Public Key Service

Certificate Practice Statement

Version: 3.5
Stand: 01.08.2018
Status: Freigegeben

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

T · · Systems ·

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
3.3	08.04.2016	TH, LK, JS	Review 2016
3.3	08.04.2016	DD	Freigabe
3.4	01.08.2017	LK, TH JS	Review, Überarbeitung für eIDAS
3.5	01.08.2018	JS	Review, Überarbeitung nach letztem Audit

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 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.

Die Deutsche Telekom AG betreibt seit 1994 ein Trust Center, das 1998 als erstes Trust Center bundesweit die Genehmigung zur Ausgabe von Zertifikaten für die digitale Signatur gemäß dem damaligen Deutschen Signaturgesetz erhielt. Mit dieser Genehmigung wurde zu Beginn des Jahres 1999 der Public Key Service (PKS) etabliert, stetig weiterentwickelt und ist seit 1.7.2016 konform zu der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS).
Seit der Betriebsaufnahme hat das Telekom Trust Center mehr als 200 Millionen Zertifikate ausgestellt. Zu den vom Telekom Trust Center angebotenen Leistungen gehört der TeleSec Public Key Service (PKS), der die Ausstellung qualifizierter Zertifikate gemäß der EU Verordnung eIDAS 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 International GmbH. Die aktuelle Version der PKS CPS stellt den tatsächlichen Stand der Zertifizierungstätigkeit dar und gilt ausschließlich für die Dienstleistung TeleSec PKS.

Der in Kapitel 1.5.1 genannte Bereich ist verantwortlich dafür, dass die beschriebenen Abläufe, Tätigkeiten, Systeme, Rollen und Sicherheitsmaßnahmen auch für den Fall durchgesetzt werden, dass diese ausgelagert werden.

Im Einzelnen enthält die PKS CPS die folgenden Aspekte:

- Bedeutung und Verwendung von qualifizierten Public Key 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.

Kunden können qualifizierte Signaturzertifikate durch Attribute erweitern um die Verwendung des entsprechenden Signaturschlüssels einzuschränken oder zusätzliche Informationen (z. B: Vertretungsmacht) kenntlich zu machen.

1.2 Dokumentenidentifikation

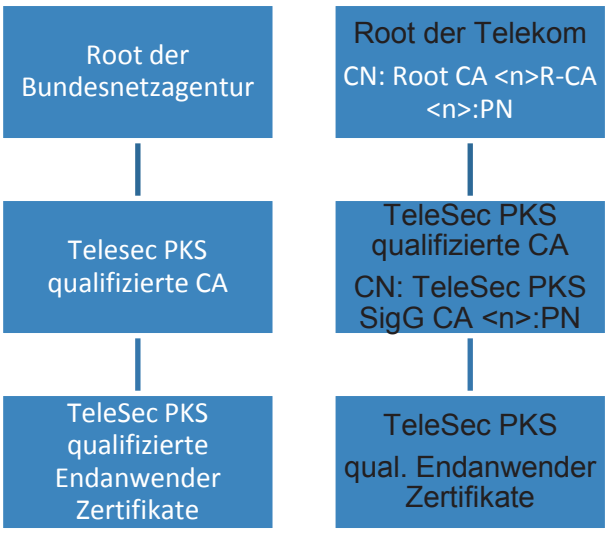
Name:	Zertifizierungsrichtlinie für TeleSec Public Key Service ® (PKS CPS)
Version:	3.4
Datum	01.08.2017
Objektbezeichnung (Object Identifier)	1.3.6.1.4.1.7879.13.27

1.3 PKI Beteiligte

1.3.1 Zertifizierungsstellen

1.3.1.1 Qualifizierte Zertifikate

Der TeleSec Public Key Service für qualifizierte 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 nach den Vorgaben der eIDAS Verordnung durch T-Systems International GmbH erstellt. Um den Status eines qualifizierten Vertrauensdienstes zu erlagen, werden die Zertifikate nach einer eIDAS-Konformitätsbetätigung in die Trustlist der Europäischen Union[2] aufgenommen und veröffentlicht. Die Grafik oben veranschaulicht die Zertifizierungshierarchie anhand von beispielhaft ausgewählten Zertifikaten.

Gemäß der eIDAS Verordnung stellt die PKS CA nur qualifizierte Zertifikate 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.

Als Schlüsselmittel für die Endkundenzertifikate kommen ausschließlich zertifizierte QSCD zum Einsatz. Die Schlüssel werden im Rahmen der Kartenproduktion durch evaluierte Schlüsselgeneratoren auf der jeweiligen Karte selbst erzeugt. Die Gültigkeit der Zertifizierung der eingesetzten QSCD wird regelmäßig sowie bei Bedarf in den internen und externen Audits geprüft. Vor Ablauf einer Zertifizierung wird rechtzeitig der Einsatz einer anderen zertifizierten QSCD geplant und umgesetzt.

Zertifikate für technische Tests können nach Absprache mit dem TSP aus der Testumgebung bezogen werden. Diese sind eindeutig als Testzertifikate gekennzeichnet.

Für qualifizierte Zertifikate gelten die Bestimmungen der EU Verordnung Nr. 910/2014 (eIDAS).

1.3.1.2 Nicht qualifizierte Zertifikate

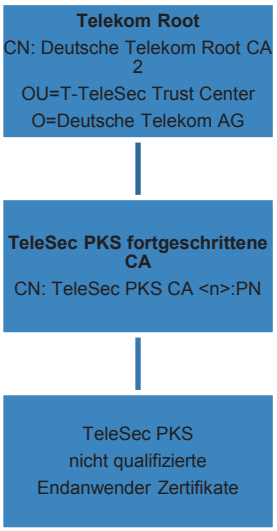
Die Ausstellung nicht qualifizierter Zertifikate, zusätzlich zu einem qualifizierten Zertifikat ist optional. Diese werden teilweise auch als fortgeschrittene Zertifikate Bezeichnet. Kunden, die speziellen geschlossenen Benutzergruppen angehören erhalten möglicherweise keine nicht qualifizierten Zertifikate. Dies ist abhängig von

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

[2] Regelungen zur Trustlist können in der eIDAS-Verordnung eingesehen werden.

den Vereinbarungen mit dem Leiter der Benutzergruppe. Eine nachträgliche Erstellung nicht qualifizierter Zertifikate ist nicht möglich.

Der TeleSec Public Key Service für nicht qualifizierte 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 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 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 OCSP-Responder und CRL-Server des PKI-Service TeleSec PKS

Von jeder gültigen CA zur Ausstellung qualifizierter Zertifikate werden für die Erbringung des OCSP-Service Zertifikate für den OCSP-Responder ausgestellt. Dieser Zertifikatstyp steht ausschließlich nur dem PKI-Betreiber T-Systems zur Verfügung.

Die CRL für den nicht qualifizierten Dienst wird durch die jeweilige CA signiert.

1.3.3 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 Prüfstellen gemäß den Anforderungen der eIDAS-Verordnung 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. Für Mitarbeiter aus Kommunen, Landes- und Bundesbehörden in Deutschland ist außerdem die Identifizierung durch das BehördenIdent-Verfahren verfügbar.
Die Registrierungsstellen der T-Systems haben insbesondere folgende Aufgaben:

- Entgegennahme von Aufträgen und Prüfung der Identifikationsunterlagen,
- Prüfen der Dokumente auf Echtheit und Vollständigkeit,
- Identitätsprüfung

Sie werden durch entsprechende Verträge auf die jeweils gültigen gesetzlichen Grundlagen und den Datenschutz verpflichtet.

1.3.4 Zertifikatsinhaber

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

1.3.5 Vertrauende Dritte

Vertrauende Dritte sind natürliche Personen oder Subjekte, die sich auf die Vertrauenswürdigkeit der ausgestellten Zertifikate verlassen. Zur Nutzung und Verifikation der Zertifikate durch Dritte z.B. zur Verschlüsselung oder Signaturprüfung stehen die Zertifikate und Sperrinformationen zum Abruf in den Verzeichnissen bereit.

1.3.6 Weitere Beteiligte

1.3.6.1 Identitätsprüfer

Identitätsprüfer sind die Notare im Falle des Notaridents, Mitarbeiter der Deutschen Post im Fall des Verfahrens PostIdent oder die Mitarbeiter der Behörden im Fall des Verfahrens BehördenIdent.

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 der eIDAS Verordnung eingesetzt.
Qualifizierte Benutzerzertifikate für die diese CPS gilt entsprechen der Policy QCP-n-qcsd.
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 Kompromittierung des verwendeten Schlüsselmaterials.

1.4.3 Fortgeschrittene Zertifikate

TeleSec PKS fortgeschrittene Zertifikate werden zur Authentisierung, zur Verschlüsselung und für fortgeschrittene Signaturen 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 kein OCSP-Service angeboten (vgl. Kap. 2.1).

1.4.4 Gültigkeitsmodell

Zur Prüfung der Gültigkeit einer Signatur bzw. eines Zertifikates existieren zwei unterschiedliche Gültigkeitsmodelle. Bedingt durch die Festlegung durch das deutsche Signaturgesetz gilt für alle Endanwender Zertifikate, die bis zum Juli 2017 ausgestellt wurden das Kettenmodell.
Das Kettenmodell besagt, dass 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.

Ab Inbetriebnahme der eIDAS konformen Zertifizierungshierarchie am 01. August 2017 gilt für Endanwenderzertifikate das Schalenmodell.

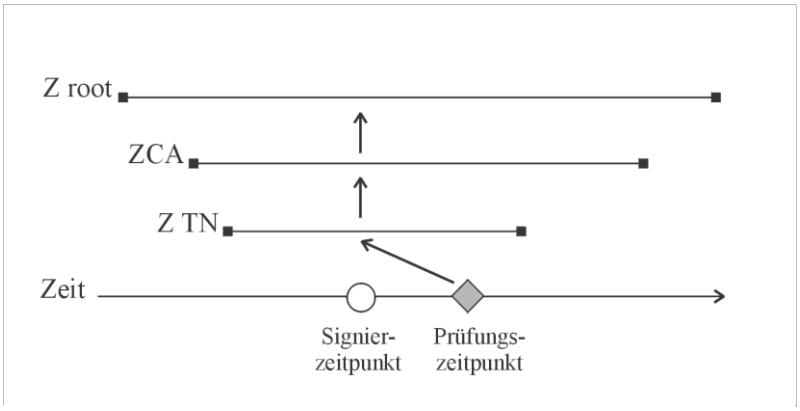


Abbildung 1: Schalenmodell

Das Schalenmodell besagt, dass alle Zertifikat zum Zeitpunkt der zu prüfenden Signatur gültig gewesen sein müssen. Das bedeutet, zum Signaturzeitpunkt eines Dokumentes müssen alle Zertifikat in der Zertifikatshierarchie gültig gewesen sein.

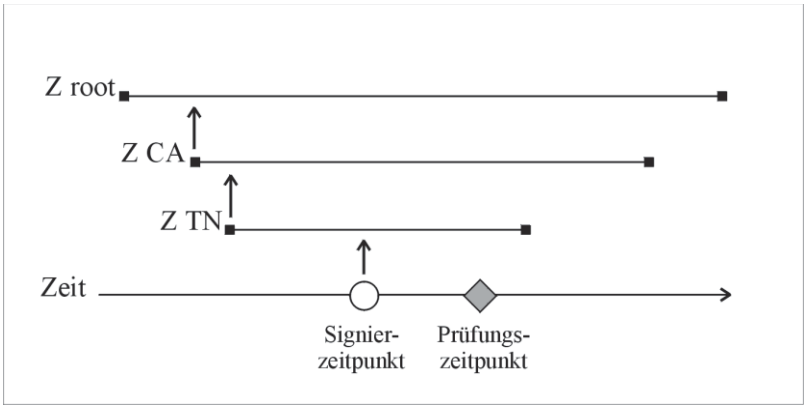


Abbildung 2: Kettenmodell

1.5 Organisation zur Verwaltung dieses Dokuments

1.5.1 Zuständigkeit für das Dokument

Diese CPS wurde von T-Systems International GmbH herausgegeben und wird von dieser gepflegt.

1.5.2 Kontaktinformationen

Adresse:
T-Systems International GmbH

Untere Industriestraße 20, 57250 Netphen
Postfach 1465, 57238 Netphen

Telefon: +49 (0) 1805 268 204 [3]

Sperrhotline:

Aus Deutschland	116 116
Aus dem Ausland	+49 30 4050 4050

E-Mail: telesec_support@t-systems.com

WWW: http://www.telesec.de

[3] 14 Ct/Minute aus dem deutschen Festnetz, max. 42 Ct/Minute aus dem Mobilfunk

1.5.3 Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP entscheidet

In Kapitel 1.5.1 ist die Organisation aufgeführt, die sich verantwortlich zeigt, dass diese CP/CPS oder Dokumente, die dieses Dokument ergänzen oder untergeordnet sind, mit der Zertifizierungsrichtlinie (Certificate Policy, CP) vereinbar sind.

1.5.4 Genehmigungsverfahren dieses Dokuments

Dieses Dokument wird durch den im Betriebsleitfaden des Trust Centers definierten Qualitätssicherungs- und Freigabeprozesses behandelt. Dieser sieht ein bei Anpassungen eine Qualitätssicherung mit anschließender Freigabe durch den Leiter des Trust Centers vor.

Die vorliegende CPS wird unabhängig von weiteren Änderungen einem jährlichen Review unterzogen. Das jährliche Review ist in der Änderungshistorie des CPS zu vermerken. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden.

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
eIDAS	EU Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.
ETSI	Europäisches Institut für Telekommunikationsnormen
FIPS	Federal Information Processing Standard ist die Bezeichnung für öffentlich bekanntgegebene Standards der Vereinigten Staaten.
LDAP	Lightweight Access Protocol
LRA	Lokale RA
OCSP	Online Certificate Status Protocol
PKD	Public Key Directory
PKS	Public Key Service
QCSD	Signaturerstellungseinheit für qualifizierte Signaturen gemäß der eIDAS Verordnung.
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
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 der eIDAS-Verordnung) zu erreichen:

- http://www.telesec.de/signaturkarte/ → 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 ermöglichet der OCSP-Service das **Nachprüfen des Status aller ausgestellten qualifizierten Zertifikate** (gesperrt/nicht gesperrt).
Für die nicht qualifizierten Zertifikate zur Signatur, Verschlüsselung und Authentisierung wird eine Sperrliste (CRL) aber kein OCSP-Service angeboten. Für qualifizierte Zertifikate wird ausschließlich OCSP zur Statusüberprüfung angeboten.

2.2 Veröffentlichung von Informationen

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

- 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 bei sicherheitskritischen Vorfällen 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 Abruf der Zertifikate und Sperrlisten erfolgt über LDAPv3, der Zugriff auf die OCSP-Responder erfolgt per http. Alle Zugriffe unterliegen keiner Zugriffsbeschränkung. Der Lesezugriff auf diese Informationen unterliegt keiner Beschränkung.

Die Integrität und Authentizität der Sperrlisten und OCSP-Auskünfte wird durch die Signatur mit vertrauenswürdigen Signern gewährleistet. (Siehe Kapitel 1.3.2.)

Der Zertifikatsstatus-Service steht rund um die Uhr an 7 Tagen die Woche zur Verfügung. Die Antwortzeit des OCSP-Responders beträgt unter normalen Betriebsbedingungen weniger als 10 Sekunden.

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)
- email (Zertifikatserweiterung)

Als Zeichensatz wird ISO-8859-1 unterstützt.

E-Mail-Adressen dürfen nur dann ins Zertifikat aufgenommen werden, sofern der Zertifikatsinhaber den Zugriff auf das angegebene E-Mail-Postfach bestätigt hat.

Wenn der Auftraggeber ein Pseudonym als Name wünscht, wird zusätzlich das Attribut Pseudonym in das Zertifikat eingetragen. 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.
- Falls der Name für die Eintragung ins Zertifikat zu lang ist wird er durch das Trust Center gekürzt.

3.3 Pseudonymität / Anonymität

Auf expliziten Wunsch kann dem Auftraggeber auch ein pseudonymisiertes 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 CA“, politische Parolen, Namen, die Berechtigungen suggerieren, die der Zertifikatsinhaber nicht besitzt).

Der Zertifizierungsdiensteanbieter übermittelt die Identität eines Signaturschlüssel-, Verschlüsselungsschlüssel- und Authentisierungsschlüssel-Inhabers mit Pseudonym an die zuständigen Stellen soweit dies der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Auflagen der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.

3.4 Erkennung, Authentifizierung und Rolle von Markennamen

Nicht anwendbar, da Zertifikate nur für natürliche Personen ausgestellt werden, welche im Subject-DN den Namen der Person enthalten.

3.5 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.

Die Art des Ausweisdokumentes sowie die Ausweisnummer und die Gültigkeitsdaten des Ausweises werden auf dem Antragsformular aufgeführt und in der Datenbank gespeichert. Eine Kopie des Ausweisdokumentes muss dem Antrag beigefügt sein und wird im Archiv des Trust Centers abgelegt.

Als Identifizierungsdaten werden Name, Meldeanschrift, Geburtsdatum und Geburtsort des Antragstellers erfasst und somit eine eindeutige Identifizierung gewährleistet.

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.

3.6 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.

3.7 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 Auftragsformulars.

Eine unverzügliche Sperrung des Zertifikates kann durch Anruf der Sperrhotline erreicht werden, die 7x24h betrieben wird. Für eine telefonische Sperrung ist die „Tele-PIN“ des Zertifikates notwendig. Die Tele-PIN wird durch das Auftragssystem festgelegt und dem Auftraggeber während des Beauftragungsprozesses mitgeteilt. Die Tele-PIN 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 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 von nicht qualifizierten Zertifikaten

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

4.2 Bearbeitung von Zertifikatsaufträgen

Auf Grund des technischen Fortschritts werden die Algorithmen der verwendeten Schlüssel und Signaturalgorithmen regelmäßig angepasst. Die folgende Tabelle zeigt einen Überblick wann welche Schlüssel verwendet wurden.

Schlüssel	Verwendet bis/seit
RSA 1024 Bit	31.12.2007
RSA 2048 Bit	31.12.2014
Elliptische Kurven	Verwendet seit 15.01.2013

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 Algorithmenkatalog ergänzen die hier getätigten Angaben zu der maximalen Gültigkeitsdauer und haben den hier getätigten Angaben Vorrang.

Nicht qualifizierte Endanwenderzertifikate haben den gleichen Gültigkeitszeitraum wie das qualifizierte Zertifikat der gleichen Chipkarte.

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 Konformitätsbewertungsstelle gemäß eIDAS kontrolliert.

Alle Auftragsunterlagen zur Aufträgen, welche vor dem 31. Juli 2017 produziert wurden, 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. Auftragsunterlagen zu Aufträgen, welche ab dem 1.August 2017 produziert wurden, werden im Trust Center entsprechend den Bestimmungen des Vertrauensdienstegesetzes archiviert. Bei Folgeaufträgen gilt die Aufbewahrungsfrist des Zertifikates mit der längsten Archivierungsdauer.

Durch die Archivierung dieser Unterlagen sind auch die Aufträge für die nicht qualifizierten Zertifikate mit archiviert.

Die rein digitale Übermittlung eines Neuauftrags zur Erstellung qualifizierter Zertifikate wird 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 nicht qualifizierten Zertifikaten

Nicht qualifizierte 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 erfolgt im Regelfall durch den Versand der persönlichen Chipkarte des Zertifikatsinhabers im verschlossenen Umschlag an die von ihm im Auftrag angegebene Lieferanschrift.

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 erstmaligen 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 der eIDAS-Verordnung, 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.

Die Übermittlung der Empfangsbestätigung kann vom Kunden online (über ein Webformular) oder auf dem Postweg vorgenommen werden. Für die Bearbeitung einer auf dem Postweg eingegangen Empfangsbestätigung werden zusätzliche Anlagen (Kopie Personalausweis oder Kopie Auftragsunterlagen) benötigt.

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.
Nicht qualifizierte Zertifikate werden 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/signaturkarte/ → Support → Downloadbereich → Hinweise heruntergeladen werden.

Darüber hinaus unterliegen 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
- 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 3.6 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) 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 Zertifikats:

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 eingetragen wurde (siehe Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**).
    - Für berufsbezogene oder sonstige Angaben zuständige Stelle, falls eine berufsbezogene oder sonstige Angabe in das qualifizierte Zertifikat aufgenommen wurde (siehe Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**).
    - 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 die Tele-PIN erforderlich.

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/signaturkarte/ → Sperrservice.

Auch im Falle von Systemdefekten, Servicearbeiten oder und anderen Faktoren, die außerhalb dem Einflussbereich 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 für qualifizierte Zertifikate nicht zulässig 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 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) zur Statusprüfung qualifizierter Zertifikate 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 nicht qualifizierte Zertifikate werden in die Sperrliste (CRL) aufgenommen, die regelmäßig mindestens alle 6 Stunden erneuert wird.
Die Aufnahme eines Zertifikats in die Sperrliste wird als Bestätigung für die erfolgreiche Durchführung der Sperrung verwendet. Die Sperrliste für fortgeschrittene Zertifikate kann vom LDAP Server unter ldap://pks-ldap.telesec.de/o=T-Systems International GmbH,c=de jederzeit abgerufen werden

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

4.11 Schlüsselhinterlegung und Wiederherstellung

Die Hinterlegung und Wiederherstellung von Schlüsseln wird aus Sicherheitsgründen nicht angeboten.

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.
Die angewendeten physikalischen, organisatorischen und personellen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept nach IT-Grundschutz festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen.

Die für den operativen Betrieb notwendigen Sicherheitsmaßnahmen sind in dem Service- und Organisations-Handbuch sowie den Betriebsleitlinien des Trust Centers beschrieben.

Die Anforderungen aus ETSI EN 319 401 Kap. 5, 6.3 und 7.3 sind umgesetzt, d.h. es sind Festlegungen

- zur Risikobewertung im Rahmen des ISMS,
- zu den Richtlinien zur Informationssicherheit,
- zum Asset-Management

beschrieben.

5.1 Physikalische Sicherheitsmaßnahmen

Die Produktion von Signaturkarten erfolgt im Trust Center der T-Sytems. Das Trust Center ist als Zertifizierungsstelle eIDAS-konform und erfüllt somit sehr hohe Ansprüche an die physikalische Sicherheit. Die Maßnahmen sind detailliert im Sicherheitskonzept beschrieben. Die Anforderungen aus ETSI EN 319 401 Kap. 7.6 sind umgesetzt.

5.1.1 Standort und bauliche Maßnahmen

T-Systems betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Teilen, zwei getrennt arbeitenden Energietrakten (Elektro, Klima, Wasser) mit Gebäudemanagementsystem und Notstromaggregaten verfügt.
Die Errichtung und der Betrieb des Trust Centers erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Gesamtverband der Deutschen Versicherungswirtschaft (GDV), der einschlägigen DIN-Normen zu Brandschutz, Rauchschutz und Angriffhemmung.
Das Trust Center ist sicherheitstechnisch vom 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 zu den Sicherheitsbereichen ist 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.

5.1.6 Aufbewahrung von Datenträgern

Datenträger, die Produktionssoftware und -daten, Audit-, Archiv- oder Sicherungsinformationen enthalten, werden in Räumen gelagert, die mit den entsprechenden physischen Zutrittskontrollen versehen sind und Schutz vor Unfallschäden (z.B. Wasser-, Brand- und elektromagnetische Schäden) bieten.

Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen und vorgenommene Sperrungen, werden bis zum Ablauf der gesetzlichen Aufbewahrungsfrist gespeichert.

Audit- und Event Logging Daten werden entsprechend den aktuellen gesetzlichen Bestimmungen archiviert.

5.1.7 Entsorgung

Vertrauliche Dokumente und Materialien werden vor ihrer Entsorgung physisch zerstört. Datenträger, die vertrauliche Informationen enthalten, werden vor ihrer Entsorgung derart behandelt, dass diese Daten nicht auslesbar oder wieder herstellbar sind. Kryptografische Geräte werden vor ihrer Entsorgung gemäß den Richtlinien des Herstellers physisch vernichtet. Andere Abfälle werden gemäß den regulären Entsorgungsrichtlinien von T-Systems entsorgt.

5.1.8 Externe Sicherung

T-Systems führt routinemäßige Sicherungen von kritischen Systemdaten, Audit-Protokolldaten und anderen vertraulichen Informationen durch. Die Sicherungskopien werden räumlich getrennt von den Ursprungsdaten gelagert.

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 Konformitätsbewertungsstelle gemäß eIDAS 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.
- Die Bestimmungen zur Einbindung von externen Dienstleistern ist entsprechend den gültigen Gesetzen und Verordnungen in den Verträgen umgesetzt so dass die Einhaltung von Sicherheitsmaßnahmen jederzeit vom Trust Center oder von externen Auditoren überprüft werden kann.
- Alle Mitarbeiter des Trust Centers sind verpflichtet die strengen internen Datenschutz- und Sicherheitsrichtlinien des Konzerns Deutsche Telekom AG einzuhalten.
- Die Systeme des Trust Centers werden regelmäßig auf sicherheitsrelevante Veränderungen untersucht. Alle sicherheitsrelevanten Veränderungen müssen vor Inbetriebnahme durch das Change Advisory Board des Trust Centers freigegeben werden.
- Alle sicherheitsrelevanten Prozesse sind im Sicherheitskonzept dokumentiert und geprüft.

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 Organisatorische Sicherheitsmaßnahmen

Die organisatorischen Maßnahmen sind im Sicherheitskonzept niedergelegt und werden durch das Betriebskonzept des Trust Centers umgesetzt. Die relevanten Anforderungen aus ETSI EN 319 401 Kap. 7.4 b, c, d, e sind umgesetzt.

5.3.1 Vertrauenswürdige Rollen

Vertrauenswürdige Personen sind alle Personen (T-Systems Mitarbeiter, Auftragnehmer, und Berater) mit Zugang zu oder Kontrolle über Authentifizierungs- oder Kryptografische Abläufe, die erhebliche Auswirkungen auf Folgendes haben können:

- die Validierung von Informationen in Zertifikatsaufträgen,
- die Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatsaufträgen, Sperraufträgen oder Erneuerungsaufträgen,
- die Vergabe oder den Widerruf von Zertifikaten, einschließlich Personal, das Zugang und Zugriff auf die Datenbanksysteme hat,
- den Umgang mit Informationen oder Aufträgen von Endteilnehmern.

Vertrauenswürdige Personen sind insbesondere:

- Mitarbeiter des Trust Centers (z.B. Systemadministration),
- Mitarbeiter kryptografischer Abteilungen,
- Sicherheitspersonal,
- zuständiges technisches Personal und
- für die Verwaltung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

Die oben genannten vertrauenswürdigen Personen müssen die in diesem CPS festgelegten Anforderungen (siehe Kapitel 5.4.1) erfüllen.

Das Change Advisory Board des T-Systems Trust Centers ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten, im CP/CPS der vom T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.3.2 Anzahl der für eine Aufgabe erforderlichen Personen

Die Aufrechterhaltung des Betriebs der Zertifizierungsstelle und des Verzeichnisdienstes (Administration, Sicherung, Wiederherstellung) wird von fachkundigen und vertrauenswürdigen Mitarbeitern wahrgenommen. Arbeiten an hochsensitiven Komponenten (z.B. Schlüsselerstellungssystem, HSM) sind durch besondere interne Kontrollverfahren geregelt und werden von mindestens zwei Mitarbeitern durchgeführt.

5.3.3 Identifizierung und Authentifizierung für jede Rolle

T-Systems Mitarbeiter, die als besonders vertrauenswürdige Personen eingestuft sind und besonders vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer T-Systems-internen Sicherheitsüberprüfung (siehe Kapitel 5.4.2).
T-Systems stellt sicher, dass Mitarbeiter einen vertrauenswürdigen Status erlangt haben und die Zustimmung der Abteilung erteilt wurde, bevor diese Mitarbeiter:

- Zugangsgeräte und Zugang zu den erforderlichen Einrichtungen erhalten,
- die Berechtigung zum Zugriff auf die Systeme der Zertifizierungsstelle und andere IT-Systeme erhalten,
- zur Durchführung bestimmter Aufgaben im Zusammenhang mit diesen Systemen zugelassen werden.

Die Mitarbeiter des Trust Centers werden nach positiver Prüfung formell vom Leiter des Trust Centers ernannt.

5.3.4 Rollen, die eine Aufgabentrennung erfordern

Die folgenden Rollen erfordern eine Aufgabentrennung und werden daher von verschiedenen Mitarbeitern begleitet:

- Auftragseingabe und Zertifikatsfreigabe
- Sicherung und Rücksicherung von Datenbanken und HSMs,
- Generierung von qualifizierten Zertifikaten,
- Key Lifecycle Management von CA- und Root-CA-Zertifikaten.

5.4 Personelle Sicherheitsmaßnahmen

T-Systems setzt umfassende personelle Sicherheitsmaßnahmen um, die einen hohen Schutz ihrer Einrichtungen und der Zertifizierungsdienste gewährleisten. Im Trust Center ist der Einsatz von qualifiziertem geschultem Personal obligatorisch, die personellen Maßnahmen sind im Sicherheitskonzept niedergelegt.
Die Anforderungen aus ETSI EN 319 401 Kap. 7.2 sind umgesetzt und werden sowohl in internen als auch in externen Audits geprüft.
Die vertrauenswürdigen Personen müssen die in dieser CP/CPS festgelegten Anforderungen (Kapitel 5.4.3) erfüllen.
Ebenfalls müssen diese vertrauenswürdigen Personen frei von Interessenskonflikten gestellt werden, damit die ausgeübten Rollen unbefangen und vorurteilsfrei ausgeübt werden können. Die Mitarbeiter verpflichten sich zur Anerkenntnis und Einhaltung des vom Konzern vorgegebenen „Code of Conduct“.
Das T-Systems Advisory Board ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten und CP/CPS der von T-Systems Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.4.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

T-Systems verlangt von seinen Mitarbeitern, die eine vertrauenswürdige Rolle einnehmen sollen, entsprechende Nachweise über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.
In regelmäßigen Abständen ist ein neues Führungszeugnis der T-Systems vorzulegen.

5.4.2 Sicherheitsüberprüfung

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt T-Systems eine Sicherheitsüberprüfung durch mit folgendem Inhalt durch:

- Überprüfung und Bestätigung der bisherigen Beschäftigungsverhältnisse,
- Überprüfung von Arbeitszeugnissen,
- Bestätigung des höchsten oder maßgebenden Schul-/Berufsabschlusses,
- polizeiliches Führungszeugnis.

Sofern die in diesem Abschnitt festgelegten Anforderungen nicht erfüllt werden können, macht T-Systems ersatzweise Gebrauch von einer gesetzlich zulässigen Ermittlungsmethode, die im Wesentlichen die gleichen Informationen liefert.
Ergebnisse einer Sicherheitsüberprüfung, die zu einer Ablehnung eines Anwärters für eine vertrauenswürdige Person führt, können beispielsweise sein

- falsche Angaben seitens des Anwärters oder der vertrauenswürdigen Person,
- besonders negative oder unzuverlässige berufliche Referenzen, und
- gewisse Vorstrafen.

Berichte, die solche Informationen enthalten, werden durch Mitarbeiter der Personalabteilung und Sicherheitspersonal bewertet, die das weitere angemessene Vorgehen festlegen. Das weitere Vorgehen kann Maßnahmen bis einschließlich zur Rücknahme des Einstellungsangebots an Anwärter für vertrauenswürdige Positionen führen oder der Kündigung von vertrauenswürdigen Personen beinhalten.
Die Verwendung von in einer Sicherheitsüberprüfung ermittelten Informationen zur Ergreifung solcher Maßnahmen unterliegt geltendem Recht.

5.4.3 Schulungs- und Fortbildungsanforderungen

Das Personal des T-Systems Trust Centers besucht Fortbildungsmaßnahmen die zur kompetenten und zufriedenstellenden Erfüllung ihrer beruflichen Pflichten erforderlich sind. T-Systems führt Unterlagen über diese Schulungsmaßnahmen.
Die Schulungsprogramme sind auf die individuellen Tätigkeitsbereiche abgestimmt und beinhalten u.a.:

- fortgeschrittene PKI-Kenntnisse,
- Verfahrensweisen nach ITIL,
- Datenschutz,
- Daten- und Fernmeldegeheimnis,
- Informationsschutz,
- Zutrittsschutz,
- Antikorruption,
- Sicherheits- und Betriebsrichtlinien und –verfahren von T-Systems,

- Verwendung und Betrieb eingesetzter Hardware und Software,
- Meldung von und Umgang mit Störungen und Kompromittierungen und
- Verfahren für die Schadensbehebung im Notfall (Disaster Recovery) und Geschäftskontinuität (Business Continuity).

Mitarbeiter, welche mit der Validierung von Zertifikatsaufträgen befasst sind, erhalten zusätzlich Schulungen in den folgenden Bereichen:

- Richtlinien, Verfahren und aktuelle Entwicklungen zu Validierungsmethoden,
- Inhalte und insbesondere relevante Änderungen des vorliegenden CPS,
- Relevante Anforderungen und Vorgaben aus den Zertifizierungsnormen,
- Allgemeine Bedrohungs- und Angriffsszenarien bzgl. der Validierungsmethoden (z.B. Social Engineering)

5.4.4 Nachschulungsintervalle und -anforderungen

Das Personal der T-Systems erhält im erforderlichen Umfang und den erforderlichen Abständen Auffrischungsschulungen und Fortbildungslehrgänge.

5.4.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

5.4.6 Sanktionen bei unbefugten Handlungen

T-Systems behält sich vor, unbefugte Handlungen oder andere Verstöße gegen dieses CPS und der daraus abgeleiteten Verfahren zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen können Maßnahmen bis einschließlich der Kündigung beinhalten und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.

5.4.7 Anforderungen an unabhängige Auftragnehmer

T-Systems behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter von T-Systems in vergleichbarer Position.
Obiger Personenkreis, der die in Kapitel 5.4.2 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von T-Systems nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.4.8 Dokumentation für das Personal

Um die beruflichen Pflichten angemessen erfüllen zu können, stellt T-Systems seinen Mitarbeitern alle dafür erforderliche Dokumente (Schulungsunterlagen, Verfahrensanweisungen) und Hilfsmittel zur Verfügung.

5.5 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.

5.6 Sicherung der Aufzeichnungen

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

5.7 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.
Betroffene Nutzer werden über diese Maßnahme informiert.

5.8 Standards und Kontrollen für kryptographische Module

Die privaten Schlüssel der CAs werden auf einem FIPS 140-2/ Level 3 evaluiertem Hardware Security Modul (HSM) abgelegt. Die Sicherung der Schlüssel wird unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken durchgeführt.

Zum Schutz der kryptographischen Geräte während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet, die während der FIPS- und CC-Zertifizierungen geprüft wurden. Die Geräte werden hierbei getrennt von den zum Betrieb und zur Nutzung benötigten Token aufbewahrt, so dass die Kompromittierung einer einzelnen Lokation nicht ausreicht, um die Geräte missbräuchlich zu verwenden

5.9 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme auf eine Kompromittierung privater Schlüssel von CA- oder Root-CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.

Die betroffenen Beteiligten werden über die mögliche Kompromittierung schriftlich informiert. Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechenden Informationen an die Aufsichtsbehörde weiterzuleiten. Die Generierung neuer Schlüssel und Zertifikate ist gemäß den Arbeitsanweisungen zu dokumentieren und gemäß den Auflagen des jeweiligen Sicherheitskonzepts zu überwachen.

Von diesen Zertifikaten ausgestellte Benutzerzertifikate werden ebenfalls gesperrt. Die betroffenen Zertifikatsinhaber werden über die Sperrung informiert.

5.10 Umgang mit Störungen und Kompromittierungen

T-Systems hat ein IT-Servicemanagement gemäß ITIL sowie ISMS Prozesse etabliert, über die Störungen und Sicherheitsvorfälle nach definierten Standard-Prozessen bearbeitet werden.

Durch die Festlegung aller erforderlichen Ansprechpartner und entsprechend eingerichteter Gruppen in den IT-Servicemanagement-System sowie der Etablierung einer Rufbereitschaft und des MoD (Manager on Duty) ist sichergestellt, dass die Bearbeitung von Störungen und Sicherheitsvorfälle kurzfristig beginnt, damit der Schaden möglichst gering bleibt und schnell beseitigt werden kann.

Störungen werden vom Endteilnehmer über die in der PKS-Info definierten Kontakte des Service Desk eingereicht und im Rahmen des Service Managements bearbeitet.

Das Personal des Service Desk bewertet zunächst die Störung, bevor die Störung in die Störungsbearbeitungsanwendung der T-Systems eingegeben, priorisiert und an den/die Fachbereich(e) zwecks Störungsbeseitigung weitergeleitet wird. In der EDV-Anwendung werden transparent alle Informationen revisionssicher gespeichert, um jederzeit den Bearbeitungsstand der Störung bis zur Beseitigung nachvollziehen zu können.

Das Service Desk wird, entsprechend der Störungsklasse, von dem Fachbereich über den Bearbeitungszustand in Kenntnis gesetzt, um der beauftragten Drittpartei (Delegated Third Party) entsprechende Informationen bereitstellen zu können.

Betroffene Kunden werden, sofern erforderlich, schnellstmöglich informiert und in den Prozess eingebunden.

Hat eine Störung eine sicherheitskritische Auswirkung so wird über die im Vertrauensdienstegesetz festgelegten Verfahren die zuständige Aufsichtsbehörde innerhalb von 24 Stunden informiert.

5.10.1 Geschäftskontinuität nach einem Notfall

T-Systems hat für den Rechenzentrumsbetrieb einen Notfallplan entwickelt, implementiert und getestet, um die Auswirkungen von Katastrophen jeder Art (Naturkatastrophen oder Katastrophen menschlichen Ursprungs) zu mildern und die Verfügbarkeit kritischer Geschäftsprozesse schnellstmöglich wieder herzustellen. Dies umfasst auch alle Prozesse, Komponenten, Systeme und Dienste des Trust Centers. Dieser Plan wird mindestens jährlich überprüft, getestet und entsprechend aktualisiert, um im Falle einer Katastrophe gezielt und strukturiert reagieren zu können.

Der Notfallplan enthält mindestens die folgenden Informationen:

- Die notwendigen Kriterien für die Aktivierung des Planes,
- Mögliche Notfallmaßnahmen (je nach Situation),

- Ausweichverfahren,
- Wiederanlauf-Verfahren,
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung,
- Sensibilisierungsmaßnahmen,
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals,
- Die Verantwortung der Individuen (Rollenbeschreibung und -zuweisung),
- Wiederanlaufzeit (RTO),
- Regelmäßige Durchführung der Notfallpläne zu Testzwecken,
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der Geschäftstätigkeit nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse,
- Eine Verpflichtung kritische kryptographische Geräte und Informationen an einem anderen Standort zu sichern bzw. vorzuhalten,
- Festlegung der maximal tolerierbaren Ausfallzeit (MTO) und entsprechende Zeiten zur Wiederherstellung,
- Häufigkeit, in der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden,
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur Hauptgeschäftsstelle bzw. zum Rechenzentrum des Trust Centers,
- Verfahren zur bestmöglichen Sicherung der Betriebsstätten und –Einrichtungen nach einer Katastrophe (Notbetrieb) bis zur Wiederherstellung eines den Anforderungen entsprechend gesicherten Normalbetriebs.

Im Rahmen eines Compliance-Audits ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

Schlüsselmaterial des Endteilnehmers, das auf Smartcards ausgestellt wurde, ist nicht im Rahmen dieses Notfallplans abgedeckt. Siehe dazu Kapitel 5.8.

5.11 Einstellung des Betriebes

5.11.1 Zertifizierungsdiensteanbieter gemäß eIDAS

Im Falle der Einstellung des Zertifizierungsdienstes geht die Zertifizierungsstelle entsprechend den Vorgaben aus ETSI EN 319 401 Kap. 7.12 vor und hat dafür einen Beendigungsplan erstellt.
Dieser Beendigungsplan enthält unter anderem die folgenden Punkte:

- Benachrichtigung der Endteilnehmer und Vertrauende Dritte über die geplante Einstellung des Dienstes, diese Information enthält auch die Beschreibung über den zukünftigen Zugang zu den archivierten Daten,
- Fortführung der Sperrfunktionalitäten einschließlich der regelmäßigen Erstellung von Sperrlisten, Abruf der Zertifikatsstatusinformationen und Service Desk-Funktionen,

- 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 Zertifizierungsstelle (CA)

Vor der Einstellung des Dienstes werden alle möglichen Maßnahmen getroffen, um den potentiellen Schaden für alle Beteiligten möglichst gering zu halten, alle Beteiligten werden so früh wie möglich informiert.

Alle Rechte der Mitarbeiter der Zertifizierungsstelle und der Registrierungsstellen werden entzogen, die privaten Schlüssel der CA werden vernichtet. Alle noch gültigen Zertifikate werden gesperrt.
Alle elektronisch erfassten Daten mit Ausnahme der Zertifikate und Sperrlisten werden gelöscht. Die Zertifikate und Sperrlisten sowie Papierdokumente werden archiviert, um ggf. zur Beweissicherung in Gerichtsprozessen darauf zugreifen zu können.
Die Archivierung erfolgt dabei weiterhin nach Vorgaben dieses Dokumentes und der gültigen Gesetze.

5.11.2 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 werden von geschultem und vertrauenswürdigem Fachpersonal (Trusted Roles) in einem abstrahlarmen Raum auf einem sicherheitsüberprüften Hardware Security Module (FIPS 140-2/ Level 3 evaluiert) in der sogenannten “Key Ceremony” (Schlüsselgenerierungsverfahren) erzeugt und abgelegt.

Bei CA- und Root-CA-Zertifikaten werden die privaten Schlüssel auf einem evaluierten HSM (FIPS 140-1/ Level 3 evaluiert) erzeugt und abgelegt.

Alle Aktivitäten während der “Key Ceremony“ werden protokolliert und von allen beteiligten Personen unterzeichnet. Diese Aufzeichnungen werden zu Audit- und Nachverfolgungszwecken für einen von T-Systems als angemessen erachteten Zeitraum aufbewahrt.

Die Systeme der Offline-CA, bestehend aus Zertifizierungsinstanz, kryptografischen Hardware-Moduls (HSM) (inkl. Back-Up-Token) und Browser, werden „offline“, d.h. ohne Anbindung an irgendeine eine Netzstruktur, betrieben. Die Systeme der Offline-CA sind in einem verschließbaren Computer-Rack untergebracht und gehen Öffnung und Austausch versiegelt. Die Unversehrtheit der Versiegelung wird bei jeder Nutzung der Offline-CA geprüft und dokumentiert.

6.1.1 Generierung und Installation der Schlüsselpaare für die CA-Zertifikate

Als Schlüsselträger für CA-Zertifikate kommt sicherheitsüberprüfte Hardware zum Einsatz Diese verfügt zum Beispiel über Zertifizierungen gemäß eIDAS QSCD oder FIPS-140-2 oder vergleichbare Zertifizierungen.

6.2 Generierung und Erneuerung von CA- und Root-Zertifikaten

Die Generierung von CA-Zertifikaten erfolgt an einem System ohne Netzwerkanbindung (Offline) im Vier-Augen-Prinzip.
Schlüsselbackups werden, sofern die eingesetzte Hardware auf der sich der CA-Schlüssel befinden dies unterstützt, ausschließlich im Vier-Augen-Prinzip durchgeführt. Der Zugriff auf diese Backups (inkl. Rücksicherung) ist nur im Vier-Augen-Prinzip möglich.
Die Auswahl der Algorithmen für CA- und Root-Zertifikate erfolgt in Zusammenarbeit mit der Bundesnetzagentur und der Konformitätsbewertungsstelle für eIDAS.
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.

Die Zertifikatsgültigkeit beginnt mit der Generierung des Zertifikats und endet mit Ablauf des Gültigkeitszeitraums oder durch Sperrung. Die Gültigkeitsdauer von Schlüsselpaaren entspricht der Gültigkeitsdauer des zugehörigen Zertifikats.

Weitere Details zu diesem Vorgang können der Prozessdokumentation der Offline-CA entnommen werden.

6.3 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 erstellten Audit-Protokolle/History-Daten/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft T-Systems ihre Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen.

Eingeleitete Maßnahmen, die als Reaktion aus der Auswertung von Audit-Protokollen/Logging-Dateien stammen, werden ebenfalls protokolliert.

Auf den Systemen des Trust Centers werden Betriebssysteme eingesetzt, die die Durchsetzung von Sicherheitseinstellungen unterstützen. Keines der Systeme kann ohne Benutzeranmeldung verwendet werden.

Die Durchsetzung der Zugangsbeschränkungen an den Systemen wird durch die umgesetzte restriktive Password Policy unterstützt.

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

Die Nutzung der Anwendung zur Ausstellung von Zertifikaten ist durch Multi-Faktor-Authentisierung abgesichert.

Der TSP lässt einen Penetrationstest (PEN-Test) an den TSP-Systemen durchführen

- bei der Einrichtung,
- umfangreichen Upgrades oder Änderungen der Infrastruktur oder der Anwendungen,
- mindestens aber ein Mal pro Jahr,

die der TSP als wesentlich erachtet.

Der TSP erbringt den Nachweis, dass jeder Penetrationstest von einer Person oder Organisation durchgeführt wurde, die über die erforderlichen Fähigkeiten, Werkzeuge, Kenntnisse, ethischen Grundsätze und Unabhängigkeit verfügt, um einen zuverlässigen Bericht erstellen zu können.

Die Einstellungen der Systeme werden regelmäßig von einer Konformitätsbewertungsstelle gemäß eIDAS überprüft.

6.3.1 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.

T-Systems hat Mechanismen zum Schutz der zentralen Datenablage (Repository) gegen nicht autorisierten Versuche implementiert, um Manipulationen an diesem System (hinzufügen, löschen, ändern) zu verhindern.

6.3.2 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. Die Durchsetzung der Zugangsbeschränkungen an den Systemen wird durch die umgesetzte restriktive Passwort Policy unterstützt.

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

T-Systems hat insbesondere Mechanismen zum Schutz des Sperrstatus-Dienstes (CRL, ARL, OCSP) gegen unbefugte Versuche implementiert, um Manipulationen an Sperrstatusinformationen (hinzufügen, löschen, ändern) zu verhindern.

6.3.3 Verwendung sicherheitsüberprüfter Komponenten

Die eIDAS-Verordnung fordert für verschiedene Zwecke den Einsatz sicherheitsüberprüfter Medien für die Speicherung der Zertifikate und Schlüsselmaterialien. Die nachfolgende Aufstellung zeigt einen Teil der verwendeten Komponenten:

- Die eingesetzten Chipkarten zur Generierung und Speicherung privater Schlüssel sind nach Common Criteria EAL4+ evaluiert und verfügen über die Zulassung als qualifizierte Signaturerstellungseinheit gemäß der eIDAS Verordnung.

6.4 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 Bandbrei-

te. 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 Konformitätsbewertungsstelle gemäß eIDAS überprüft.

Alle berechtigten Nutzer müssen sich gegenüber den Systemen mit festgelegten Mechanismen authentifizieren, nicht mehr benötigte Accounts werden gelöscht oder deaktiviert.

Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.8 umgesetzt.

6.5 Systementwicklungskontrollen

T-Systems hat Mechanismen und Kontrollen implementiert, um eingekaufte, entwickelte oder veränderte Software auf Schadelemente oder bösartigen Code (z.B. Trojaner, Viren) überwachen und schützen zu können. Die Integrität wird vor der Installation manuell verifiziert.
Neue Software-Versionen der Software (geplante Updates) oder Fehlerbeseitigungen (kurzfristige Bugfixes) werden zunächst auf einem Entwicklungssystem des Herstellers/Entwicklers bereitgestellt und getestet.
Nach Prüfung erfolgt die Installation auf dem Testsystem der T-Systems. Erst nach erfolgreichen Tests erfolgt die Installation auf dem Wirksystem der T-Systems.
Das bei der T-Systems etablierte Change- und Release-Management findet Anwendung.

6.6 Sicherheitskontrollen des Lebenszyklus

T-Systems hat Mechanismen und Kontrollen implementiert, dass Sicherheitspatchs innerhalb einer angemessenen Zeit, nachdem sie verfügbar sind, installiert werden. Die Integrität des Sicherheitspatchs wird vor der Installation manuell verifiziert.

Ein Sicherheitspatch wird nicht installiert, wenn zusätzliche Sicherheitslücken oder Instabilitäten entstehen, die die Vorteile der Anwendung des Sicherheitspatchs überwiegen. Der Grund für die Nichtanwendung von Sicherheitspatchs wird dokumentiert

6.7 Schwachstellenbewertung

Nach jeder signifikanten System- oder Netzwerkänderung erfolgt innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan). Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen

festgelegt und in einem definierten Plan umgesetzt. Die Schwachstellenüberprüfungen, ihre Ergebnisse und Aktionen (Behebungen, Austausch) werden dokumentiert.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen, die dem TSP mitgeteilt wurden, werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Im Falle, dass eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

Zusätzlich werden einmal jährlich sogenannte Penetrationstests durchgeführt. Auch hier werden entsprechend Maßnahmen abgeleitet und umgesetzt, sofern dies notwendig ist.

7 Zertifikatsprofile und Sperrlistenprofile

7.1 Zertifikatsprofil

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

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

7.2 Sperrlistenprofil

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

8 Audits und andere Bewertungskriterien

Zur Prüfung der Konformität werden die TSP sowohl durch interne Auditoren als auch durch eine anerkannte Konformitätsbewertungsstelle (gemäß ETSI EN 319 403) auditiert. Im Rahmen der Audits wird neben der Dokumentation (Sicherheitskonzept, Betriebskonzept sowie weitere interne Dokumente) die Umsetzung der Prozesse und Einhaltung der Vorgaben überprüft.

TeleSec Public Key Service (qualifizierter Bereich):
Die T-Systems Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319411-1, policy QCP) unterzogen. T-Systems führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen durch.

TeleSec Public Key Service (nicht qualifizierter Bereich):
Die T-Systems Prozesse werden regelmäßig durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319411-1 policy NCP+) unterzogen. T-Systems führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen durch.

8.1 Intervall und Grund von Prüfungen

Compliance-Audits finden in der Regel jährlich oder bei Bedarf statt. Darüber hinaus werden jährlich Notfallübungen im Trust Center durchgeführt.

8.2 Identität/Qualifikation des Prüfers

Die Trust Center-spezifischen Compliance-Audits werden von qualifizierten Mitarbeitern der T-Systems oder einem Dritten (z.B. qualifiziertes Unternehmen wie TÜV IT) durchgeführt, die Erfahrung in den Bereichen Public-Key-Infrastructure-Technologie, Sicherheits-Auditing und Verfahren und Hilfsmittel der Informationssicherheit vorweisen können.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die eIDAS-Zertifizierungen handelt es sich um einen unabhängigen und qualifizierten Auditor (z.B. Wirtschaftsprüfer, Gutachter).

Selbstaufsichtsmaßnahmen (Quality Assesments) werden von dafür qualifizierten T-Systems Mitarbeitern durchgeführt.

8.4 Abgedeckte Bereiche der Prüfung

Zielsetzung der Überprüfung ist die Umsetzung dieses Dokuments. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Identitätsprüfungen der Endteilnehmer,
- Zertifikatsbeauftragungsverfahren,
- Bearbeitung von Zertifikatsaufträgen,
- Zertifikatserneuerung,
- Zertifikatssperrungen,
- Zutrittsschutz,
- Berechtigungs- und Rollenkonzept ,
- Einbruchshemmende Maßnahmen,
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen der Audit-Kriterien der in der oben aufgeführten ETSI-Normen geprüft.

Das T-Systems Trust Center führt jährlich eine Risikobewertung durch.

Die Überprüfung beinhaltet zumindest die folgenden Punkte:

- Identifikation vorhersehbarer externer, als auch interner Gefährdungen (d.h. insbesondere die zu Grunde liegenden Schwachstellen), welche
    - zu unbefugten Zugriffen auf relevante Daten oder Systeme,
    - zur Weitergabe oder einem Missbrauch von relevanten Daten,
    - zu Veränderungen oder Zerstörung von relevanten Daten,
    - zur Beeinträchtigung, Störung oder Ausfall von Teilen oder des gesamten Zertifikatsverwaltungsprozesses

  führen können.
- Beurteilung der Eintrittswahrscheinlichkeit und der daraus resultierenden potenziellen Schäden (d.h. Schadenshöhe) durch das Ausnutzten einer Schwachstelle. Dabei ist der besondere Schutzbedarf der Zertifikatsdaten und des Zertifikatsverwaltungsprozesses zu berücksichtigen.
- Beurteilung der Wirksamkeit und Angemessenheit der getroffenen Gegenmaßnahmen (z.B. Richtlinien, Verfahren, eingesetzte Sicherheits-Systeme, Technologien, Versicherungen) welche die Gefährdung beseitigen oder das Risiko minimieren.

Basierend auf der Risikobewertung hat das T-Systems Trust Center einen Sicherheitsplan entwickelt, der regelmäßig überprüft und bei Bedarf angepasst wird. Der Sicherheitsplan besteht aus Verfahren, Maßnahmen und Produkten um die Bewertung und Management der während der Risikobewertung identifizierten Risiken

zu unterstützen. Der Sicherheitsplan enthält entsprechend der Sensibilität der Daten und des Zertifikatsverwaltungsprozesses administrative, organisatorische, technische und physische Sicherheitsmaßnahmen.

8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Werden bei einem Compliance-Audit oder von einem Prüfer Mängel oder Fehler bei dem Betreiber der Zertifizierungsstelle festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durch zu führen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheidet der Leiter Trust Center über den Zeitrahmen der Behebung.

8.6 Mitteilung der Ergebnisse

Die Ergebnisse der Prüfung werden in einem vom Prüfer erstellten Bericht dokumentiert und T-Systems übergeben.

T-Systems behält sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der T-Systems.

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/signaturkarte/ → 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/signaturkarte/ → Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.2.1 Versicherungsschutz

T-Systems verfügt über einen Betriebs- und Vermögenshaftpflichtversicherungsschutz. Es ist sichergestellt, dass die Anforderungen, die sich hinsichtlich des Versicherungsschutzes ergeben, erfüllt werden.

9.2.2 Sonstige finanzielle Mittel

Nicht anwendbar.

9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit betrieblicher Informationen

9.3.1 Umfang von vertraulichen Informationen

Als vertraulich gelten alle Informationen von PKI-Beteiligten, die nicht veröffentlicht oder zur Veröffentlichung explizit freigegeben werden und die nicht unter Kap. 9.3.2 fallen.

9.3.2 Umfang von nicht vertraulichen Informationen

Unter nicht vertraulichen Informationen werden alle impliziten und expliziten Informationen eingestuft, die in ausgegebenen Zertifikaten, Sperrlisten, Statusinformationen enthalten sind oder davon abgeleitet werden können.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortlichkeit für den Schutz der vertraulichen Informationen sowie über die Einhaltung der datenschutzrechtlichen Bestimmungen liegt bei T-Systems als Zertifzierungsstelle.
Darüber hinaus sind auch die Kammermitarbeiter durch die Übernahme von Tätigkeiten im Rahmen der Freigabe und Attributbestätigung verpflichtet, vertrauliche Informationen entsprechend zu behandeln.

9.4 Datenschutz

9.4.1 Datenschutzkonzept

Zur Leistungserbringung muss T-Systems personenbezogene Daten elektronisch speichern und verarbeiten. T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 BDSG sicher.
Entsprechend den Konzernvorgaben wurde ein Datenschutzkonzept erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte um den PKI-Dienst zusammen.
Das Datenschutzkonzept kann in Auszügen auf Anforderung bereitgestellt werden.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kap. 9.3.1.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kap. 9.3.2.

9.4.4 Verantwortung für den Schutz vertraulicher Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kap. 9.3.3.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Antragsteller stimmt der Nutzung von personenbezogenen Daten durch die Zertifiztierungsstelle oder der zuständigen Kammer zu, soweit dies zur Leistungserbringung erforderlich ist.
Ferner dürfen alle Informationen veröffentlicht werden, die nach Kap. 9.4.3 als nicht vertraulich behandelt werden.

9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die Verpflichtung zur Geheimhaltung der vertraulichen Informationen oder personenbezogener Daten entfällt, soweit die Offenlegung kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens bestehen, die zur Offenlegung vertraulicher oder privater Informationen führen könnten, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei hierüber unter Beachtung der gesetzlichen Bestimmungen informieren.

9.4.7 Andere Umstände zur Offenlegung von Daten

Keine Bestimmungen.

9.5 Urheberrecht

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von T-Systems unzulässig.

9.6 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.

9.7 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/signaturkarte/→ Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.8 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/signaturkarte/→ Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.9 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/signaturkarte/ → Support → Downloadbereich → Allgemeine Geschäftsbedingungen und Preise

9.10 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.

9.11 Bestimmendes Recht

Die eIDAS-Verordnung regelt generell die Ausstellung von qualifizierten Zertifikaten. Ferner gilt das Recht der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist Frankfurt /Main.

9.12 Andere Regelungen

9.12.1 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.

9.12.2 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.

9.12.3 Beschwerden und Eskalationen

9.12.3.1 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.

9.12.3.2 Eskalation

Falls die Streitigkeit nicht innerhalb von zehn (10) Tagen nach der anfänglichen Mitteilung gemäß CPS § 9.12.3.1 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.