifikaten ggf. vorhandene Backups der privaten Schlüssel) werden unbrauchbar gemacht in dem die Chipkarte auf dem sie gespeichert sind vernichtet wird.

6.2.1 Generierung von qualifizierten CA-Zertifikaten

Die Generierung von qualifizierten CA- und Dienste-Zertifikaten erfolgt durch die Bundesnetzagentur und liegt außerhalb des Einflusses von T-Systems. Die Veröffentlichung dieser Zertifikate und deren Gültigkeitsüberprüfung gemäß den auf der Webseite des Verzeichnisdienstes der Bundesnetzagentur http://www.nrca-ds.de angegebenen Informationen.

6.2.2 Generierung von fortgeschrittenen CA-Zertifikaten

Der PKCS#10 Request wird von einem Root-Zertifikat auf einem System signiert welches besonders abgesichert ist. Siehe dazu die Beschreibung in CP und CPS zum Root-Zertifikat Deutsche Telekom Root CA 2 auf der Webseite http://www.telesec.de/pki/roots.html.
Das Root-Zertifikat und die Prozesse zur Zertifikatsgenerierung nicht qualifizierter CA-Zertifikate sind gemäß Webtrust Zertifiziert und werden regelmäßig überprüft.
Die Veröffentlichung dieser Zertifikate erfolgt mittels LDAP über die URL ldap://ldap.telesec.de. Auf diesem LDAP-Server liegen ebenfalls die Sperrlisten (ARL's) für die Gültigkeitsüberprüfung.

6.3 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.

Backup-Chipkarten für fortgeschrittene CA-Schlüssel sind so eingestellt das der private Schlüssel des CA-Zertifikats nur nach der Eingabe von zwei PIN's im Vier-Augen-Prinzip ausgelesen werden kann. Auf der fortgeschrittenen CA-Signaturkarte ist der private Schlüssel nicht auslesbar gespeichert.

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. Die Entschlüsselung erfolgt im Vier-Augen-Prinzip durch die Anmeldung von zwei Personen mit deren persönlichen Chipkarten.

CA- und Dienste-Signaturkarten kommen nur in der besonders gesicherten Umgebung des Trust Centers zum Einsatz und werden dort nur für die Ausstellung von Zertifikaten und Sperrlisten, so wie bei qualifizierten Zertifikaten zur Signatur von Statusauskünften (OCSP) verwendet.

6.4 Sicherheitsmaßnahmen an technischen Komponenten

Im Trust Center von T-Systems kommen ausschließlich Systeme zum Einsatz, die für die Verwendung in Rechenzentren vorgesehen sind. Auf den Systemen sind, zusätzlich zum Betriebssystem, nur die für den Betrieb notwendigen Softwarekomponenten installiert. Alle Kernsysteme des Trust Centers sind redundant ausgelegt. Die Hardware wird auf Fehlfunktionen und defekte überwacht und regelmäßig getauscht. Die vorgenommenen Einstellungen werden regelmäßig, automatisch überprüft so dass Veränderungen erkannt werden. Die Funktionen der angebotenen Dienste werden in kurzen Abständen überprüft. Sicherheitsrelevante Veränderungen, Fehlfunktionen oder defekte werden nach auftreten sofort an die zuständigen Personen weitergegeben so dass diese angemessen reagieren können.

Alle Systeme werden in Zugangsgeschützen Bereichen betrieben so dass physische Veränderungen an den Systemen oder die Manipulation von Datenträgern ausgeschlossen sind.

Alle wichtigen Aktionen auf allen Servern werden zentral protokolliert. Die Protokolle werden nach Abschluss integritätsgeschützt so dass nachträgliche Veränderungen erkannt werden.

Die Einstellungen der Systeme werden regelmäßig von einer Bestätigungsstelle für SigG überprüft.

6.4.1 Datensicherung

Alle wichtigen Daten des Zertifizierungsdienstes werden regelmäßig gesichert. Die Verwendbarkeit der Datensicherungen wird stichprobenartig überprüft. Zur Sicherstellung des Betriebs bei eintreten eines katastrophalen Ereignisses werden Datensicherungen in bestimmten Abständen ausgelagert.

6.4.2 Zugangsschutz zu den Systemen

Auf den Systemen des Trust Centers werden Betriebssysteme eingesetzt, die die Durchsetzung von Sicherheitseinstellungen unterstützen. Keines der Systeme kann ohne Benutzeranmeldung verwendet werden. Sicherheitskritische Einstellungen (beispielsweise Nutzkonten) können nur im Vier-Augen-Prinzip verändert werden.

Besonders sicherheitskritische Applikationen (beispielweise die Zertifikatsgenerierung) erfordern zusätzliche Authentisierungen des Bedieners im Trust Center.

6.4.3 Verwendung sicherheitsüberprüfter Komponenten

Das Signaturgesetz fordert für verschiedene Zwecke den Einsatz sicherheitsüberprüfter Komponenten. Die nachfolgende Aufstellung zeigt einen Teil der verwendeten Komponenten:

- Die eingesetzten Chipkarten zur Generierung und Speicherung privater Schlüssel (mit Ausnahme der Backup-Chipkarten für fortgeschrittene CA) sind nach Common Criteria EAL4+ evaluiert und gemäß dem deutschen SigG bestätigt. Zum Zeitpunkt der Erstellung dieser CPS kommen zwei unterschiedliche Chipkartentypen zum Einsatz. Es handelt sich dabei um die *TCOS 3.0 SignatureCard, Version 1.1* und die *TCOS 3.0 SignatureCard, Version 2.0*. Die Bestätigungen sind auf der Internetseite der Bundesnetzagentur veröffentlicht.

- Die Signaturanwendungskomponente *TCrypt-TCM, Version 2.0*, die zur Signatur von Endanwender-Zertifikaten und zur Signatur von PKCS#10 Requests verwendet wird ist nach ITSEC E2 Mechanismenstärke hoch evaluiert und gemäß dem deutschen SigG bestätigt. Die Bestätigung ist auf der Internetseite der Bundesnetzagentur veröffentlicht.

- Der Schlüsselgenerator zur Erstellung von Schlüsseln für qualifizierte CA- und Dienste-Zertifikate ist nach ITSEC E4 Mechanismenstärke hoch evaluiert und gemäß dem deutschen SigG bestätigt. Die Bestätigung des Schlüsselgenerators *Trust Center Schlüsselgenerator TCSg, Version 2.0* ist auf der Internetseite der Bundesnetzagentur veröffentlicht. Für die Erzeugung der Schlüssel für nicht qualifizierte CA-Zertifikate kommt eine geringfügig abgewandelte Version zum Einsatz, die den Schlüssel in einer Backup-Chipkarte speichert.

6.5 Netzwerktechnische Sicherheitsmaßnahmen

Alle Netzwerkkernkomponenten sind redundant ausgelegt. Die Anbindungen an das Internet und an andere Kommunikationsnetze sind redundant ausgelegt und verfügen über die für den Betrieb notwendige Bandbreite. Die Netzwerkkomponenten werden regelmäßig, automatisch auf Fehlfunktionen, Defekt, oder Manipulation überwacht.

Das Netzwerk des Trust Centers ist in mehrere Zonen mit unterschiedlichen Sicherheitsanforderungen aufgeteilt. Jede Zone kann mit einer anderen Zone nur über eine Firewall kommunizieren. In den Firewalls sind nur die minimal erforderlichen Regeln für die Kommunikation zwischen den verschiedenen Zonen zugelassen.

Die Kommunikation zwischen verschiedenen Standorten des Trust Centers erfolgt mittels verschlüsselter VPN Verbindungen. Für VPN Verbindungen kommen Sitzungsschlüssel zum Einsatz die regelmäßig gewechselt werden. Die Verschlüsselungsgeräte nehmen Verbindungen nur von den in der eigenen White List enthaltenen anderen Verschlüsselungsgeräten an.

Die Einstellungen der Netzwerkkomponenten werden regelmäßig von einer Bestätigungsstelle für SigG überprüft.

7 Zertifikatsprofile und Sperrlistenprofile

7.1 Zertifikatsprofil

Die Spezifikation des Zertifikatsprofils für qualifizierte Signaturen und Attribut-Zertifikate ist auf den TeleSec PKS Webseiten verfügbar unter
https://www.telesec.de/pks/ → Support → Downloadbereich → Technische Dokumentation

Die Spezifikation des Zertifikatsprofils für fortgeschrittene Zertifikate ist auf den TeleSec PKS Webseiten verfügbar unter
https://www.telesec.de/pks/ → Support → Downloadbereich → Technische Dokumentation

7.2 Sperrlistenprofil

Die Spezifikation der Sperrliste (CRL) ist auf den TeleSec PKS Webseiten verfügbar unter
https://www.telesec.de/pks/→ Support → Downloadbereich → Technische Dokumentation

7.3 OCSP Profil

Die Spezifikation des OCSP-Responders ist auf den TeleSec PKS Webseiten verfügbar unter
https://www.telesec.de/pks/ → Support → Downloadbereich → Technische 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. Die Überprüfung der Anforderungen von ETSI TS 102 042 erfolgt einmal pro Jahr.

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

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

Der Leiter des Zertifizierungsdiensteanbieters ist verantwortlich für die korrekte Umsetzung der Bestimmungen aus den einschlägigen Gesetzen, internationalen Standards, dem Sicherheitskonzept und den internen Verfahrens- und Arbeitsanweisungen. Er prüft diese Umsetzung regelmäßig durch die Beauftragung von internen Audits, deren Ergebnisse alle 3 Jahre bei externen Audits vorgelegt werden.

9 Sonstige geschäftliche und rechtliche Angelegenheiten

9.1 Preise

Die aktuelle Preisliste ist jederzeit auf den TeleSec PKS Webseiten verfügbar unter
https://www.telesec.de/pks/ → Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.2 Finanzielle Verantwortlichkeiten

Die finanziellen Verantwortlichkeiten werden in den Allgemeinen Geschäftsbedingungen (AGB) für den TeleSec Public Key Service beschrieben, diese sind jederzeit verfügbar unter
https://www.telesec.de/pks/ → Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

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 International 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 International GmbH jegliche Haftung ab.

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

9.6 Haftungsbeschränkungen

Haftungsfragen sind in den Allgemeinen Geschäftsbedingungen (AGB) für den TeleSec Public Key Service geregelt, diese sind jederzeit unter der folgenden Adresse verfügbar
https://www.telesec.de/pks/→ Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.7 Schadensersatz

Schadensersatzansprüche sind in den Allgemeinen Geschäftsbedingungen (AGB) für den TeleSec Public Key Service geregelt, dies sind jederzeit unter der folgenden Adresse verfügbar
https://www.telesec.de/pks/→ Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.8 Fristen und Kündigung

Fristen und Kündigungen sind in den Allgemeinen Geschäftsbedingungen (AGB) für den TeleSec Public Key Service geregelt, dies sind jederzeit unter der folgenden Adresse verfügbar
https://www.telesec.de/pks/ → Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.9 Änderungen der CPS

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich die T-Systems International GmbH das Recht vor, Änderungen und Anpassungen an dieser CPS durchzuführen. Änderungen der CPS werden auf der Internetseite (https://www.telesec.de/pks) 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-Systems 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 dieser CPS werden durch die Mitarbeiter des Trust Centers vorgenommen. Nach Durchführung der Änderungen wird das Dokument dem Change Advisory Board des Trust Centers, zu welchem unter anderem der Leiter des Trust Centers gehört, vorgelegt. Das Change Advisory Board überprüft die Änderung und gibt die CPS zur Veröffentlichung frei.

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

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. Die aktuelle Version dieser CPS ist jederzeit von der URL http://pks.telesec.de/cps/cps.pdf downloadbar.

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 zugesichert 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 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.