Deutsche Telekom Qualified.ID - Certificate Practice Statement

Zertifizierungsrichtlinie für Deutsche Telekom Qualified.ID

Deutsche Telekom Security GmbH

Telekom Security

Öffentlich

Version: 10.00

Gültig ab: 25.05.2023

Status: Freigegeben

Letztes Review: 16.05.2023

IMPRESSUM

Tabelle 1 – Impressum

Angaben	Ausprägung
Herausgeber	Deutsche Telekom Security GmbH Bonner Talweg 100 53113 Bonn Deutschland
Dateiname	telekom security-pks-cps_v10.00.docx
Gültig ab	25.05.2023
Titel	Deutsche Telekom Qualified.ID - Certificate Practice Statement
Version	10.00
Letztes Review	16.05.2023
Status	Freigegeben
Autor	Telekom Security
Inhaltlich geprüft von	Telekom Security
Freigegeben von	Telekom Security
Beteiligte Organisationseinheit	Telekom Security
Ansprechpartner	Telekom Security
Kurzbeschreibung	Zertifizierungsrichtlinie

ÄNDERUNGSHISTORIE

Tabelle 2 – Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
1.0	14.01.2005	T-Systems	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
4.0	01.01.2020	JS	Überarbeitung für Fernsignatur
5.0	01.03.2020	T-Systems	Strukturierung nach RFC 3647
06.00	28.05.2020	T-Systems	Überarbeitung im Rahmen des Audits
07.00	01.07.2020	Telekom Security	Überarbeitung im Rahmen der Umfirmierung zur Deutsche Telekom Security GmbH
08.00	30.04.2021	Telekom Security	Überarbeitung im Rahmen des Audits.
09.00	11.05.2022	Telekom Security	Review, und Überarbeitung des Produktnamens
10.00	25.05.2023	Telekom Security	Review, und Überarbeitung für qualifizierte Siegel entfernen von Fernsignatur

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 EINLEITUNG

Bei dem vorliegenden Dokument handelt es sich um die **Zertifizierungsrichtlinie** (engl. Certification Practice Statement, kurz **CPS**) für die Dienstleistung **Deutsche Telekom Qualified.ID (kurz Qualified.ID)**. Im Folgenden wird es als die **Qualified.ID CPS** bezeichnet. Die Qualified.ID CPS findet ausschließlich Anwendung auf die Ausstellung qualifizierter Zertifikate sowie fortgeschrittener Zertifikate im Rahmen der Qualified.ID Dienstleistung. Für den Bereich der qualifizierten Zertifikate findet diese **Qualified.ID CPS** Anwendung für die Zertifikate auf einer Chipkarte, dabei kann es sich um Signaturzertifikate oder um Siegelzertifikate handeln. Sollte eine Differenzierung an einigen Stellen notwendig sein, so wird diese im Text entsprechend hervorgehoben.

Hinweis:

Unter fortgeschrittenen Zertifikaten sind im Kontext der Dienstleistung QUALIFIED.ID 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 Deutsche Telekom Security GmbH (Telekom Security) 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 (heute Qualified.ID) 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.

Die Qualified.ID 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 Qualified.ID der Deutschen Telekom GmbH. Die aktuelle Version der Qualified.ID CPS stellt den tatsächlichen Stand der Zertifizierungstätigkeit dar und gilt ausschließlich für die Dienstleistung Qualified.ID.

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 behandelt die Qualified.ID CPS die folgenden Aspekte:

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

1.1.1 PKI-Service Magenta Security Qualified.ID

Mit dem Dienst Qualified.ID werden dem Kunden ein Zertifikat und ein Schlüsselpaar zur elektronischen Signatur zur Verfügung gestellt. Dieses qualifizierte Zertifikat unterliegt den Regelungen der eIDAS-Verordnung der Europäischen Union und dem deutschen Vertrauensdienstegesetz. Mit einem qualifizierten PKS-Zertifikat kann ein Teilnehmer nachweisen, dass ein elektronisches Dokument mit seinem (privaten) Signaturschlüssel, der auf einer qualifizierten Signaturerstellungseinheit (QSCD) 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 Name und Kennung des Dokuments

Tabelle 3 - Dokumenteninformation

Name:	Zertifizierungsrichtlinie für Qualified.ID (Qualified.ID CPS)
Version:	10.00
Datum	11.05.2022
Objektbezeichnung (Object Identifier)	1.3.6.1.4.1.7879.13.27

1.3 PKI-Beteiligte

Die Gesamtverantwortung, für die in dieser CPS dargestellten Dienste liegt, immer beim Vertrauensdiensteanbieter Deutsche Telekom AG, auch wenn Teile der Tätigkeit nach Vorgaben dieser CPS von Dritten durchgeführt werden.

1.3.1 Zertifizierungsstellen

1.3.1.1 Qualifizierte Zertifikate

Der Qualified.ID für qualifizierte Zertifikate ist in eine zweistufige Zertifizierungshierarchie eingegliedert:

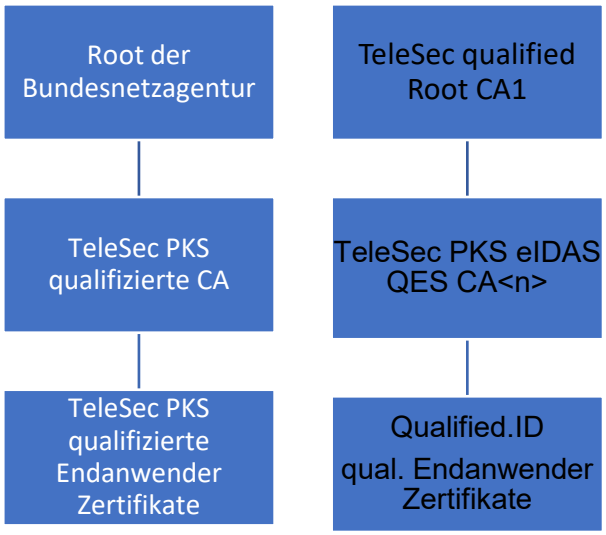

Abbildung 1 - Zertifizierungshierarchie qualifizierte Zertifikate

Die Grafik oben veranschaulicht die Zertifizierungshierarchie anhand von beispielhaft ausgewählten Zertifikaten. Der linke Teil zeigt die verwendete Zertifikatshierarchie für qualifizierte Zertifikate, die unter den Vorgaben des Signaturgesetzes (vor dem 01.08.2017) ausgestellt wurden. Der rechte Teil gilt für die Zertifikate nach dem VDG und der eIDAS-Verordnung (nach dem 01.08.2017).

Momentan sind folgende CA-Zertifikate in Benutzung: TeleSec PKS eIDAS QES CA 1 und TeleSec PKS eIDAS QES CA 5 für die Signatur von Endanwenderzertifikaten auf Signaturkarten.

Für die Signatur von qualifizierten Siegelzertifikaten für Endanwender wird das CA-Zertifikat [CA]_Telekom_Security_QualifiedID_eIDAS_QSeal_CA_1 und das Zertifikat [CA]_Telekom_Security_QualifiedID_eIDAS_QSeal_CA_2 verwendet.

Diese CA-Zertifikate werden nur für die Signatur von OCSP-Signern und Enduserzertifikaten verwendet

Die Wurzel-Zertifikate sowie die CA- und Dienste-Zertifikate für die Verwendung nach dem 01.08.2017 werden durch die Deutsche Telekom AG erstellt. Um den Status eines qualifizierten Vertrauensdienstes zu erlagen, werden die Zertifikate nach einer eIDAS-Konformitätsbetätigung in die Trusted List der Europäischen Union aufgenommen und veröffentlicht. Der Betrieb dieser Wurzel-Zertifikate wurde nahtlos von der Telekom Security fortgeführt.

Gemäß der eIDAS Verordnung stellt die PKS eIDAS 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 durch evaluierte Schlüsselgeneratoren auf dem jeweiligen Gerät 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.

Endanwenderzertifikate werden für den Nutzer und vertrauende Dritte über LDAP zum Abruf bereitgestellt, sofern der Nutzer der Veröffentlichung nicht widersprochen hat.

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 den Vereinbarungen mit dem Ansprechpartner der Benutzergruppe.

Die nicht qualifizierten Zertifikate im Produkt Qualified.ID folgen einer zweistufigen Zertifizierungshierarchie:

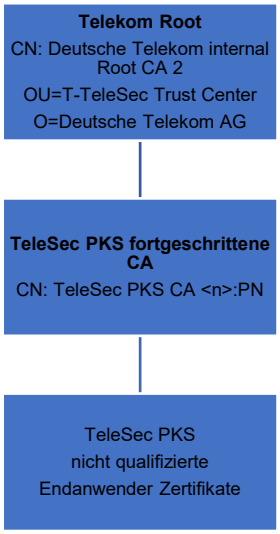

Abbildung 2 - Zertifizierungshierarchie nichtqualifizierte Zertifikate

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

Die TeleSec PKS CA zertifiziert ausschließlich Zertifikate für Endanwender der Qualified.ID.

Registrierungsstellen

Qualified.ID angegliederte Stellen betreiben etliche Registrierungsstellen, die die 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 Post-Ident 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 Telekom Security 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.

1.3.2 Zertifikatsinhaber

Zertifikatsinhaber für ein qualifiziertes Signaturzertifikat sind natürliche Personen, die ein Qualified.ID Zertifikat beauftragen bzw. erhalten, nachdem eine erfolgreiche Identifizierung und Authentifizierung durchgeführt wurde.

Zertifikatsinhaber für ein qualifiziertes Siegelzertifikat ist die juristische Person, auf die dieses Siegelzertifikat ausgestellt wurde. Zur Identifikation der juristischen Person wird eine natürliche Person identifiziert, die eine gültige Vertretungsmacht für die juristische Person nachweisen muss.

1.3.3 Vertrauende Dritte

Vertrauende Dritte sind natürliche Personen oder juristische Personen, 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.

1.3.4 Weitere Beteiligte

1.3.4.1 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.

1.3.5 Endteilnehmer (End Entity)

Im Kontext der Qualified.ID werden unter Endteilnehmer alle Zertifikatsnutzer verstanden, auf die ein Zertifikat ausgestellt werden kann und selbst keine Rolle einer Zertifizierungsstelle repräsentieren.

1.4 Zertifikatsverwendung

1.4.1 Allgemeine Grundlagen

Die Zertifikate dürfen nur im zulässigen und geltenden gesetzlichen Rahmen verwendet werden. Dies gilt insbesondere unter Beachtung der länderspezifischen geltenden Ausfuhr- und Einfuhrbestimmungen. Bei Verlust der Chipkarte oder Missbrauch 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 CA-Zertifikate

Die CA-Zertifikate werden über die Homepage des Trust Centers in einem ZIP-File veröffentlicht.

1.4.3 Qualifizierte Zertifikate

Die qualifizierten Signaturzertifikate werden für qualifizierte Signaturen im Sinne der eIDAS Verordnung eingesetzt.

Qualifizierte Benutzerzertifikate für die diese CPS gilt entsprechen der Policy QCP-n-qcsd.

Die qualifizierten Siegelzertifikate werden für qualifizierte Siegel im Sinne der eIDAS Verordnung eingesetzt.

Qualifizierte Siegelzertifikate für die diese CPS gilt entsprechen der Policy QCP-l-qcsd.

1.4.4 Fortgeschrittene Zertifikate

Qualified.ID fortgeschrittene Zertifikate werden zur Authentisierung, zur Verschlüsselung und für fortgeschrittene Signaturen eingesetzt. Die Prozesse und das Sicherheitsniveau zur Beauftragung, Produktion und Auslieferung von

fortgeschrittenen QUALIFIED.ID-Zertifikaten sind exakt identisch zu denen, der qualifizierten Zertifikate. Lediglich die Root-Hierarchie ist unterschiedlich.

1.4.5 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.

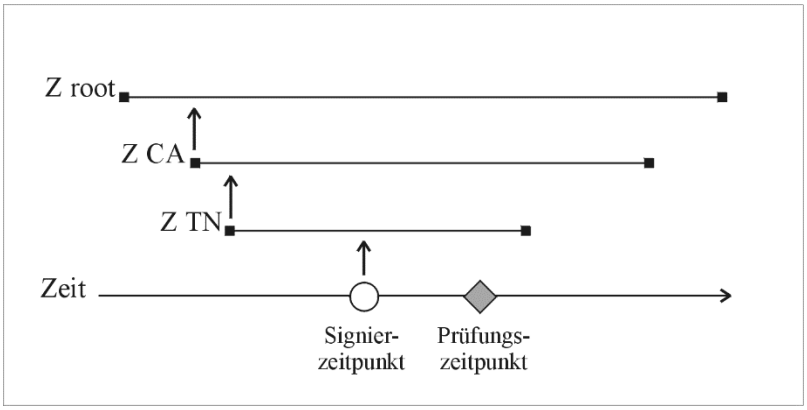

Abbildung 3 - Kettenmodell

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.

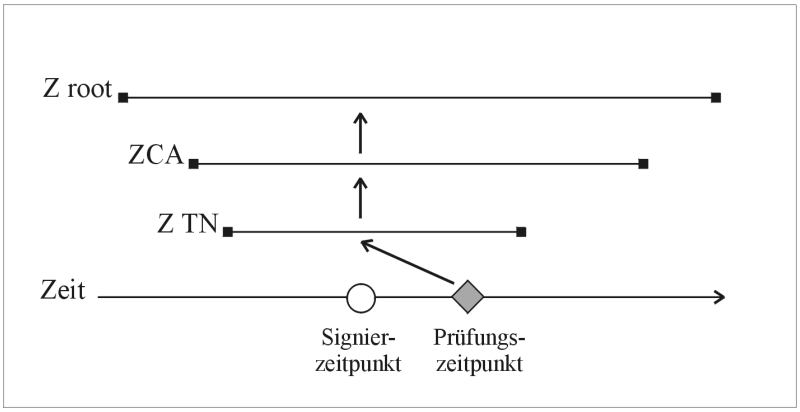

Abbildung 4 - Schalenmodel

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

1.5 Verwaltung der Richtlinien

1.5.1 Zuständigkeit für das Dokument

Diese CP/CPS wird herausgegeben von:

Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn
Deutschland

Der Vertrauensdienst wird nach außen durch den Leiter VDA und seinem Stellvertreter vertreten.

1.5.2 Kontaktinformationen

Adresse:
Deutsche Telekom Security GmbH

Untere Industriestraße 20, 57250 Netphen
Postfach 1465, 57238 Netphen

Telefon: +49 (0) 1805 268 204 [1]

Sperrhotline:

National	116 116
International	+49 30 4050 4050

E-Mail: telesec_support@t-systems.com

WWW: https://www.telesec.de

Über die oben genannte URL können im Bereich Public Key Service/Download alle relevanten Dokumente zum Dienst Qualified.ID gefunden werden.

1.5.3 Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP/CPS 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] 14 Ct/Minute aus dem deutschen Festnetz, max. 42 Ct/Minute aus dem Mobilfunk

1.5.4 Genehmigungsverfahren dieses Dokuments

Dieses Dokument wird durch den im Betriebsleitfaden des Trust Centers definierten Qualitätssicherungs- und Freigabeprozesses behandelt. Dieser sieht 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.

1.6 Akronyme und Definitionen

BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamte für Sicherheit in der Informationstechnik
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.
HSM	Hardware Security Modul
LDAP	Lightweight Access Protocol
LRA	Lokale RA
OCSP	Online Certificate Status Protocol
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
TSP	Trusted Service Provider
VDG	Vertrauensdienstegesetz
Zertifikatsinhaber	bezeichnet eine Person, die Gegenstand eines Zertifikats ist und der ein Zertifikat erteilt worden ist.

2 VERANTWORTLICHKEITEN VON VERÖFFENTLICHUNGEN UND ABLAGEN

2.1 Ablagen

Der Abruf der Zertifikate und Sperrlisten erfolgt über LDAPv3, der Zugriff auf die OCSP-Responder erfolgt per http. Der Zugriff auf den OCSP Responder durch die Endteilnehmer, Vertrauende Dritte oder Registrierungsstellen unterliegt keiner Zugriffsbeschränkung. Der LDAP Server erlaubt pro Lesezugriff eine Abfrage auf maximal 100 Datensätze.

Die Integrität und Authentizität der Sperrlisten und OCSP-Auskünfte wird durch die Signatur mit vertrauenswürdigen Signern gewährleistet.

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 eine Sekunde.

Weiterhin werden für die Öffentlichkeit relevante Dokumente in Form einer zentralen Datenablage (Repository) zur Verfügung gestellt. Dies umfasst insbesondere die entsprechenden CP/CPS Dokumente der beteiligten Stamm- und Zwischenzertifizierungsstellen (Root- und Sub-CAs). Dieses Verzeichnis ist 7x24h Stunden verfügbar. Die Ausfallzeit beträgt maximal 1,5 Tage im monatlichen Mittel.

2.2 Veröffentlichung von Zertifikatsinformationen

Die Qualified.ID publiziert die folgenden Informationen über http://www.telesec.de/signaturkarte:

- Informationen zum Ausfüllen des QUALIFIED.ID-Auftrages
- Technische Beschreibung zum Verzeichnisdienst (LDAP, OCSP Responder)
- Zertifikatsprofile
- Informationen zum Sperrservice

Die Zertifikatsinhaber und Rahmenvertragspartner 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.

Bei Änderungen der Informationssicherheitspolitik werden die betroffenen Rahmenvertragspartner sowie die Registrierungsstellen über die Änderungen informiert.

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

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

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

- Zertifikate werden umgehend nach Durchführung der Empfangsbestätigung in den Verzeichnisdienst eingestellt. Zertifikate werden nach Ablauf ihrer Gültigkeit mindestens noch ein Jahr im Verzeichnisdienst veröffentlicht.
- Richtlinien werden nach Bedarf aktualisiert.

2.4 Zugang zu den Ablagen und Verzeichnisdiensten

Der Verzeichnisdienst der Qualified.ID Dienstleistung ist unter den folgenden Adressen jederzeit (7x24 entsprechend den Anforderungen der eIDAS-Verordnung) zu erreichen:

-
- http://pks.telesec.de/ocspr
- ldap://pks-ldap.telesec.de

In dem Public Key Directory können ausgestellte und zum Abruf freigegebenen Zertifikate online abgerufen werden. Ferner ermöglichet der OCSP-Service das Nachprüfen des Status aller ausgestellten Zertifikate (gesperrt/nicht gesperrt).

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 Namensregeln

Die ausgestellten 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 ins Zertifikat aufgenommen werden, sofern der Zertifikatsinhaber den Zugriff auf das angegebene E-Mail-Postfach bestätigt hat. In E-Mail-Adressen sind keine Umlaute zulässig.

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.

3.1.1 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. Sollten einzelne Zeichen des Namens nicht im oben genannten Zeichensatz darstellbar sein, gilt für das Zertifikat die Schreibweise des Namens in der maschinenlesbaren Zone des Identifikationsdokumentes.
- 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 dieser durch das Trust Center gekürzt.

3.1.2 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 Vertrauensdiensteanbieter 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.

3.1.3 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.

3.2 Identitätsprüfung bei Neuauftrag

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.

Als weitere Identifizierungsmethode kann der Auftraggeber das PostIdent-Verfahren mit Online-Ausweisfunktion durchführen.

Die Art des Ausweisdokumentes sowie die Ausweisnummer (nicht bei PostIdent mit OnlineAusweisfunktion) 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. Diese Kopie des Ausweises ist bei der Nutzung der Online-Ausweisfunktion nicht mehr notwendig.

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.

3.2.1 Zusätzliche Prüfungen bei qualifizierten Siegelzertifikaten

Die Identitätsprüfung für den Vertretungsberechtigten einer juristischen Person erfolgt analog zu diesem Vorgehen. Dabei werden die in diesem Dokument beschriebenen Identifikationsverfahren eingesetzt. Die Existenz der juristischen Person so wie die Gültigkeit der Vertretungsmacht wird auf Basis der Vorgelegten Unterlagen aus den jeweiligen Registern oder anderen vorgelegten Urkunden geprüft

Für die Prüfungen wird eines der drei folgenden Verfahren angewendet:

- Die rechtliche, physische und betriebliche Existenz und Identität einer Organisation werden über staatlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert. Beispiele dafür sind Handelsregister, berufsständige Körperschaften öffentlichen Rechts und das Bundeszentralamt für Steuern. Für eine Prüfung werden die vom Antragsteller bereitgestellten Informationen für eine manuelle Suche in den entsprechenden Registern verwendet. Daraus resultierende Ergebnisse werden mit den bereitgestellten Informationen abgeglichen.
- Die rechtliche, physische und betriebliche Existenz und Identität einer Organisation werden über privatrechtlich geführte und für die Identifikation als zuverlässig eingestufte Quellen validiert. Diese Quellen werden hinsichtlich ihrer Zuverlässigkeit evaluiert, bevor sie von Telekom Security genutzt werden. Beispiele sind Wirtschaftsauskunftsdienste wie z.B. Dun&Bradstreet. Für eine Prüfung werden die vom Antragsteller bereitgestellten Informationen manuell mit der Datenbank abgeglichen.
- Der Antragsteller weist die rechtliche, physische und betriebliche Existenz und Identität einer Organisation durch Vorlage eines durch einen Notar ausgestellten Bescheinigungsschreiben (Verified Professional Letter gemäß [EVCG]) oder durch Vorlage einer amtlichen Beglaubigung nach. Voraussetzung für die Akzeptanz eines notariellen Nachweises ist, dass der Notar in einem entsprechend anerkannten Notarverzeichnis geführt wird.

3.2.2 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 nur einmalig mittels einer qualifizierten Signatur mit dem noch gültigen Zertifikat erfolgen. Auf der Grundlage eines Folgezertifikats kann somit kein weiteres Folgezertifikat ausgestellt werden.

3.3 Identifizierung und Authentifizierung bei Aufträgen auf Schlüsselerneuerung

Eine Schlüsselerneuerung wird nicht unterstützt.

3.4 Identifizierung und Authentifizierung bei Sperraufträgen

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

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

Eine unverzügliche Sperrung des Zertifikates kann online oder durch Anruf der Sperrhotline erreicht werden, die 7x24h betrieben wird. Für beide Wege 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.

Sperrberechtigte Institutionen (z.B. berufsständige Kammern) erhalten nach der Zertifikatsgenerierung eine „Tele-PIN“ zur Sperrung mitgeteilt.

Für die Sperrung der Zertifikate des VDA gilt ein analoger Prozess. Die Sperrung eines CA-Zertifikates kann durch autorisierte Personen entweder per signierter E-Mail 7x24h oder schriftlich beauftragt werden. Sind die

Voraussetzungen zur Sperrung (Berechtigung und Grund) erfüllt, wird die Sperrung vorgenommen, und das gesperrte Zertifikat in die Sperrinformationen übernommen.

Die autorisierte Person oder Institution werden über die Durchführung der Sperrung informiert. Die zum Prozess gehörenden Dokumente werden gemäß den Vorgaben archiviert.

4 BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsauftrag

Aufträge im Rahmen für Qualified.ID sind nur schriftlich möglich. Der Auftrag muss mit einer handschriftlichen Unterschrift des Auftraggebers versehen sein. Die notwendigen Formulare sind auf den Webseiten der Qualified.ID 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.

Alle Schritte der Zertifikatsgenerierung und auch die vorbereitenden Schritte bei den verwendeten QSCDs werden geloggt.

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 Qualified.ID Auftragsformular zu finden.

4.1.2 Beauftragung eines qualifizierten Siegelzertifikates

Neben dem vollständig und lesbar ausgefüllten Auftragsformular ist eine Kopie des Identifikationsdokumentes (z. B. Personalausweis) einer Vertretungsberechtigten Person und der Nachweis der Vertretungsmacht erforderlich, um ein qualifiziertes Siegelzertifikat zu beauftragen. Eine Liste weiterer akzeptierter Dokumente ist in den Erläuterungen zum Qualified.ID Auftragsformular zu finden.

4.1.3 Beauftragung von nicht qualifizierten Zertifikaten

Die Beauftragung von nicht qualifizierten Zertifikaten erfolgt zusammen mit der Beauftragung einer Signaturkarte für qualifizierte Signatur. Eine einzelne Beauftragung von nicht qualifizierten Zertifikaten ohne ein qualifiziertes Zertifikat ist nicht möglich.

4.2 Bearbeitung von Zertifikatsaufträgen

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 weiterer Dokumente und Formulare im Original (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 (In der Filiale oder über Online-Ausweisfunktion), 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 hier festgelegten Prozesse überprüft. Diese Prozesse werden in regelmäßigen Abständen durch eine anerkannte Konformitätsbewertungsstelle gemäß eIDAS kontrolliert.

Alle Auftragsunterlagen zu den 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 Zertifikatsausstellung

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 sichergestellt. Das ausgestellte Zertifikat wird auf der persönlichen Chipkarte des Zertifikatsinhabers und in der Kundendatenbank des Trust Centers gespeichert.

4.3.2 Ausstellung qualifizierter Siegelzertifikate

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 sichergestellt. Das ausgestellte Zertifikat wird auf der persönlichen Chipkarte des Zertifikatsinhabers und in der Kundendatenbank des Trust Centers gespeichert.

4.3.3 Ausstellung von nicht qualifizierten Zertifikaten

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

Zertifikatsakzeptanz

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 Identifikationsdokument oder Kopie Auftragsunterlagen) benötigt.

4.4.1 Annahme durch den Zertifikatsinhaber

4.4.1.1 Signaturkarte

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 sowie den korrekten Zertifikatsinhalt bestätigt hat. Der Zertifikatsinhaber sollte sich vor der Durchführung der Empfangsbestätigung vom richtigen Zertifikatsinhalt überzeugt haben.

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 zurückversetzen. Dadurch können sicherheitskritische Manipulationen an der erhaltenen Chipkarte erkannt werden.

Bei qualifizierten Siegelzertifikaten werden diese Schritte durch den Vertretungsberechtigten der juristischen Person durchgeführt.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

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

Qualified.ID 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 sowie zur Erstellung fortgeschrittener Signaturen ausgestellt.

Der Endanwender muss die Voraussetzungen zur Nutzung des Zertifikates, 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 heruntergeladen werden.

Darüber hinaus unterliegen nicht veröffentlichte Zertifikate dem Datenschutz.

Erhält der Zertifikatsendanwender Kenntnis 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.

Die Zertifikatsinhaber haben die alleinige Kontrolle über die Nutzung ihres Zertifikates. Dies wird durch Nutzung von zwei Faktoren für die Nutzung des Zertifikates sichergestellt.

Im Falle der Signaturkarte wird die Chipkarte und die zugehörige PIN benötigt.

Eine Nutzung des Zertifikates ohne diese beiden Bestandteile ist nicht möglich.

4.5.2 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.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Eine automatisierte Zertifikatserneuerung wird nicht angeboten. Kunden, die einen Folgeauftrag stellen, erhalten neues Schlüsselmaterial. Bei einer Folgebeauftragung wird ein vereinfachtes Auftragsverfahren durchlaufen. Der Kunde wird über die aktuell gültigen Vertragsdokumente unterrichtet und erkennt diese an. Eine Rezertifizierung des vorhandenen Schlüsselmaterials ist im derzeitigen Prozess nicht vorgesehen.

4.7 Schlüsselerneuerung von Zertifikaten (Re-Key)

Nicht anwendbar.

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
7. Das Zertifikat ist nicht mehr mit der gültigen Version des CP vereinbar.

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.
    - Für berufsbezogene oder sonstige Angaben zuständige Stelle, falls eine berufsbezogene oder sonstige Angabe in das qualifizierte Zertifikat aufgenommen.
    - Rechnungsempfänger
- Das Telekom Trust Center kann die Sperrung eines Zertifikates gemäß den Allgemeinen Geschäftsbedingungen für die Qualified.ID 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:

https://www.telesec.de/signaturkarte/ → Sperrservice.

Auch im Falle von Systemdefekten, Servicearbeiten oder und anderen Faktoren, die außerhalb des Einflussbereichs von Telekom Security liegen, wird Telekom Security 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 E-Mail in der er über die erfolgte Sperrung benachrichtigt wird. In dieser E-Mail wird ihm auch der genaue Sperrzeitpunkt mitgeteilt.

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.

4.9.1 Umstände einer Suspendierung

Die Suspendierung (temporäre Sperrung) von Zertifikaten wird nicht unterstützt.

4.9.2 Wer kann eine Suspendierung beantragen?

Nicht anwendbar.

4.9.3 Verfahren der Suspendierung

Nicht anwendbar.

4.9.4 Beschränkung des Suspendierungszeitraums

Nicht anwendbar.

4.10 Statusauskunftsdienste von Zertifikaten

4.10.1 Betriebseigenschaften

Von jeder gültigen CA zur Ausstellung von Zertifikaten werden für die Erbringung des OCSP-Service Zertifikate für den OCSP-Responder ausgestellt. Dieser Zertifikatstyp steht ausschließlich nur dem PKI-Betreiber Telekom Security/Deutsche Telekom AG zur Verfügung. OCSP Zertifikate werden regelmäßig, ohne Ankündigung, gewechselt.
Es werden keine Sperrlisten angeboten.

4.10.2 Verfügbarkeit des Dienstes

Der OCSP-Dienst als auch die CRL/ARL auf dem LDAP-Verzeichnisdienst stehen 7x24h Stunden zur Verfügung.
Die Antwortzeit des OCSP-Responders und LDAP-Verzeichnisdienst beträgt unter normalen Betriebsbedingungen weniger als 10 Sekunden.
Über den Zeitraum von einem Jahr wird im Mittel eine Verfügbarkeit von mehr als 99% erreicht.

4.10.3 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 Qualified.ID Webseiten verfügbar.

4.10.4 Statusauskunftsdienst

Das Telekom Trust Center betreibt einen öffentlich zugänglichen OCSP-Responder, der jederzeit (7x24) zur Statusprüfung der Zertifikate genutzt werden kann. Die Adresse des OCSP-Responders lautet http://pks.telesec.de/ocspr.
Die Schnittstellenspezifikation zu diesem Dienst ist auf den Qualified.ID Webseiten verfügbar:
https://www.telesec.de → Service → Downloads → Produkte & Lösungen → Public Key Service → Signaturkarte PKS → Technische Dokumentation
Die OCSP Antwort ist nicht von der Lebensdauer der CA abhängig, da der TSP autorisierte OCSP-Auskünfte auch nach Ablauf der ausstellenden CA zur Verfügung stellt.

Für die Prüfung der CA-Zertifikate steht eine ARL zur Verfügung. Diese wird bei Bedarf (Erstellung oder Sperrung einer CA) oder spätestens nach 6 Monaten erneuert.

4.10.5 Sperrliste

Nicht anwendbar.

4.10.6 Optionale Funktionen

Nicht anwendbar.

4.11 Beendigung des Vertragsverhältnisses

Es besteht kein Dauerschuldverhältnis mit dem Zertifikatsinhaber. Daher ist neben der Sperrung des Zertifikates keine weitere Vertragskündigung notwendig.

4.12 Schlüsselhinterlegung und Wiederherstellung

Die Hinterlegung und Wiederherstellung von Schlüsseln auf der Signaturkarte werden aus Sicherheitsgründen nicht angeboten.

4.12.1 Richtlinien für Schlüsselhinterlegung und –wiederherstellung

Nicht anwendbar.

4.12.2 Sitzungsschlüsselkapselung und Richtlinien für die Wiederherstellung

Nicht anwendbar.

5 GEBÄUDE-, VERWALTUNGS- UND BETRIEBSKONTROLLEN

Das Trust Center der Telekom Security 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.
Das Management genehmigt die Risikobewertung und akzeptiert das identifizierte Restrisiko.

5.1 Physikalische Kontrollen

Die Produktion von Signaturkarten erfolgt im Trust Center der Telekom Security. 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

Telekom Security betreibt ein Trust Center, welches aus zwei voll redundant ausgelegten Standorten. Beide Standorte verfügen über eigenständige Energietrakte (Elektro, Klima, Wasser) mit einem eigenen Gebäudemanagementsystem und Notstromaggregaten.
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 Angriffshemmung. Das Trust Center ist sicherheitstechnisch 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 Räumlicher 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, ortsfesten Notstromaggregaten mit einer Leistung, die der Volllast des Rechenzentrums entspricht.

5.1.4 Wassergefährdung

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 Räume sind Brandfrühsterkennungssystemen (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 Telekom Security/Deutsche Telekom AG entsorgt.

5.1.8 Externe Sicherung

Telekom Security 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 Maßnahmen

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 und 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 Risikokonzept 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 deren Umsetzung wird geprüft.

5.2.1 Vertrauenswürdige Rollen

Vertrauenswürdige Personen sind alle Personen (Telekom Security/Deutsche Telekom AG 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,
- Registrierungsmitarbeiter
- die Security Officer
- System-Auditoren
- Sicherheitspersonal,

- zuständiges technisches Personal und
- für die Verwaltung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

Dabei werden folgende Aufgaben zurzeit ganz oder teilweise durch Auftragnehmer oder unabhängige Dritte durchgeführt:

- Betrieb des Rechenzentrums (maximal bis auf Betriebssystemebene der IT-Systeme)
- Registrierung von Endkunden
- Archivierung von Dokumenten in entsprechenden Hochsicherheitsarchiven

Die oben genannten vertrauenswürdigen Personen müssen die in diesem CPS festgelegten Anforderungen (siehe Kapitel 5.3.1) erfüllen.
Diese vertrauenswürdigen Personen müssen die jeweilige(n) Rolle(n) zugewiesen werden. Durch eine schriftliche Bestätigung (z.B. per E-Mail) akzeptieren diese Personen ihre zugewiesene(n) Rolle(n). Diese Nachweise müssen mindestens 7 (Sieben) Jahre archiviert werden.
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 Change Advisory Board des Trust Centers der Telekom Security ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten, im CP/CPS der vom Trust Center der Telekom Security betriebenen Zertifizierungsstellen dargestellt werden.

5.2.2 Anzahl involvierter Personen pro Aufgabe

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. Der Kreis der Personen, die diese Tätigkeiten ausführen dürfen, ist auf ein Minimum reduziert.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Telekom Security Mitarbeiter, die als besonders vertrauenswürdige Personen eingestuft sind und besonders vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer Telekom Security-internen Sicherheitsüberprüfung. Telekom Security 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.

5.2.4 Rollen, die eine Funktionstrennung erfordern

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

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

Die Ausschlüsse der verschiedenen Rollen erfolgt über alle Teile des TSP. Sollten sich darüber hinaus Rollenkonflikte aus der Tätigkeit in anderenTeilen des TSP ergeben, wird der entsprechende Mitarbeiter nur in einem Teil eingesetzt.

5.2.5 Schwachstellenbewertung

Nach jeder signifikanten System- oder Netzwerkänderung oder einer Aufforderung 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.

5.2.6 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.

5.2.7 Standards und Kontrollen für kryptographische Module

Die privaten Schlüssel der CAs werden auf eine FIPS 140-2/ Level 3 evaluiertem Hardware Security Modulen (HSM) oder QSCD evaluierten Geräten abgelegt. Die Sicherung der Schlüssel bei Verwendung von HSMs 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

5.3 Personelle Maßnahmen

Telekom Security 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 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 Telekom Security Change Advisory Board ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten und CP/CPS der von Telekom Security Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Telekom Security 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 polizeiliches Führungszeugnis der Telekom Security vorzulegen.

5.3.2 Sicherheitsüberprüfung

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt Telekom Security 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 Telekom Security 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.

5.3.3 Schulungs- und Fortbildungsanforderungen

Das Personal des Telekom Security Trust Centers besucht Fortbildungsmaßnahmen, die zur kompetenten und zufriedenstellenden Erfüllung ihrer beruflichen Pflichten erforderlich sind. Telekom Security 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 Telekom Security,
- 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)

5.3.4 Nachschulungsintervalle und -anforderungen

Das Personal der Telekom Security erhält im erforderlichen Umfang und spätestens nach Ablauf von 12 Monaten Auffrischungsschulungen und Fortbildungslehrgänge.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

5.3.6 Sanktionen bei unbefugten Handlungen

Telekom Security 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.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Telekom Security behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter von Telekom Security in vergleichbarer Position.
Obiger Personenkreis, der die beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von Telekom Security nicht gestattet.
Alle eingesetzten unabhängigen Auftragnehmer werden vor Aufnahme der Tätigkeit über entsprechende Verträge eingebunden. Dabei achtet der VDA darauf die vom Auftragnehmer erbrachten Leistung so festzulegen, dass der VDA seinerseits allen Verpflichtungen nachkommen kann. Dies gilt insbesondere beim Schutz personenbezogener Daten und anderen gesetzlichen Verpflichtungen.
Verstöße gegen die Regularien können je nach Ursache und Schwere des Verstoßes unterschiedlich sanktioniert werden. Diese Sanktionen reichen von einer Nachschulung des Personals, über den Ausschluss bestimmter Mitarbeiter des Dienstleisters von der Tätigkeit für den TSP bis zur kompletten Beendigung der Zusammenarbeit mit diesem Dienstleister.

5.3.8 Dokumentation für das Personal

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

5.4 Protokollereignisse

Es ist im Loggingkonzept sowie im Installationshandbuch festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden und wie sie vor Verlust und unbefugtem Zugriff geschützt werden. Es werden dabei die Anforderungen aus [ETSI EN TSP] Kap. 7.10 umgesetzt.

5.4.1 Art der aufgezeichneten Ereignisse

Generell enthalten alle Protokolleinträge mindestens das Datum und die Uhrzeit des Eintrags, einen Verweis auf die Person oder das System, welches den Eintrag generiert hat, sowie eine Beschreibung des Ereignisses.

5.4.1.1 CA-Schlüsselpaare und CA-Systeme

Für das Lifecycle–Management für CA-Schlüsselpaare bzw. von CA-Systemen protokolliert das Telekom Security Trust Center für Qualified.ID mindestens die folgenden Ereignisse:

a) Erzeugung, Vernichtung, Speicherung, Sicherung und Wiederherstellung, sowie Archivierung des Schlüsselpaares oder Teile des Schlüsselpaares
b) Ereignisse im Lebenszyklus-Management von kryptografischen Geräten (z.B. HSM), sowie der eingesetzten CA-Software

5.4.1.2 EE- und CA-Zertifikate

Für das Lifecycle-Management von EE- als auch CA-Zertifikaten und deren Validierung protokolliert das Telekom Security Trust Center für Qualified.ID mindestens die folgenden Ereignisse:

a) Auftrag und Sperrung von Zertifikaten
b) Alle Tätigkeiten im Zusammenhang mit der Verifikation von Informationen
c) Annahme oder Ablehnung von Zertifikatsaufträgen
d) Ausstellung eines Zertifikates
e) Erzeugung von Sperrlisten (CRL) und OCSP-Einträgen

5.4.1.3 Sonstige sicherheitsrelevante Ereignisse

Zusätzlich werden vom Telekom Security Trust Center für den Betrieb der Infrastruktur alle sicherheitsrelevanten Ereignisse protokolliert. Das beinhaltet mindestens die folgenden Ereignisse:

a) Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI
b) Durchgeführte Aktionen an und durch PKI- und sonstigen sicherheitsrelevanter Systeme
c) Änderungen an Sicherheitsprofil
d) Systemabstürze, Hardware-Ausfälle und andere Anomalien
e) Firewall- und Router-Aktivitäten
f) Zutritt und Verlassen von Einrichtungen des Trust Centers
g) Ergebnisse von Netzwerkprüfungen (Schwachstellenüberprüfungen)
h) Start und Beendigung des Loggingprozesses

5.4.2 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/History-Daten/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft Telekom Security 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.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Audit-Protokolle/History-Daten/Logging-Dateien werden nach Bearbeitung gemäß den gesetzlichen Verpflichtungen archiviert.

5.4.4 Schutz der Audit-Protokolle

Audit-Protokolle/History-Daten/Logging-Dateien werden mit Betriebssystemmechanismen gegen unbefugten Zugriff geschützt.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Eine inkrementelle Sicherung von Audit-Protokollen/History-Daten/Logging-Dateien wird täglich durchgeführt.

5.4.6 Audit-Erfassungssystem (intern vs. extern)

Audit-Daten/History-Daten/Logging-Dateien von Anwendungs-, Netzwerk- und Betriebssystemebene werden automatisch erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von Telekom Security -Mitarbeitern aufgezeichnet.

5.4.7 Benachrichtigung des ereignisauslösenden Subjekts

Ereignisse, die das Audit-Monitoringsystem erfasst, werden bewertet an das zuständige Trust-Center-Personal weitergeleitet. Ereignisse mit hoher Priorität werden unverzüglich -auch außerhalb der Regelarbeitszeit- an das Trust-Center-Personal weitergeleitet.

5.4.8 Schwachstellenbewertung

Nach jeder signifikanten System- oder Netzwerkänderung oder einer Aufforderung des CA/Browserforums 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.

5.5 Datenarchivierung

5.5.1 Art der archivierten Datensätze

Telekom Security archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener Form (z.B. Angebote, Aufträge),

- Informationen in Zertifikatsanträgen und zum Zertifikatslebenszyklus (z.B. Sperr- und Erneuerungsanträge),
- alle Audit-Daten/History-Daten/Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden,

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Alle Aufzeichnungen innerhalb des Telekom Security Trust Centers werden, wenn sie sich auf qualifizierte Zertifikate gemäß dem deutschen Signaturgesetz beziehen, 30 Jahre lang aufbewahrt. Andere Aufzeichnungen werden entsprechend der derzeit gültigen Gesetze aufbewahrt.
Audit-, History- und Event-Logging Daten werden bis zu zweiundvierzig (42) Tage archiviert.

5.5.3 Schutz von Archiven

Telekom Security stellt sicher, dass nur autorisierte und vertrauenswürdige Personen Zutritt zu Datenträgerarchiven erhalten. Archivdaten sind gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt.

5.5.4 Sicherungsverfahren für Archive

Eine inkrementelle Sicherung der elektronischen Archive wird täglich durchgeführt.

Telekom Security bewahrt die Datenträger auf, die die Archivdaten und die zur Verarbeitung der Archivdaten erforderliche Anwendungen enthalten, um die Archivdaten für den in dieser CP/CPS festgelegten Archivierungszeitraum zu gewährleisten.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Datensätze wie beispielsweise Zertifikate, Zertifikatssperrlisten, OSCP-Antworten, Loging-Dateien enthalten Informationen über Datum und Uhrzeit. Als Zeitquelle dient das Empfangssignal des DCF 77, aus dem die UTC abgeleitet wird. Die einzelnen Systeme gleichen die Systemzeit mit der Zeitquelle mehrmals am Tag ab.

5.5.6 Archiverfassungssystem (intern oder extern)

Telekom Security verwendet für die elektronische Archivierung ausschließlich interne Archivierungssysteme. Papierunterlagen werden, sofern kein Zugriff mehr im normalen Arbeitsablauf notwendig ist, bei einem zertifizierten externen Dienstleister in hochsicheren Archiven aufbewahrt.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Nur autorisiertes und vertrauenswürdiges Personal erhält Zutritt zu Archiven und damit Zugang und Zugriff auf Archivdaten. Bei der Wiederherstellung der Archivdaten werden diese auf Authentizität verifiziert.
Für den Zugriff auf die Daten ist eine begründete Anfrage bei einer der folgenden Rollen (gemäß Kap. 5.2.1) zu stellen:

- Leiter Trust Center
- Leiter VDA
- Trust Center Information Security Officer
- Solution Manager des betroffenen Trust Services

Nach Prüfung der Begründung werden die Informationen über die autorisierten Mitarbeiter (gemäß Kap. 5.5.3) zur Verfügung gestellt.

5.6 Schlüsselwechsel

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

Betroffene Nutzer werden über diese Maßnahme informiert.

5.7 Kompromittierung und Wiederherstellung (Disaster Recovery)

5.7.1 Umgang mit Störungen und Kompromittierungen

Telekom Security 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 QUALIFIED.ID-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 Telekom Security 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.

Der 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.

5.7.2 Beschädigung von EDV-Geräten, Software und/oder Daten

Bei einer Beschädigung der EDV-Komponenten, Software und/oder Daten wird der Vorfall unmittelbar untersucht und der Sicherheitsabteilung der Telekom Security gemeldet. Das Ereignis initiiert eine entsprechende Eskalation, Störfalluntersuchung, Störfallreaktion bis hin zur finalen Störungsbeseitigung. Abhängig von der Störungsklassifizierung erfolgt die Wiederherstellung (Disaster Recovery).

Jegliche Hard- und Software, die zur Bereitstellung des QUALIFIED.ID-Service erforderlich ist, wird als Vermögensgegenstand (Asset) und Anwendung im Konfigurationsmanagement der Telekom Security geführt.

Diese Anwendung bildet auch die Basis für ein Problem-Management.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme über 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. Auskünfte zum Sperrstatus von Enduser-Zertifikaten sowie die Enduser-Zertifikate, die auf kompromittierten privaten Schlüsseln basieren sind unter Umständen nicht mehr gültig.

5.7.4 Geschäftskontinuität nach einem Notfall

Telekom Security 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 wiederherzustellen. 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. Die Wiederherstellung der Daten nach einem Notfall erfolgt über zu diesem Zweck regelmäßig angelegte Backups. Diese werden in regelmäßigen Abständen auf ihre Funktionsfähigkeit geprüft.

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.

5.8 Betriebsbeendigung einer Zertifizierungs- oder Registrierungsstelle

5.8.1 Beendigung der Zertifizierungsstelle

5.8.1.1 Vertrauensdiensteanbieter 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 gilt für alle qualifizierten Signaturzertifikate und die qualifizierten Siegelzertifikate des TSP.

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.

5.8.1.2 Zertifizierungsdiensteanbieter für nicht qualifizierte Zertifikate

Eine Betriebsbeendigung kann nur durch die Telekom Security 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.

5.8.2 Beendigung der externen Registrierungsstelle

Da alle Kunden zentral über die Zertifizierungsstelle verwaltet werden, und keine Dokumente bei einer Registrierungsstelle verbleiben, hat die Beendigung einer Registrierungsstelle keine Auswirkungen auf den Betrieb und den Kunden.

6 TECHNISCHE SICHERHEITSKONTROLLEN

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

6.1.1.1 Generierung von Schlüsselpaaren Endanwender

Schlüsselpaare für Endanwender-Zertifikate werden auf der QSCD (Chipkarte des Zertifikatsinhabers oder HSM des VDA) selbst erzeugt, die über eine Zertifizierung für qualifizierte Signaturerstellungseinheiten gemäß eIDAS (QSCD) verfügen. Nach der Generierung werden die Schlüssel sicher auf der jeweiligen QSCD gespeichert. Im Falle der Chipkarte wird der private Schlüssel auf der Chipkarte sicher abgelegt, kann nach der Speicherung nicht mehr ausgelesen werden. Schlüsselgenerierung (Vorproduktion) und die Generierung und Speicherung des Zertifikats des Endanwenders erfolgen in getrennten Produktionsschritten.

Für die Schlüsselgenerierung und Schlüsselverwendung gelten die Anforderungen des SOG-IS Algorithmenkatalogs.

6.1.1.2 Generierung und Erneuerung von CA- und Root-Zertifikaten

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) oder auf QSCD Geräten in der sogenannten “Key Ceremony” (Schlüsselgenerierungsverfahren) erzeugt und abgelegt. An der Generierung der Schlüssel nehmen neben einem Administrator als Root-Fachkraft, und einem verantwortlichen für die Root auch ein Auditor teil. Abhängig von den Anforderungen an die ausgestellten Zertifikate ist dies ein interner oder ein externer Auditor.

Alle Aktivitäten während der “Key Ceremony“ werden protokolliert und von allen beteiligten Personen unterzeichnet.

Diese Aufzeichnungen werden zu Audit- und Nachverfolgungszwecken für einen von Telekom Security als angemessen erachteten Zeitraum aufbewahrt.

Bei einem regulären Wechsel der CA-Zertifikat stellt die Telekom Security einen angemessenen Zeitraum für den Übergang zwischen den CA-Zertifikate sicher. Insbesondere wird die Gültigkeitsprüfung für die bestehenden Enduserzertifikate berücksichtig.

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 gegen Öffnung und Austausch gesichert.

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.

Kurz vor dem Ablauf des CA-Zertifikates wird dieses dann im Betrieb durch ein neu generiertes Zertifikat ersetzt. Nicht mehr benötigte CA-Zertifikate (inkl. Backups der privaten Schlüssel) werden unbrauchbar gemacht.

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.

Die CA-Schlüssel werden nur für die Signatur von Endanwenderzertifikaten verwendet.

Über den Qualified.ID Newsletter wird rechtzeitig über den Austausch der Zertifikate informiert. Jeder mit plausiblem Interesse kann sich beim QUALIFIED.ID Support als Empfänger für den Newsletter registrieren.

6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Smartcards werden auf dem Postweg an den Endteilnehmer versendet

6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller

Die Zertifikatsausstellung erfolgt ausschließlich beim TSP.

6.1.4 Zustellung öffentlicher Zertifizierungsstellenschlüssel an Vertrauende Dritte

Nicht anwendbar.

6.1.5 Schlüssellängen

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.

Tabelle 4 - Verwendete Schlüsselalgorithmen

Schlüssel	Verwendet bis/seit
RSA 1024 Bit	Verwendet bis 31.12.2007
RSA 2048 Bit	Verwendet bis 31.12.2014
Elliptische Kurven	Verwendet seit 15.01.2013
RSA 2048 Bit	Verwendet vom 01.06.2020 bis 12.05.2023 für Fernsignaturzertifikate

Bei allen Zertifikaten gilt, dass diese nicht länger gültig sind, wie der von der SOG-IS Crypto Working Group herausgegebene Algorithmenkatalog die verwendeten Algorithmen als sicher einstuft. Die Angaben aus dem Algorithmenkatalog ergänzen die hier getätigten Angaben zu der maximalen Gültigkeitsdauer und haben den hier getätigten Angaben Vorrang.

6.1.6 Generierung der Parameter vom öffentlichen Schlüssel und Qualitätskontrolle

Nicht anwendbar.

6.1.7 Schlüsselverwendungen (gemäß X.509v3-Erweiterung „key usage“)

Die Schlüsselverwendung richtet sich nach den Regeln des RFC5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” und ist darin beschrieben.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptographischer Module

Das Trust Center der Telekom Security hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA- und Root-CA-Schlüsseln gewährleisten zu können. Diese Mechanismen werden auch für den Schutz der Endanwenderschlüssel auf dem HSM angewendet, damit die alleinige Verfügungsgewalt über die Schlüssel und das Zertifikat durch den rechtmäßigen Nutzer gewährleistet ist. Für den Schutz der privaten Schlüssel auf der Chipkarte ist der Endanwender verantwortlich.

Um das Risiko eine Schlüsselkompromittierung bei der Übertragung zwischen zwei HSM zu verhindern werden Verschlüsselungsmechanismen eingesetzt. Die gültigen Schlüssel für die Verbindung zwischen zwei HSM wird auf einem Trägermedium in einem Tresor des TSP aufbewahrt. Dieser Tresor befindet sich nicht am RZ-Standort. Neben dem eingesetzten Schlüssel wird ein direkter Zugang zum HSM am jeweiligen RZ-Standort benötigt. Auf dieses Weise ist sichergestellt, dass eine Kompromittierung auf dem Übertragungskanal nicht möglich ist.

Die Endanwender sind verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um den Verlust, Offenlegung und unberechtigte Nutzung von privaten Schlüsseln zu verhindern.

6.2.1 Standards und Kontrollen für kryptographische Module

Die privaten Schlüssel der CAs, für die Nutzung im Umfeld das Karten basierten Dienste werden auf geeigneten QSCDs 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.

6.2.2 Mehrpersonenkontrolle (m von n) bei privaten Schlüsseln

Telekom Security hat technische, organisatorische und prozessuale Mechanismen implementiert, die die Teilnahme mehrerer vertrauenswürdiger und geschulter Personen des Telekom Security Trust Centers (Trusted Roles) erfordern, um vertrauliche kryptografische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentification mit Key) geschützt, der nur hierfür zuständigen Personen bekannt ist. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

6.2.3 Hinterlegung von privaten Schlüsseln

Nicht anwendbar.

6.2.4 Sicherung von privaten Schlüsseln

Nicht anwendbar.

6.2.5 Archivierung privater Schlüssel

Nicht anwendbar.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptographischen Modul

Nicht anwendbar.

6.2.7 Speicherung privater Schlüssel auf kryptographischen Modulen

Das Telekom Security Trust Center speichert CA-Schlüssel in sicherer Form auf kryptografischen Hardware-Security-Modulen (HSM), welche nach FIPS 140-2/ Level 3 evaluiert sind.

Smartcards speichern extern erzeugte Schlüssel oder selbst generierte Schlüssel in sicherer Form.

6.2.8 Methode zur Aktivierung privater Schlüssel

Alle Endteilnehmer müssen die Aktivierungsdaten (z.B. PIN) für ihren privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß der vorliegenden CP/CPS schützen.

Der private Schlüssel des Zertifikats einer Zwischenzertifizierungsstelle (Sub-CA) bleibt aktiv bis der Gültigkeitszeitraum überschritten wurde oder ein Sperrgrund vorliegt, der die Zertifikatssperrung auslöst.

6.2.9 Methode zur Deaktivierung privater Schlüssel

Die Deaktivierung von CA- und Root-CA-Schlüsseln erfolgt ereignisbezogen und obliegt dem Personal des Trust Centers der Telekom Security.

Die Deaktivierung von privaten Schlüsseln (Endteilnehmer, Registratoren) obliegt dem Endanwender.

6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von CA-Schlüsseln erfordert die Teilnahme mehrerer vertrauenswürdiger Personen (Trusted Roles) des Trust Centers. Dabei ist sicherzustellen, dass nach Vernichtung keine Fragmente des Schlüssels übrigbleiben, die zu einer Rekonstruktion des Schlüssels führen könnte.

Telekom Security verwendet zur sicheren Schlüsselvernichtung eine integrierte Löschfunktion des HSM. Schlüssel auf einer Chipkarte werden durch die physikalische Zerstörung der Chipkarte vernichtet.

Wenn kryptografische Module am Ende ihrer Nutzungsdauer oder aufgrund eines Defekts außer Betrieb genommen werden, so werden alle privaten Schlüssel, die in diesen Modulen gespeichert sind, wie oben beschrieben zerstört. Die Zerstörung betrifft nicht die Kopien der privaten Schlüssel, sofern die Schlüssel in anderen bzw. neuen kryptografischen Modulen noch weiter genutzt werden sollen.

6.2.11 Die Vernichtung von privaten Schlüsseln der Endteilnehmer obliegt diesen selbst.Bewertung kryptographischer Module

Siehe Kapitel 6.2.1

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Im Rahmen der regelmäßigen Sicherungsmaßnahmen von Telekom Security werden die Zertifikate (CA-, Root-Zertifikate) gesichert und archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

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. Die Zertifikate können jedoch weiterhin zur Entschlüsselung und Signaturvalidierung verwendet werden, sofern der dazu passende Schlüssel vorliegt.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Um die auf dem HSM hinterlegten privaten Schlüssel der CA- und Root-CA-Zertifikate schützen zu können, werden Aktivierungsdaten (Geheimnisanteile) nach dem in Kapitel 6.2.2 dieser CP/CPS beschriebenen Anforderungen und dem Dokument „Key Ceremony“ generiert. Die Erstellung und Verteilung von Geheimnisanteilen werden protokolliert.

6.4.2 Schutz von Aktivierungsdaten

Die Trust-Center-Administratoren bzw. autorisierte Personen der Telekom Security verpflichten sich, die Geheimnisanteile für die Aktivierung der privaten Schlüssel der CA-, Root-CA und OCSP-Zertifikate zu schützen.

6.4.3 Weitere Aspekte von Aktivierungsdaten

Sofern Aktivierungsdaten für private Schlüssel, unabhängig vom Übertragungsmedium, übertragen werden, müssen die Trust-Center-Administratoren die Übertragung mithilfe von Methoden zum Schutz gegen Verlust, Diebstahl, Änderung, unbefugter Offenlegung oder Nutzung dieser privaten Schlüssel schützen.

Bei der Verwendung der Kombination von Benutzername und Passwort zur Anmeldung an Netzwerken als Aktivierungsdaten für einen Endteilnehmer, müssen die in einem Netzwerk zu übertragenen Kennwörter ebenfalls gegen den Zugriff durch unbefugte Benutzer geschützt werden.

6.5 Computer-Sicherheitskontrollen

Im Trust Center von Telekom Security 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 Telekom Security ihre Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen.

Audit-, History- und Event-Logging Daten werden entsprechend den aktuellen gesetzlichen Bestimmungen archiviert. Die Aufbewahrungszeit bei Log-Daten die nicht in direktem Zusammenhang mit dem Zertifikatslebenszyklus stehen beträgt 42 Tage. 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.

Die Sicherheitsmaßnamen umfassen

- Physikalische Sicherheit und Sicherung der Umgebung,
- Die CA-Systeme sind so konfiguriert, dass nicht benötigte Ports, Accounts, Anwendungen, Services und unsichere Kommunikations-Protokolle entweder deaktiviert oder entfernt wurden,
- Maßnahmen zum Schutz der Systemintegrität, die mindestens aus Konfigurationsmanagement, Schutz von Sicherheitsanwendungen und Malware-Erkennung und -verhinderung bestehen,
- Netzwerksicherheit und Firewall Management, inklusive Portsperren und IP Adressfilterung, als auch Intrusion Detection System (IDS) und Intrusion-Prevention-Systeme (IPS),
- Benutzerverwaltung, Berechtigungsmatrix, Aufklärung, Sensibilisierung und Schulung/Ausbildung sowie
- Verfahrenskontrollen, Aktivitätsprotokollierung und Abschaltung bei Timeouts.

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

Alle diese Maßnahmen stehen im Einklang mit dem vom TSP erstellten Zugriffskonzept.

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 die der TSP als wesentlich erachtet,
- mindestens aber ein Mal pro Jahr.

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.

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

6.5.1.1 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 QSCDs zur Generierung und Speicherung privater Schlüssel verfügen über die Zulassung als qualifizierte Signaturerstellungseinheit gemäß der eIDAS Verordnung.
- Die eingesetzten HSMs für die Zertifikatssignatur und OSCP verfügen über vergleichbare Zertifizierungen.

6.5.1.2 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.

Telekom Security hat insbesondere Mechanismen zum Schutz des Sperrstatus-Dienstes (CRL, ARL, OCSP) gegen unbefugte Versuche implementiert, um Manipulationen an Sperrstatusinformationen (hinzufügen, löschen, ändern) zu verhindern. Diese Sicherungsmechanismen unterliegen der Überwachung des Alarmierungssystems, so das eine permanente Überwachung der Konfiguration erfolgt. Darüber hinaus werden die Konfigurationsdateien aller Systeme regelmäßig, in einem maximalen Abstand von 3 Monaten überprüft.

6.5.1.3 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.

Telekom Security hat Mechanismen zum Schutz der zentralen Datenablage (Repository) gegen nicht autorisierte Versuche implementiert, um Manipulationen an diesem System (hinzufügen, löschen, ändern) zu verhindern.

6.5.2 Bewertung der Computersicherheit

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 mindestens einmal jährlich sogenannte Penetrationstests durchgeführt. Auch hier werden entsprechend Maßnahmen abgeleitet und umgesetzt, sofern dies notwendig ist. Die Penetrationstest und Schwachstellenscans werden von dafür geschultem Personal durchgeführt. Die eingesetzten Werkzeuge entsprechen dabei dem aktuellen Stand der Technik.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Systementwicklungskontrollen

Telekom Security 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 Telekom Security. Erst nach erfolgreichen Tests erfolgt die Installation auf dem Wirksystem der Telekom Security. Alle Änderungen an den Systemen werden entsprechend den Vorgaben des Change- und Release-Prozess der Telekom Security dokumentiert.

Das bei der Telekom Security etablierte Change- und Release-Management findet Anwendung.

6.6.2 Sicherheitsverwaltungskontrollen

Telekom Security hat Mechanismen und/oder Richtlinien implementiert, um die Konfiguration seiner CA-Systeme kontrollieren und überwachen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Die Systemkonten (System Accounts) der Trust-Center-Administratoren werden spätestens nach 90 Kalendertagen überprüft. Nicht mehr benötigte Accounts werden deaktiviert.

6.6.3 Sicherheitskontrollen des Lebenszyklus

Telekom Security 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.

6.6.3.1 Kapazitätsmanagement

Telekom Security führt alle PKI-Funktionen mit Hilfe vertrauenswürdiger und geeigneter Systeme durch. Die Systeme werden von Monitoring-Systemen fortlaufend auf Funktion und Kapazität geprüft, so dass im Bedarfsfall zeitnah eine Erweiterung von Ressourcen durchgeführt werden kann.

Die im Monitoring (periodisch alle 5 Minuten) erhobenen Daten zu CPU-, Speicher- und Disk-Auslastung sind mit Warn- und Alarm-Schwellen versehen. Spätestens mit Eintreten der Warn-Stufe wird die Ressourcen-Planung geprüft und ggf. durch Erweiterungen (z.B. Hardware-Nachrüstung, Verlagerung von Diensten auf andere Systeme oder Zuweisung von weiteren Ressourcen an virtuelle Maschinen) angepasst.

6.7 Netzwerk-Sicherheitskontrollen

Netze und Systeme werden mithilfe mehrstufiger Firewalls, IDS und IPS, Segmentierung sowie weiteren Schutzmaßnahmen vor unautorisierten Zugriffen und Angriffen geschützt. Die Segmentierung des Netzwerks basiert auf einer Risikobetrachtung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehungen zwischen vertrauenswürdigen Systemen und Diensten. Verbindungen sind so eingeschränkt, dass nur die zum Betrieb erforderlichen Verbindungen möglich sind, nicht benötigte Verbindungen werden explizit verboten oder deaktiviert. Die Netzwerke zur Administration der Systeme sind von den operativen Netzwerken separiert.

Die Konfigurationen der Systeme werden hinsichtlich der Einhaltung dieser Regeln in regelmäßigen Abständen und bei Bedarf geprüft.

Alle für den CA-Betrieb kritischen Systeme sind in sicheren oder hochsicheren Zonen untergebracht. Innerhalb einer Zone gelten für alle Systeme die gleichen Mindestsicherheitsanforderungen.

Das Zertifikatsmanagementsystem und die dazugehörigen HSMs der Root-CAs werden auf einer reinen Offline-CA betrieben, d.h. in einem physisch abgeschotteten Netzwerk ohne Netzverbindung zu anderen Netzwerken.

Die Kommunikation ist grundsätzlich auf mehreren Schichten verschlüsselt und wird für fast alle Systeme, mindestens jedoch für die vertrauenswürdigen Systeme, über vertrauenswürdige Kanäle realisiert, die eine sichere Identifizierung ihrer Endpunkte gewährleisten.

Alle externen Netzanbindungen sind redundant aufgebaut.

Nach signifikanten System- oder Netzwerkänderungen erfolgt i.d.R. innerhalb einer Woche, mindestens jedoch einmal je Quartal eine Schwachstellenprüfung an öffentlichen und privaten IP-Adressen.

Bei Inbetriebnahme oder signifikanten Änderungen an der Infrastruktur bzw. Anwendungen, mindestens jedoch einmal pro Jahr, werden Penetrationstests durchgeführt.

Schwachstellenscans und Penetrationstests werden von Personen oder Organisationen durchgeführt, die über die für eine zuverlässige Prüfung und Dokumentation erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung wird zusammen mit den Ergebnissen dokumentiert.

Nach Bekanntwerden einer kritischen Schwachstelle wird diese i.d.R., sofern es keine guten Gründe gibt, die Schwachstelle nicht zu beseitigen, innerhalb von 48 Stunden behoben. Sollte eine Behebung innerhalb von 48 Stunden nicht möglich sein, so wird ein Plan zur Minderung der Schwachstelle, inkl. einer Priorisierung der Aktivitäten, erstellt und in dem dort festgelegten Zeitraum abgearbeitet. Sollte entschieden werden, eine Schwachstelle nicht zu beheben, so wird die begründete Entscheidung dokumentiert.

6.8 Zeitstempel

Zertifikate, Sperrlisten, Online-Statusprüfungen und andere wichtige Informationen enthalten Datums- und Zeitinformationen, die aus einer zuverlässigen Zeitquelle abgeleitet werden. Ein kryptografischer Zeitstempel wird nicht verwendet.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofil

Die Spezifikation des Zertifikatsprofils für qualifizierte Signaturen ist auf den Qualified.ID Webseiten verfügbar unter
https://www.telesec.de → Service → Downloads → Produkte & Lösungen → Public Key Service → Signaturkarte PKS → Technische Dokumentation
Die Spezifikation des Zertifikatsprofils für qualifizierte Siegel ist auf den Qualified.ID Webseiten verfügbar unter
https://www.telesec.de → Service → Downloads → Produkte & Lösungen → Public Key Service → Signaturkarte PKS → Technische Dokumentation
Die Spezifikation des Zertifikatsprofils für fortgeschrittene Zertifikate ist auf den Qualified.ID Webseiten verfügbar unter
https://www.telesec.de → Service → Downloads → Produkte & Lösungen → Public Key Service → Signaturkarte PKS → Technische Dokumentation

7.2 Sperrlistenprofil

Nicht anwendbar.

7.3 OCSP-Profil

Die Spezifikation des OCSP-Responders ist auf den Qualified.ID Webseiten verfügbar unter
https://www.telesec.de → Service → Downloads → Produkte & Lösungen → Public Key Service → Signaturkarte PKS → Technische Dokumentation

Der eingesetzte OCSP-Responder erfüllt die Anforderungen des RFC6960.

8 COMPLIANCE-AUDITS UND ANDERE PRÜFUNGEN

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.

Qualified.ID (qualifizierter Bereich): Die Telekom Security Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319411-2, policy QCP-n-qcsd) unterzogen. Telekom Security führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen durch.

Für Qualified.ID werden die geforderten Audits nach dem ETSI EN 319 411-2 Kriterien (in Kombination mit ETSI EN 319 401 and ETSI EN 319 411-1) abgelegt. Die zugehörigen Berichte werden auf der Internetseite https://www.telesec.de veröffentlicht.

8.1 Intervall oder Gründe 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 Telekom Security 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).

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 dem oben aufgeführten ETSI-Normen geprüft.

8.5 Maßnahmen zur Mängelbeseitigung

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 Telekom Security übergeben.

Telekom Security behält sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der Telekom Security.

8.7 Selbst-Audits

Telekom Security führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen durch. Diese Selbstaufsichtsmaßnahmen (Quality Assesments) werden von dafür qualifizierten Telekom Security Mitarbeitern durchgeführt.

Das Telekom Security Trust Center führt zusätzlich 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,
- zu einem wirtschaftlichen Risiko 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 Telekom Security 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.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

Die aktuelle Preisliste ist jederzeit auf den Qualified.ID Webseiten verfügbar unter

https://www.telesec.de → Service → Downloads → Allgemeine Geschäftsbedingungen

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

Telekom Security ist berechtigt, für das Ausstellen von Endteilnehmer-Zertifikaten Entgelte zu berechnen. Dies gilt insbesondere für die Bereitstellung und Überlassung des Dienstes QUALIFIED.ID.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Telekom Security berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst des Public Key Service keine Entgelte.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

Telekom Security berechnet für den Zugriff auf Sperrungs- oder Statusinformationen für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile keine Entgelte.

9.1.4 Entgelte für andere Leistungen

Telekom Security berechnet keine Entgelte auf den Abruf und der damit verbundenen Betrachtung dieses Dokuments „CP/CPS“. Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1), die das Urheberrecht des Dokuments besitzt.
Ebenfalls ist die Nutzung dieser CP/CPS entgeltfrei, sofern Sie als mit geltende Vertragsunterlage für die Vertragsbeziehung zwischen dem jeweiligen Partner und Telekom Security dient.

9.1.5 Entgelterstattung

Die Erstattung von Entgelten durch Telekom Security erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts.

9.2 Finanzielle Verantwortlichkeiten

Die finanziellen Verantwortlichkeiten werden in den Allgemeinen Geschäftsbedingungen (AGB) für die Qualified.ID beschrieben, diese sind jederzeit verfügbar unter
https://www.telesec.de → Service → Downloads → Allgemeine Geschäftsbedingungen

9.2.1 Versicherungsschutz

Die Telekom Security verfügt über die Deutsche Telekom AG über einen Betriebs- und Vermögenshaftpflichtversicherungsschutz. Es ist sichergestellt, dass die Anforderungen, die sich hinsichtlich des Versicherungsschutzes ergeben, erfüllt werden. Darüber hinaus bestehet eine Deckungsvorsorge nach dem § 10 VDG.

9.2.2 Sonstige finanzielle Mittel

Nicht anwendbar.

9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

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 Telekom Security als Zertifizierungsstelle.
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 Schutz von personenbezogenen Daten (Datenschutz)

9.4.1 Datenschutzkonzept

Zur Leistungserbringung muss Telekom Security personenbezogene Daten elektronisch speichern und verarbeiten. Telekom Security 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 Zertifizierungsstelle 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 Gründe zur Offenlegung von Daten

Nicht anwendbar.

9.5 Rechte des geistigen Eigentums (Urheberrecht)

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

9.6 Zusicherungen und Gewährleistungen

9.7 Haftungsausschluss

Trotz größter Sorgfalt bei der Erstellung dieser Dokumentation können die Deutsche Telekom AG oder die Telekom Security 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 Deutsche Telekom Security GmbH jegliche Haftung ab.
Es gibt keinen gesetzlichen Anspruch auf die Ausstellung eines Zertifikates durch die Qualified.ID.

9.8 Haftungsbeschränkungen

Haftungsfragen sind in den Allgemeinen Geschäftsbedingungen (AGB) für die Qualified.ID geregelt, diese sind jederzeit unter der folgenden Adresse verfügbar
https://www.telesec.de → Service → Downloads → Allgemeine Geschäftsbedingungen

9.9 Schadenersatz

Schadensersatzansprüche sind in den Allgemeinen Geschäftsbedingungen (AGB) für die Qualified.ID geregelt, dies sind jederzeit unter der folgenden Adresse verfügbar
https://www.telesec.de → Service → Downloads → Allgemeine Geschäftsbedingungen

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Die Erstveröffentlichung dieses Dokuments „CP/CPS“ als auch dessen Änderungen treten mit der Veröffentlichung auf öffentlichen Webseiten der Telekom Security in Kraft.

9.10.2 Beendigung

Diese CP/CPS bleibt in der jeweils gültigen Version in Kraft, bis sie durch eine neue Version ersetzt wird.

9.10.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung des Dienstes Public Key Service bleiben alle Endteilnehmer-Zertifikaten an die in der CP/CPS enthaltenen Regelungen gebunden, bis das letzte ausgegebene Zertifikat ungültig oder gesperrt wird.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Falls nicht anders vertraglich vereinbart, werden für individuelle Mitteilungen und Kommunikation mit dem TSP Deutsche Telekom AG die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben.

9.12 Änderungen

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich die Telekom Security das Recht vor, Änderungen und Anpassungen dieses Dokuments durchzuführen.

9.12.1 Verfahren für Änderungen

Änderungen dieser CP/CPS können nur von Change Advisory Board des Herausgebers durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und Veröffentlichungsdatum.
Änderungen treten unverzüglich mit der Veröffentlichung in Kraft.

Aktualisierte Versionen dieses Dokuments setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet das Telekom Security Advisory Board über die weitere Vorgehensweise.

Innerhalb bestehender Verträge sind Änderungen dieser CP/CPS mindestens sechs Wochen vor Wirksamwerden schriftlich der beauftragten Drittpartei (Delegated Third Party) mitzuteilen. Bei Änderungen zu Ungunsten der

beauftragten Drittpartei (Delegated Third Party) steht diesem ein Sonderkündigungsrecht zum Zeitpunkt des Wirksamwerdens der Änderung zu. Erfolgt seitens der beauftragten Drittpartei (Delegated Third Party) innerhalb von sechs Wochen nach Zugang der Änderungsmitteilung keine schriftliche Kündigung, werden die Änderungen zum Zeitpunkt des Wirksamwerdens Vertragsbestandteil.

9.12.2 Benachrichtigungsverfahren und -zeitraum

Die Mandanten werden über die Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch ein zu legen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion wie unter Kapitel 9.12.1 in Kraft. Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.
Falls das Telekom Security Advisory Board der Ansicht ist, dass z.B. gravierende sicherheitsrelevante Änderungen unverzüglich erforderlich sind, dann tritt die neue CP/CPS unverzüglich mit der Freigabe (siehe Kapitel 9.12.1) in Kraft.

9.12.3 Gründe, unter denen die Objekt-Kennung (Objekt – ID) geändert werden muss

Telekom Security Advisory Board entscheidet darüber, ob Änderungen der Objekt-ID der CP/CPS notwendig werden. Andernfalls erfordern Änderungen keine Änderungen der Objekt-ID der Zertifizierungsrichtlinie.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei.

9.14 Geltendes 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.

9.15 Einhaltung geltenden Rechts

Das vorliegende Dokument unterliegt den geltenden deutschen Gesetzen, Vorschriften, Richtlinien, Verordnungen, Erlassen und Anordnungen, insbesondere den darin beschriebenen Import und Export Bestimmungen von Security-Komponenten (Software, Hardware oder technischer Informationen). Geltende zwingende Gesetze, Vorschriften, Richtlinien, Verordnungen, Erlasse und Anordnungen setzen die entsprechenden Bestimmungen der vorliegenden CP/CPS außer Kraft.

9.16 Verschiedene Bestimmungen

9.16.1 Vollständiger Vertrag

Nicht anwendbar.

9.16.2 Abtretung

Nicht anwendbar.

9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieser CP/CPS unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser CP/CPS im Übrigen nicht. Statt der unwirksamen und undurchführbaren Bestimmung gilt eine solche Bestimmung als vereinbart, die dem wirtschaftlichen Zweck dieses Dokuments in rechtswirksamer Weise am nächsten kommt. Das Gleiche gilt für die Ergänzung etwaiger Vertragslücken.

9.16.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Nicht anwendbar.

9.16.5 Höhere Gewalt

Es gelten die Regelungen des Einzelvertrags.

Innerhalb des gesetzlich zulässigen Rahmens müssen Verträge mit Partnern, Vertrauende Dritte oder Endteilnehmer Schutzklauseln über Höhere Gewalt enthalten, um Telekom Security schützen zu können.

Mit dieser Regelung soll sichergestellt werden, dass Telekom Security mit seinen Mandanten, Vertrauende Dritte oder Endteilnehmer vereinbart, dass Telekom Security nicht in Verzug gerät, wenn sich die Leistung infolge höherer Gewalt verzögert oder unmöglich wird.

9.17 Sonstige Bestimmungen

9.17.1 Andere Dokumente

Weitere Dokumente wie die AGB und die QUALIFIED.ID-Info sind über folgenden Link erhältlich:
https://www.telesec.de/de/signaturkarte/support/downloadbereich

9.17.2 Barrierefreiheit

Der Zugang zu den TC-Services erfolgt im Wesentlichen browserbasiert. Betriebssysteme bieten hier eine Vielzahl unterschiedlicher Barrierefreiheitsfeatures, um behinderten Personen den Zugriff auf die Web-Portale der Trust Center Services zu erleichtern. Diese kompensieren insbesondere Einschränkungen des Seh- und Hörvermögens, physischen Einschränkungen sowie Wahrnehmungsstörungen (z.B. „Informationen zur Barrierefreiheit für IT-Experten“).
Des Weiteren erfolgen Analysen mit den SW-Entwicklungspartnern des Trust Centers, ob es ergänzend zu diesen Standardboardmitteln weitere sinnvolle, betriebssystemunabhängige Möglichkeiten (z.B. mittels HTML5) zur Gestaltung der Barrierefreiheit gibt.
Sollten vorgenannte Maßnahmen nicht ausreichen, bietet Telekom Security darüber hinaus behinderten Menschen zur Unterstützung bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten kostenlosen telefonischen Support.

9.17.3 Beschwerden und Eskalationen

9.17.3.1 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.

9.17.3.2 Eskalation

Falls die Streitigkeit nicht innerhalb von zehn (10) Tagen nach der anfänglichen Mitteilung gemäß CPS § 9.17.3.1 beigelegt wird, kann eine Partei den Streitfall in schriftlicher oder elektronischer Form Telekom Security vorlegen und die Prüfung verlangen.

Daraufhin ruft Telekom Security 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.