Certification Practice Statement der D-TRUST CSM PKI

Version 1.2

Erscheinungsdatum	05.10.2015
Datum des Inkrafttretens	05.10.2015

BUNDESDRUCKEREI | D-TRUST EINE MARKE DER BUNDESDRUCKEREI

Vermerk zum Copyright

D-TRUST GMBH
Kommandantenstr. 15
10969 Berlin, Germany
Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	09.02.2015	▸ Initialversion
1.1	23.02.2015	▸ Editorische Änderungen im Rahmen der Erstzertifizierung gemäß ETSI 102 042 LCP. Es wurden diverse Inhalte aus der CP der D-TRUST GmbH in das CPS überführt.
1.2	05.10.2015	▸ Editorische Änderungen ▸ Konkretisierung der Möglichkeit das Schlüsselmaterial durch den TSP erzeugen und ausliefern zu lassen ▸ Sperrung nur noch über Online-Schnittstelle und wenn ein Sperrpass-wort vereinbart wurde telefonisch. ▸ Alle neuen Zertifikate werden immer im LDAP der D-TRUST veröffent-licht

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Certification Practice Statement (CPS) der von D-TRUST GMBH betriebenen D-TRUST CSM PKI.

1.1.1 Vertrauensdiensteanbieter

Diese Regelungen sind in der CP festgehalten.

1.1.2 Über dieses Dokument

Dieses CPS definiert Abläufe und Vorgehensweisen im Rahmen der Zertifizierungsdienste während der gesamten Lebensdauer der CA- und Endanwenderzertifikate (EE-Zertifikate). Es werden Mindestmaßnahmen konstatiert, die von allen PKI-Teilnehmern zu erfüllen sind.

Dieses CPS nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-TRUST GmbH und die ETSI Policy TS 102 042 als CP (Zertifikatsrichtlinie) und beschreibt die Umsetzung der daraus resultierenden Anforderungen.

Das gesamte CPS ist rechtsverbindlich, soweit dies im Rahmen der deutschen Gesetzgebung zulässig ist. Es enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit nicht ausdrücklich genannt, erfolgen auf Basis dieses CPS keine Zusicherungen oder Garantien im Rechtssinne.

Die Kenntnis der in dieser CPS beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatsnutzern Vertrauen in die Komponenten und PKI-Teilnehmer aufzubauen und Entscheidungen zu treffen, inwieweit das durch die PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

Die Struktur dieses Dokumentes ist eng an den Internet-Standard RFC 3647 *„Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“* angelehnt, um eine einfache Lesbarkeit und Vergleichbarkeit mit anderen CPSs zu erreichen.

1.1.3 Eigenschaften der PKI

Die Hierarchie der D-TRUST CSM PKI ist mehrstufig. Sie besteht immer aus einer Kette, die angeführt wird von einer Root-CA (Wurzelinstanz oder Vertrauensanker) und optional gefolgt von weiteren Sub-CAs (Intermediate CAs). Die letzte Sub-CA dieser Kette ist die „ausstellende CA“ (Issuing-CA). Von ihr werden EE-Zertifikate ausgestellt.

Die EE-Zertifikate lassen sich in ihrer Ausprägung den Anforderungen der einzelnen Richtlinien (Policy-Level) innerhalb der ETSI-Norm TS 102 042 zuordnen:

LCP – Leightweight Certificate Policy

NCP – Normalized Certificate Policy

OVCP – Organisation Validated Certificate Policy

EVCP – Extended Validation Certificate Policy

Derzeit werden entsprechende Policy-Level (z.B. EVCP+), die die Verwendung einer sicheren Signaturerstellungseinheit (SSEE) voraussetzen nicht angeboten. Dennoch steht es dem Zertifikatnehmer frei, eine SSEE für die Erzeugung und Aufbewahrung seiner privaten Schlüssel zu verwenden.

Soweit in diesem Dokument nicht zwischen den genannten Policy-Leveln unterschieden wird oder bestimmte Policy-Level explizit ausgeschlossen werden, sind die Anforderungen oder Bestimmungen der jeweiligen Abschnitte auf alle Policy-Level anwendbar.

EVCP
EE-Zertifikate des Policy-Levels EVCP sind entweder SSL- oder CodeSigning-Zertifikate.

OVCP
Zu den EE-Zertifikaten des Policy-Levels OVCP zählen SSL-Zertifikate und Maschinenzertifikate, die den Namen einer Organisation beinhalten.

NCP
EE-Zertifikate des Policy-Levels NCP sind Personenzertifikate, die besonders hochwertig sind und in vielen Bereichen den Anforderungen qualifizierter Zertifikate nach [SigG] entsprechen. Sie gelten aber nicht als qualifizierte Zertifikate (nach der Definition des [SigG]). Auch hier kann der Name einer Organisation als Attribut in das Zertifkat aufgenommen werden.
NCP-Zertifikate werden derzeit nicht angeboten. Daher wird im Folgenden auf die weitere Beschreibung verzichtet.

LCP
EE-Zertifikate des Policy-Levels LCP sind einfache Personenzertifikate, die hauptsächlich dazu verwendet werden E-Mails zu signieren und zu verschlüsseln. Auch hier kann der Name einer Organisation als Attribut in das Zertifkat aufgenommen werden.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname: Certification Practice Statement der D-TRUST CSM PKI

Version 1.2

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Die Zertifizierungsstellen (Certification Authority – CA) stellen Zertifikate sowie Sperrlisten aus. Möglich sind folgende Arten von Zertifikaten:

- Personenzertifikate für natürliche und juristische Personen (EE-Zertifikat),
- Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EE-Zertifikat),
- Maschinenzertifikate für IT-Prozesse und Kommunikationsverbindungen (SSL-Zertifikate / EE-Zertifikat)
- Zertifizierungsinstanzen (nachgeordnete CA-Zertifikate des TSP).

Die Wurzelinstanzen stellen Zertifikate ausschließlich mit der Erweiterung basic-Constraints: cA=TRUE (CA-Zertifikat) aus. Untergeordnete CAs stellen EE-Zertifikate und/oder weitere CA-Zertifikate aus. Die Zertifizierungsstelle ist in den ausgestellten Zertifikaten und CRLs namentlich im Feld issuer benannt.

LCP
Die ausstellende SubCA kann von der Root-CA eines Dritten cross-signiert werden. Sämtliche Festlegungen aus dieser CPS sind auch hier gültig.

1.3.2 Registrierungsstellen (RA)

Die RA identifiziert und authentifiziert Zertifikatnehmer (subscriber) oder Endanwender (subject), erfasst und prüft Anträge für verschiedene Zertifizierungsdienstleistungen.

Die konkreten Aufgaben und Pflichten, die die RA in Vertretung des TSP bzw. der CA übernimmt sind im jeweiligen Vertrag mit der RA definiert und verbindlich vereinbart. Die RA wird in diesem Rahmen eindeutig von der CA identifiziert.

Externe Registrierungsstellen werden derzeit nur für die Identifizierung im Rahmen des ETSI-Zertifizierungslevel LCP eingesetzt.

1.3.3 Zertifikatnehmer (ZNE) und Endanwender (EE)

Zertifikatnehmer (subscriber) sind natürliche oder juristische Personen, die EE-Zertifikate beantragen und inne haben. Der Zertifikatnehmer kann mit dem im Zertifikat genannten Endanwender (subject) identisch sein.

Endanwender (subject; End-Enity (EE)) verwenden die privaten Endanwender-schlüssel (EE-Schlüssel). Die Identität des Endanwenders ist mit dem Zertfikat und dem zugehörigen Schlüsselpaar verknüpft. Der Endanwender kann mit dem Zertifikatnehmer identisch sein. Zulässige Endanwender sind:

- natürliche Personen,
- Organisationen (juristische Personen – privatrechtliche und öffentlich-rechtliche, weitere staatliche Einrichtungen und Einzelunternehmen),
- Personengruppen,
- Funktionen, die durch Mitarbeiter einer Organisation ausgefüllt werden und
- IT-Prozesse (z. B. SSL-Server).

Die Verantwortung für Schlüssel und Zertifikat trägt der Zertifikatnehmer. Darüber hinaus ergeben sich nach [ETSI-F] weitere Pflichten. Spätestens zum Zeitpunkt der Antragstellung wird der Zertifikatnehmer über diese Pflichten durch die Bereitstellung dieses CPS und der Verpflichtungserklärung (subscriber agreement) informiert und muss sich zu deren Einhaltung verpflichten. Sind Zertifikatnehmer und Endanwender natürliche Personen, aber nicht identisch, muss der Zertifikatnehmer diese Pflichten dem Endanwender kenntlich machen.

Für SSL Zertifikate gilt die Verpflichtungserklärung für SSL Zertifikate. Für alle anderen Zertifikate unter dieser Policy gilt die CSM-Verpflichtungserklärung.

EVCP, OVCP
SSL-Zertifikate werden ausschließlich für juristische Personen ausgestellt.

LCP
LCP-Zertifikate, für natürliche Personen werden auch dann ausgestellt, wenn Zertifikatnehmer und Endanwender nicht identisch sind.

1.3.4 Zertifikatsnutzer (ZNU)

Zertifikatsnutzer (englisch relying parties) sind natürliche oder juristische Personen, die die Zertifikate dieser D-TRUST CSM PKI nutzen und Zugang zu den Diensten des TSP haben.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

CA-Zertifikate werden ausschließlich und in Übereinstimmung mit ihrer Erweiterung (BasicConstraints, PathLengthConstraint) für die Ausstellung von CA- oder EE-Zertifikaten und CRLs benutzt.

Die EE-Zertifikate dürfen für die Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

Zertifikatsnutzer handeln auf eigene Verantwortung. Es liegt in der Verantwortung des Zertifikatsnutzers, einzuschätzen, ob dieses CPS den Anforderungen einer Anwendung entspricht und ob die Benutzung des betreffenden Zertifikats zu einem bestimmten Zweck geeignet ist.

1.4.2 Verbotene Verwendungen von Zertifikaten

Andere Verwendungsarten als die im Zertifikat festgelegten, sind nicht zulässig.

1.5 Pflege des CPS

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird durch die D-TRUST GMBH gepflegt. Der ZDA-Leiter übernimmt die Abnahme des Dokuments.

Dieses CPS wird jährlich durch den TSP überprüft und ggf. aktualisiert. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

1.5.2 Ansprechpartner / Kontaktperson / Sekretariat

Diese Regelungen sind in der CP festgehalten.

1.5.3 Verträglichkeit von CPs fremder CAs mit diesem CPS

Sowohl in CA- als auch in EE-Zertifikaten können weitere CPs über Policy-OIDs referenziert werden, die dieser CPS nicht widersprechen. Die Referenz einer Policy-OID in den Zertifikatserweiterungen bestätigt seitens der CA die Kompatibilität der Zertfizierungspraktiken mit der referenzierten CP (z. B. NCP 0.4.0.2042.1.1 gemäß [ETSI-F]).

1.6 Begriffe und Abkürzungen

1.6.1 Deutsche Begriffe und Namen

Diese Regelungen sind in der CP festgehalten.

1.6.2 Englische Begriffe

Diese Regelungen sind in der CP festgehalten.

1.6.3 Abkürzungen

Diese Regelungen sind in der CP festgehalten.

1.6.4 Referenzen

Diese Regelungen sind in der CP festgehalten.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Diese Regelungen sind in der CP festgehalten.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen zur D-TRUST CSM PKI:

- EE-Zertifikate,
- CA-Zertifikate (Trust-Anchor),
- Sperrlisten (CRLs) und Statusinformationen,
- dieses CPS,
- die Verpflichtungserklärung für SSL-Zertifikate,
- die Verpflichtungserklärung für alle anderen Zertifikate unter dieser Policy,
- Cross-Zertifikate.

2.3 Häufigkeit von Veröffentlichungen

EE-Zertifikate werden immer in das öffentliche Verzeichnis des TSP aufgenommen. Veröffentlichte EE-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für ein weiteres Jahr und bis zum Jahresende abrufbar.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und:

- mindestens 5 Jahre (EVCP) und bis zum Jahresende bzw.
- mindestens 1 Jahr und bis zum Jahresende (OVCP, LCP)

nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig und bis zum Ende der Gültigkeit des ausstellenden CA-Zertifikats ausgestellt. Sperrlisten werden unmittelbar nach Sperrungen erstellt und veröffentlicht. Auch wenn keine Sperrungen erfolgen, stellt der TSP sicher, das mindestens alle 24 Std. eine neue Sperrliste ausgestellt wird. Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vorgehalten.

Dieses CPS wird – wie unter Abschnitt 2.1 genannt – veröffentlicht und bleibt dort mindestens so lange abrufbar, wie Zertifikate, die auf Basis dieses CPS ausgestellt wurden, gültig sind. Die Webseiten sind hochverfügbar.

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten und dieses CPS können öffentlich und unentgeltlich abgerufen werden. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

CA- und EE-Zertifikate enthalten grundsätzlich Angaben zu Aussteller (issuer) und Zertifikatnehmer bzw. Endanwender (subject). Diese Namen werden entsprechend dem Standard [X.501] als DistinguishedName vergeben.

Weitere alternative Namen können registriert und in die subjectAltName-Erweiterung der Zertifikate aufgenommen werden.

3.1.2 Notwendigkeit für aussagefähige Namen

Der verwendete DistinguishedName ist eindeutig innerhalb der D-TRUST CSM PKI.

Eine eindeutige Zuordnung des Zertifikats zum Zertifikatnehmer (bei Zertifikaten für natürliche Personen auch zum Endanwender) ist gegeben.

Bei alternativen Namen (subjectAltName) gibt es, mit Ausnahmen von SSL-Zertifikaten (einschließlich EV-Zertifikate), keine Notwendigkeit für aussagefähige Namen.

Diese Angaben dürfen keine Referenzen auf das Zertifikat selbst enthalten. IP-Adressen sind nicht zugelassen.

3.1.3 Anonymität oder Pseudonyme von Zertifikatnehmern

Pseudonyme werden ausschließlich für natürliche Personen benutzt. Generell werden Pseudonyme vom TSP vergeben.

Auch bei Zertifikaten, die mit Pseudonymen erstellt werden, wird durch den TSP oder die RA die reale Identität des Endanwenders (und ggf. des Zertifikatnehmers) in der Dokumentation festgehalten.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Attribute des *DistinguishedNames* (DN-Bestandteile) von EE-Zertifikaten werden wie folgt interpretiert:

DN-Bestandteil	Interpretation
G	*Vorname(n)* der natürlichen Person - EVCP, OVCP: Feld wird nicht verwendet - LCP: gemäß dem zur Identifizierung vorgelegten Dokument
SN	*Familienname* der natürlichen Person - EVCP, OVCP: Feld wird nicht verwendet - LCP: gemäß dem zur Identifizierung vorgelegten Dokument Bei der Verwendung von Pseudonymen entspricht der SN dem CN.
CN	*Gebräuchlicher Name:* Folgende Varianten werden verwendet: - Natürlichen Personen ohne Pseudonym: „Familienname, Rufname“. - Natürliche Personen mit Pseudonym: „Pseudonym:PN“. - Juristischen Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen. Sonderfall: ein oder mehrere Domainnamen können ebenfalls in den CN aufgenommen werden. Wildcards sind nicht zulässig bei EV-Zertifikaten. - Funktion oder Personengruppe: Name der Funktion oder Personengruppe mit dem vorangestellten Abkürzung „GRP:“ als Hinweis, dass es sich um ein Gruppenzertifikat handelt - Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.
PN	*Pseudonym*: ist identisch zu CN.
serialNumber	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Sonderfall bei EV-Zertifikate gemäß [GL-BRO]: Registernummer falls vergeben, Datum der Registrierung oder Gründung, oder eine textuelle Beschreibung, dass es sich um eine öffentlich-rechtliche Einrichtung handelt. Produktspezifisch kann das Feld anderweitig verwendet werden.
DNQ	DN Qualifier: Träger der *Seriennummer* in Zertifikaten, deren subject serialNumber-Feld anderweitig verwendet wird. Stellt die Eindeutigkeit des DN sicher (2.5.4.46 - id-at-dnQualifier) entsprechend [ETSI-F].

DN-Bestandteil	Interpretation
O	Offizielle Bezeichnung der *Organisation*, der der Zertifikatnehmer angehört oder damit sonst verbunden ist (Firma, Behörde, Verein etc.) entsprechend Existenznachweis, ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.
OU	*Organisationseinheit* (Abteilung, Bereich oder andere Unterteilung) der Organisation.
C	Das aufzuführende Land wird gemäß [ISO 3166] notiert und ergibt sich wie folgt: Ist eine Organisation O im Distinguished-Name aufge-führt, so bestimmt der Sitz der Organisation das Land C. Ist keine Organisation O eingetragen, so wird das Land aufgenommen, dass das Dokument ausgestellt hat, mit dem der Zertifikatnehmer identifiziert wurde.
Street	Postalische Adresse *Straße*
Locality	Postalische Adresse *Ort*
State	Postalische Adresse *(Bundes-)Land*
PostalCode	Postalische Adresse *Postleitzahl*
BusinessCategory	Business Category (2.5.4.15) gemäß [GL-BRO]
Jurisdiction Of Incorporation Locality	Gerichtsstand der Organisation gemäß [GL-BRO]: *Ort* (1.3.6.1.4.1.311.60.2.1.1)
Jurisdiction Of Incorporation State Or Province Name	Gerichtsstand der Organisation: *(Bundes-)Land* (1.3.6.1.4.1.311.60.2.1.2)
Jurisdiction Of Incorporation CountryName	Gerichtsstand der Organisation gemäß [GL-BRO]: *Land* (1.3.6.1.4.1.311.60.2.1.3)

Es müssen nicht alle genannten DN-Bestandteile verwendet werden. Weitere können ergänzt werden. Ergänzende DN-Bestandteile müssen [RFC 5280] und [Co PKI] entsprechen.

3.1.5 Eindeutigkeit von Namen

Der TSP stellt sicher, dass ein in EE-Zertifikaten verwendeter Name (DistinguishedName) des Zertifikatnehmers bzw. des Endanwenders (Feld subject) innerhalb der D TRUST CSM PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatnehmer bzw. Endanwender

zugeordnet ist. Die Eindeutigkeit wird mittels der Seriennummer bzw., wenn vorhanden, über den DN Qualifier (2.5.4.46 - id-at-dnQualifier) erzielt. Dadurch ist die eindeutige Identifizierung des Zertifikatnehmers anhand des im EE-Zertifikat verwendeten Namens (subject) gewährleistet.

Der TSP stellt die Eindeutigkeit von DistinguishedNames in CA-Zertifikaten sicher.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Der Zertifikatnehmer haftet für die Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten (siehe Abschnitt 9.5).

EVCP

Der TSP unternimmt notwendige Schritte um sicherzustellen, dass zum Zeitpunkt der Ausstellung des EV-Zertifikates, derjenige, der im Feld „Subject“ des Zertifikates benannt ist, das exklusive Nutzungsrecht an den im Zertifikat aufgeführten FQDN hat.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Es werden zwei Fälle unterschieden:

1) Schlüsselpaare von Zertifikatnehmern werden im Verantwortungsbereich des TSP produziert. Mit der Übergabe der Token oder Soft-PSE (LCP) und ggf. PIN-Briefe gemäß Abschnitt 4.4.1 an die Zertifikatnehmer durch den TSP wird sichergestellt, dass die privaten Schlüssel in den Besitz der Zertifikatnehmer gelangen.

2) Schlüsselpaare werden im Verantwortungsbereich des Zertifikatnehmers produziert. Der Besitz des privaten Schlüssels muss entweder technisch nachgewiesen werden oder vom Zertifikatnehmer nachvollziehbar bestätigt werden. Mit der Übersendung eines PKCS#10-Requests an den TSP bestätigt der Zertifikatnehmer verbindlich im Besitz des privaten Schlüssels zu sein.

3.2.2 Identifizierung und Authentifizierung von Organisationen

Organisationen, die entweder im Zertifikat genannt werden oder in deren Namen Zertifikate ausgestellt werden, müssen sich eindeutig authentisieren.

Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [ETSI-F] je nach Anwendbarkeit LCP, NCP, EVCP oder OVCP. Die Prüfung erfasst alle DN-Bestandteile.

EVCP
Für Identifizierung und Authentifizierung sowie Verifizierung von Antragsdaten gelten zusätzlich die Vorgaben aus [GL-BRO] (siehe CPS Annex A) sowie Abschnitt 12.2 [GL-BRO].

OVCP
Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [ETSI-F] in der Ausprägung OVCP.

LCP
Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [ETSI-F] in der Ausprägung LCP.

In den verschiedenen Zertifizierungsstufen werden die vorgestellten Prüfverfahren wie folgt auf die DN-Bestandteile nach Abschnitt 3.1.4 und ggf. weitere Attribute angewendet. Die in der folgenden Tabelle angegebenen Verfahren sind in Abschnitt 4.2.1 beschrieben.

	EVCP	**OVCP**
CN C O	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain
OU	Z-Bestätigung/ A-Bestätigung	Z-Bestätigung/ A-Bestätigung
STREET L State PostalCode	Register/ Non-Register	Register/ Non-Register
Alternativer Antragsteller (SAN)	Domain	Domain
Alle weiteren Attribute	Z-Bestätigung/ A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen/ Register/ Non-Register	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen

Wird der Antrag im Auftrag einer juristischen Person gestellt, muss der Vertreter (analog zu dem Verfahren für die Organisationszugehörigkeit aus Ab-

schnitt 3.2.3) seine diesbezügliche Berechtigung nachweisen und sich authentifizieren.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

Natürliche Personen, die Zertifikate beantragen, müssen sich eindeutig authentisieren und ggf. ihre Berechtigung zur Antragstellung durch die Organisation nachweisen.

LCP
Zertifikatnehmer die für andere natürliche Personen Zertifikate beantragen, müssen ihre Berechtigung zur Antragstellung nachweisen. Die Überprüfung der Daten bezieht sich auf den Zertifikatnehmer.

Die vorgestellten Prüfverfahren wie folgt auf die DN-Bestandteile nach Abschnitt 3.1.4 und ggf. weitere Attribute angewendet. Die angegebenen Verfahren sind in Abschnitt 4.2.1 beschrieben.

	LCP
G	HR-DB / Dok-Ident / Pers-Ident
SN	
CN	HR-DB / Register / Non-Register / Domain
C	
O	Register / Non-Register / Z-Bestätigung / A-Bestätigung/
OU	Z-Bestätigung / A-Bestätigung
STREET	Register / Non-Register
L	
State	
PostalCode	
Alternativer Antragsteller (SAN)	Domain / E-Mail-Adresse
Alle weiteren Attribute[1]	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen

[2] Sind auf dem Token zusätzlich zu den nicht-qualifizierten Zertifikaten der CSM PKI weitere Endnutzerzertifikate (qualifizierte oder qualifizierte mit Anbieterakkreditierung), ist gelten die in Aufbewahrungsfristen dieser Zertifikate.

Bei Antrag auf Zertifkate für Gruppen, Funktionen oder IT-Prozesse, werden alle in der Tabelle aufgeführten Attribute zum Endanwender (bis auf OU, E-Mail-Adresse, alle weiteren Attribute, wenn nicht zertifikatsrelevant) geprüft. Für die Aufnahme von Namen für Gruppen, Funktionen oder IT-Prozesse im CN gelten die Verfahren analog zu Zeile „Alle weiteren Attribute“.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatnehmer

Die Angaben des Zertifikatnehmers werden entsprechend den Abschnitten 3.2.2, 3.2.3 und 4.2.1 geprüft bzw. nicht geprüft. Bei alternativen Namen werden generell nur die E-Mail-Adressen geprüft. Andere Alternative Namen wie Adressen von Internetseiten und LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft (siehe hierzu auch Abschnitt 4.9.1).

Eine Ausnahme bilden hierbei SSL-Zertifikate nach EVCP, bei denen der Alternative Name für die Aufnahme weiterer URLs genutzt wird. In diesen Fällen werden auch dNSNames geprüft.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Bei natürlichen Personen werden Identitätsnachweis und ggf. die Organisationszugehörigkeit mittels der spezifischen Verfahren gemäß Abschnitt 3.2.3 ermittelt und geprüft bzw. bestätigt. Bei Organisationen wird der Existenznachweis sowie die Vertretungsberechtigung des Antragstellers spezifisch nach Abschnitt 3.2.2 geprüft bzw. bestätigt.

3.2.6 Kriterien für die Interoperabilität

Siehe Abschnitt 1.5.3.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)

Eine Schlüsselerneuerung ist gleichbedeutend mit der erneuten Produktion von Zertifikaten ggf. Token und Schlüsseln für denselben Endanwender. Schlüsselerneuerungen werden nur für OVCP- und LCP-Zertifikate, aber nicht für EV-Zertifikate angeboten. Bei EV-Zertifikate muss der gesamte Identifizierungs- und Registrierungsprozess wie bei einem Erstantrag durchlaufen werden, ggf. können aber bereits vorliegende Nachweisdokumente wiederverwendet werden, wenn sie nach Abschnitt 8.3.2 [GL-BRO] noch verwertbar sind.

3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

Für die Zeit nach Ablauf der Gültigkeit von EE-Zertifikaten oder auf Wunsch des Zertifikatnehmers werden auf Anforderung neue Zertifikate und ggf. Schlüssel und Token ausgegeben. Bei Anträgen zur Schlüsselerneuerung ist keine erneute Identifizierung erforderlich. Der Auftrag zur Schlüsselerneuerung muss signiert werden:

- elektronisch qualifiziert oder
- elektronisch mindestens gemäß der anwendbaren Klasse oder
- handschriftlich.

Abweichende Verfahren können kundenindividuell vereinbart werden. Die Bedingungen des Abschnitts 4.7 müssen erfüllt werden.

3.3.2 Schlüsselerneuerung nach Sperrungen

Schlüsselerneuerung auf Basis eines gesperrten Zertifikats wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Sperranträge eines Endanwenders sind grundsätzlich an den technischen Ansprechpartner der RA zu richten. Dieser löst dann einen Sperrauftrag beim TSP über die vereinbarte Online-Schnittstelle aus. Der technische Ansprechpartner muss sich zwingend gegenüber der Online-Schnittstelle des TSPs eindeutig authentifizieren.

Für den Fall, dass der technische Ansprechpartner, dem Endanwender das Sperrpasswort mitgeteilt hat, kann der Endanwender auch andere Sperrverfahren nutzen.

Die Sperrberechtigung wird wie folgt geprüft:

- Bei einem Sperrantrag, der in einer signierten E-Mail eingeht, muss der Sperrantragsteller entweder der Zertifikatnehmer selbst sein oder als Sperrberechtigter Dritter benannt worden sein, dessen Zertifikat dem TSP vorliegen muss.
- Bei telefonischem Sperrantrag oder einem Antrag per E-Mail ohne Signatur muss der Sperrberechtigte das entsprechende Sperrpasswort korrekt nennen.
- Sperranträge können nur dann über die Online-Schnittstelle eingereicht werden, wenn sich der Sperrantragsteller gegenüber der Schnittstelle eindeutig authentifizieren kann.

Andere Verfahren zur Authentifizierung von Sperranträgen können mit dem Zertifikatnehmer vereinbart werden.

Sperrverfahren werden in Abschnitt 4.9 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

Anträge dürfen von natürlichen Personen und juristischen Personen (deren autorisierten Vertretern) gestellt werden.

Teamzertifikate werden ausschließlich für juristische Personen und Einzelunternehmen ausgestellt.

Private EE-Schlüssel, die keine Signaturschlüssel oder kein Schlüssel zu EV-Zertifikaten sind, können gemäß den Vorgaben von 6.2.3 des CPS für eine spätere Wiederverwendung (key escrow, Wiederverwendung in einem neuen Token) vom TSP sicher hinterlegt werden, wenn der TSP dies anbietet. Der Zertifikatnehmer muss die Hinterlegung beantragen und angeben, dass der private EE-Schlüssel für denselben Zertifikatnehmer und/oder eine Personengruppe wiederverwendet werden soll. Für die Wiederverwendung der EE-Schlüssel nach 6.2.3 CPS muss der Zertifikatnehmer nachweisen, dass er berechtigt ist, diesen Schlüssel wieder zu verwenden.

EVCP
Zertifikatnehmer müssen den Anforderungen aus Abschnitt 7.2 [GL-BRO] entsprechen.

CA-Zertifikate werden ausschließlich an juristische Personen ausgegeben.

Der TSP ist berechtigt, Anträge abzulehnen (siehe Abschnitt 4.2.2).

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Einhaltung des Registrierungsprozesses gewährleistet der TSP. Die entsprechenden Aufgaben können von vertraglich gebundenen Partnern oder externen Anbietern übernommen, werden, die die Maßgaben von CP und CPS erfüllen.

EVCP
Dem Zertifikatnehmer liegen vor Beginn des Registrierungsprozesses CP und CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Zertifikatnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [ETSI-F]. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Zertifikatnehmers zur Veröffentlichung oder Nicht-Veröffentlichung der Zertifikate. Nachweise werden elektronisch oder papierbasiert hinterlegt. Die Verpflichtungserklä-

rung entspricht dem „Subscriber Agreement“ gemäß den Vorgaben aus Abschnitt 9.3 [GL-BRO].

LCP
Dem Zertifikatnehmer werden das CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) zur Verfügung gestellt, zu deren Einhaltung sich der Zertifikatnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [ETSI-F]. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Zertifikatnehmers zur Veröffentlichung oder Nicht-Veröffentlichung der Zertifikate.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Der beschriebene Identifizierungs- und Registrierungsprozess muss vollständig durchlaufen und alle nötigen Nachweise dabei erbracht werden.

Authentifizierung natürlicher Personen oder Organisationen sowie die Prüfung weiterer zertifikatsrelevanter Daten kann vor oder nach der Antragstellung erfolgen, muss aber vor Übergabe von Zertifikaten und ggf. Schlüsselmaterial sowie PINs abgeschlossen sein.

Natürliche Personen müssen eindeutig identifiziert werden, zum vollständigen Namen müssen Attribute wie Geburtsort, Geburtsdatum oder andere anwendbare individuelle Merkmale Verwechslungen verhindern. Werden juristische Personen im Zertifikat benannt, oder sind sie Zertifikatnehmer, müssen der vollständige Name und der rechtliche Status sowie ggf. relevante Registerinformationen geprüft werden.

Die Identifizierung findet gemäß Abschnitt 3.2.3 statt.

Der TSP definiert die folgenden Prüfverfahren:

Pers-Ident
Die natürliche Person muss sich gegenüber einer RA oder einem zugelassenem Partner oder einem externen Anbieter, der die Maßgaben des CPS erfüllt, anhand eines gültigen amtlichen Ausweises persönlich authentifizieren. Zulässige Dokumente sind Personalausweis oder Reisepass bei Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes, oder Dokumenten mit gleichwertiger Sicherheit. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Dok-Ident
Die nachzuweisenden Inhalte werden anhand von Kopien (Papierkopie, aber auch in elektronischer Form als gescanntes Dokument oder Fax) mit den Antragsdaten verglichen. Stichprobenartig werden Inhalte über einen telefonischen out-of-band-Mechanismus nachgefragt. Zulässige Dokumente sind die unter Pers-Ident geforderten, sowie Handelsregister- oder vergleichbare Auszüge, die nicht älter als ein halbes Jahr alt sind, Promotions-, Habilitations-, Ernennungsurkunden sowie Dokumente vergleichbaren Ranges. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Register
Es findet ein manueller oder automatisierter Abgleich (bzw. Erfassung) der Antragsdaten mit Kopien von Registerauszügen oder elektronischen Registern statt. Zulässig sind Register staatlicher Institutionen (Registergerichte, Bundeszentralamt für Steuern, berufsständischen Körperschaften öffentlichen Rechts oder vergleichbare) oder privatrechtliche Register (DUNS, vergleichbare Wirtschaftsdatenbanken, staatliche Institutionen des Privatrechts). Die Registereinträge werden nur dann als gültig akzeptiert, wenn Sie kein Attribut der Form "ungültig", "inaktiv" oder ähnliches enthalten. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Non-Register
Staatliche Einrichtungen/öffentlich-rechtliche Institutionen bestätigen zertifikatsrelevante Informationen mit Dienstsiegel und Unterschrift. Weiterhin können staatliche Organisationen mit Hilfe gesetzlicher Vorgaben authentisiert werden. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

HR-DB
Der TSP schließt vertragliche Vereinbarungen mit einer Organisation (Zertifikatnehmer) und vereinbart, dass nur valide Daten übermittelt werden, die die Vorgaben des CPS erfüllen. Ein autorisierter Mitarbeiter oder Funktionsträger einer Organisation übermittelt dem TSP über einen sicheren Kommunikationskanal Auszüge aus der Personaldatenbank (Human-Resource DB) der Organisation bzw. Requests, die auf Basis dieser Daten entstanden sind. Die anwendbaren Datenschutzanforderungen sind seitens der Organisation zu beachten. Der TSP vertraut auf die Richtigkeit und Eindeutigkeit der übermittelten Daten. Spätestens bei Übergabe der Token setzt der Zertifikatnehmer den Endanwender über dessen Pflichten aus der Verpflichtungserklärung und ggf. Sperrmöglichkeiten in Kenntnis. Es werden hinterlegt:

- elektronische oder papierbasierte Kopien der übermittelten Daten,
- die Bestätigung/der Nachweis des Übermittelnden als "autorisierten Mitarbeiter" bzw. "autorisierten Funktionsträger",

- der Nachweis, dass diese Daten von einem autorisierten Mitarbeiter zur Verarbeitung bereitgestellt wurden und der Nachweis, dass Zertifikatnehmer in die Verpflichtungserklärung eingewilligt hat.

Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Z-Bestätigung
Ein Zeichnungsberechtigter der Organisation bestätigt zertifikatsrelevante Informationen. Dies geschieht schriftlich, in Einzelfällen können elektronisch signierte Bestätigungen akzeptiert werden. Die Zeichnungsberechtigung muss entweder aus dem Existenznachweis für die Organisation ersichtlich sein oder anderweitig nachgewiesen werden. Der Zeichnungsberechtigte kann schriftlich einen Vertreter benennen (siehe A-Bestätigung). Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

A-Bestätigung
Autorisierte Mitarbeiter oder Funktionsträger innerhalb einer Organisation oder vertrauenswürdige Dritte (z. B. Partner des TSP oder staatliche Institutionen) bestätigen bestimmte zertifikatsrelevante Informationen, die in ihrer Bestätigungskompetenz liegen. Dies geschieht schriftlich, in Einzelfällen können elektronisch signierte Bestätigungen akzeptiert werden. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

out-of-band-Mechanismen
Der TSP nutzt out-of-band-Mechanismen um die Korrektheit von Antragsdaten zu prüfen, dabei werden Kommunikationswege und Prüfverfahren gewählt, die der Zertifikatnehmer nicht beeinflussen kann. Die Nachweise werden elektronisch oder papierbasiert dokumentiert und hinterlegt.

Der Existenznachweis von Organisationen oder natürlichen Personen gegenüber dem TSP kann beispielsweise mittels Banküberweisung, Lastschrift- oder Kreditkarteneinzug erfolgen. Der TSP vertraut der Bank, die die Organisation bzw. die natürliche Person als Kunden führt. Zulässig ist auch eine telefonische Nachfrage über ein öffentliches Telefonverzeichnis seitens des TSP.

Zur Identifizierung natürlicher Personen kann eine postalische Sendung mittels "Einschreiben mit Rückschein" vom TSP an den Zertifikatnehmer versendet werden, die Unterschrift auf dem Rückschein wird mit der Unterschrift auf der Passkopie oder den Antragsunterlagen verglichen.

Die Organisationszugehörigkeit des Endanwenders kann ebenfalls mittels Testpost per "Einschreiben mit Rückschein" an die Organisation zu Händen des Endanwenders nachgewiesen werden. Die Unterschrift des Einschreibens wird mit der Unterschrift auf der Passkopie oder den Antragsunterlagen verglichen. Organisationszugehörigkeit, E-Mail-Adresse, Inhalte von Extensions, sowie alle weite-

ren zertifikatsrelevanten Daten können auch mittels telefonischer Nachfrage über ein öffentliches Telefonverzeichnis seitens des TSP bestätigt werden.

Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Körperschaften
Der TSP schließt vertragliche Vereinbarungen mit Körperschaften des öffentlichen Rechts und vereinbart, dass nur Daten übermittelt werden, die die Vorgaben des CPS erfüllen. Ein autorisierter Mitarbeiter oder Funktionsträger dieser Körperschaft des öffentlichen Rechts übermittelt dem TSP über einen sicheren Kommunikationskanal Personendaten bzw. Antragsformulare, die auf Basis dieser Daten entstanden sind. Die anwendbaren Datenschutzanforderungen sind seitens der Körperschaft zu beachten. Ferner gelten die gleichen Verfahren entsprechend HR-DB. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Domain
Die Domain einer Organisation wird durch eine Domain-Abfrage in offiziellen Registern (WHOIS) geprüft.

OVCP, LCP
Es wird hinterfragt, ob der Zertifikatnehmer über das Nutzungsrecht der Domain verfügt.

EVCP
Bei EV-Zertifikaten wird zusätzlich eine Überprüfung des Domainnamens gegen bekannte Phishing Domains über Blacklists durchgeführt. Nicht registrierungspflichtige Domainnamen (keine Top-Level-Domain) sind nicht zulässig.

Die Ergebnisse der Abfrage werden hinterlegt.

E-Mail
Die Domain, die in einer eingetragenen E-Mail-Adresse verwendet wird, muss der eingetragenen Organsiation eindeutig zuzuordnen sein.

Ist dies nicht der Fall, schickt der TSP an die zu bestätigende E-Mail-Adresse eine E-Mail, deren Empfang bestätigt werden muss (Geheimnisaustausch). Die Ergebnisse der Abfrage werden hinterlegt.

Identifizierung und Authentifizierung finden gemäß den Abschnitten 3.2.2 und 3.2.3 statt.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Treten bei der Prüfung der Identität durch die RA oder den TSP oder der Prüfung auf Korrektheit der Daten im Zertifikatsantrag oder den Ausweis- und Nachweisdokumenten Unstimmigkeiten auf, die nicht restlos ausgeräumt werden können, wird der Antrag abgelehnt.

Weitere Gründe für die Antragsablehnung können sein:

- Verdacht auf die Verletzung der Namensrechte Dritter,
- Nichteinhalten von Fristen für den Nachweis der Daten,
- Zahlungsrückstände des Antragstellers gegenüber dem TSP oder
- Umstände, die den Verdacht begründen, dass eine Zertifikatsausstellung den Betreiber der CA in Misskredit bringt.

Der TSP ist berechtigt, Zertifikatsanträge auch ohne die Angabe von Gründen abzulehnen.

Erhält der TSP PKCS#10- oder andere Zertifikats-Requests, werden deren Inhalte durch den TSP auf Korrektheit überprüft. Diese Überprüfung entfällt für den TSP, wenn vertragliche Vereinbarungen mit Partnern bestehen, bei denen beauftragte, unabhängige Personen die Requests dem TSP zur Produktion zur Verfügung stellen. Bestimmte Zertifikatsinhalte (z.B. O oder OU) können inhaltlich vertraglich festgelegt werden.

Erhält der TSP vorab Zertifikatsdaten über eine mandantenfähige Onlineschnittstelle, kann eine Vorabprüfung der Zertifikatsdaten erfolgen. Wird dann die eigentliche Zertifikatsanforderung nach der Prüfung durch den TSP übermittelt, kann eine Sofortausstellung von Zertifikaten erfolgen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

entfällt

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen des TSP bei der Ausstellung von Zertifikaten

Im Hochsicherheitsbereich des Trustcenters werden die entsprechenden Zertifikate ausgefertigt.

Dabei wird sichergestellt, dass bei der Zertifikatserstellung die korrekte Zeit verwendet wird.

Die vollständige Antragsdokumentation wird entweder vom TSP gemäß Abschnitt 5.5 revisionssicher abgelegt oder der TSP schließt vertragliche Vereinba-

rungen mit Partnern, dass die Antragsunterlagen und/oder Requests sicher und vollständig bis zum Ablauf der Frist nach Abschnitt 5.5.2 zu verwahren sind.

4.3.2 Benachrichtigung des Zertifikatnehmers über die Ausstellung des Zertifikats

Es erfolgt keine gesonderte Benachrichtigung des Zertifikatnehmers nach der Fertigstellung des Zertifikats.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Soft-PSEs, deren privater Schlüssel im Bereich des TSP erstellt wurde, werden je nach Wunsch des Zertifikatnehmers auf einem Speichermedium (mit der Post an die im Antrag benannte Adresse) versandt, zum zugriffsgeschützen und SSL-verschlüsselten Download bzw. SSL-geschützter Schnittstelle (CSM) bereitgestellt oder per E-Mail gesendet (die PKCS#12-Datei ist mit einer PIN geschützt).

Wird ein Zertifikat zu einem beim Zertifikatnehmer vorhandenen Schlüsselpaar ausgestellt, wird das Zertifikat entweder zum Download bereitgestellt (z. B. im-Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

Kundenspezifisch können abweichende Verfahren vereinbart werden.

Entdeckt der Zertifikatnehmer Fehler in seinen Zertifikaten oder bei der Funktion der Schlüssel und Token, so hat er dies dem TSP mitzuteilen. Die Zertifikate werden gesperrt.

Fehlerhafte Angaben in den Zertifikaten gelten nur insoweit als vertraglicher Mangel im Sinne des Gesetzes, soweit der TSP nach diesem CPS eine Überprüfung der von dem Fehler betroffenen Angaben vornimmt. Im Übrigen gelten im Falle von Fehlern und deren Bestehen die entsprechenden Nacherfüllungsregeln der jeweils gültigen [AGB].

Eine Abnahme durch den Kunden erfolgt nicht, es handelt sich um eine Dienstleistung, nicht um eine Werkleistung.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

Die Zertifikate werden nach der Produktion grundsätzlich in den öffentlichen Verzeichnisdienst eingestellt.

Der Status ist in beiden Fällen nach Produktion über OCSP abrufbar (siehe Abschnitt 2.1).

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Sperrberechtigte Dritte nach Abschnitt 4.9.2 werden schriftlich benachrichtigt und erhalten das Sperrpasswort, sofern nichts anderes mit der Organisation oder dem Sperrberechtigten Dritten vereinbart wurde.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer

Zertifikatnehmer und Endanwender dürfen ihre privaten Schlüssel ausschließlich für die Anwendungen nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

Für Zertifikatnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Zertifikate der D-TRUST CSM PKI können von allen Zertifikatsnutzern verwendet werden. Es kann jedoch nur dann darauf vertraut werden, wenn

- die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Extentions) benutzt werden,
- die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt werden kann,
- der Status der Zertifikate über den Statusabfragedienst (OCSP) positiv geprüft wurde und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifische Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

Hinweis: Im Gegensatz zu qualifizierten Signaturen gilt für nicht qualifizierte Signaturen vor Gericht nicht die Beweislastumkehr, d. h. die Gültigkeit der Signatur muss mittels Gutachten bewiesen werden.

4.6 Zertifikatserneuerung (certificate renewal)

Eine Zertifikatserneuerung ist die erneute Ausstellung eines Zertifikats, das auf den Inhaltsdaten und Schlüsseln des ursprünglichen Zertifikats beruht. Für die

erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle CP und CPS.

Bei CA-Schlüsseln wird generell keine Zertifikatserneuerung durchgeführt.

Bei LCP-Zertifikaten werden Zertifikatserneuerungen in individueller Abstimmung mit dem Kunden vereinbart.

4.6.1 Bedingungen für eine Zertifikatserneuerung

Haben sich grundsätzliche Änderungen an den Nutzungsbedingungen ergeben, wird der Zertifikatnehmer darüber informiert. Der Zertifikatnehmer bestätigt die neuen Bedingungen.

Bei einem Antrag auf Zertifikatserneuerung kann – im Gegensatz zu einem neuen Antrag auf ein Zertifikat – der Vorgang der initialen Identifizierung entfallen.

Voraussetzung ist, dass das Zertifikat für denselben Endanwender ausgestellt wird. Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Zertifikatserneuerung noch gültig sein.

LCP

Im Rahmen von Verträgen kann ein Nachladeverfahren implementiert werden, bei dem der Antrag durch Beauftragte erfolgt und der Zertifikatsnehmer im Nachladeverfahren persönlich durch Eingabe der PIN der Aufbringung des neuen Zertifikates auf seiner Karte und ggf. neuen Nutzungsbedingungen zustimmt.

Die zu rezertifizierenden Schlüssel und der kryptographische Algorithmus müssen den Mindestanforderungen des zum Zeitpunkt der Antragstellung gültigen CPS entsprechen, siehe Abschnitte 3.2.1, 6.1.1 CPS und 6.1.5 CPS und dürfen nicht kompromittiert sein.

4.6.2 Berechtigung zur Zertifikatserneuerung

Jeder Zertifikatnehmer, der (nach Abschnitt 4.1.1) berechtigt ist, einen erneuten Zertifikatsantrag zu stellen, kann eine Zertifikatserneuerung beantragen, wenn die Bedingungen nach Abschnitt 4.6.1 erfüllt sind und der TSP ein entsprechendes Verfahren für das gewählte Produkt anbietet.

4.6.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Zertifikatnehmer, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, nutzen eine produktspezifisch bereitgestellte Onlineschnittstelle des TSP zur Antragstellung.

Über die entsprechenden Schnittstellen gestellte Anträge werden automatisiert auf Berechtigung und Inhalt geprüft.

4.6.4 Benachrichtigung des Zertifikatnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die in Abschnitt 4.3.2 festgelegten Regelungen.

4.6.5 Verhalten bei der Ausgabe einer Zertifikatserneuerung

Das erzeugte Zertifikat wird über die bereitgestellte Online-Schnittstelle zur Verfügung gestellt. Weiterhin gelten die in Abschnitt 4.4.1 festgelegten anwendbaren Regelungen.

PINs werden im Zuge der Zertifikatserneuerung nicht verändert.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch den TSP

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen, je nach Angaben im Erstantrag. Der Zertifikatnehmer kann seine Entscheidung zur Veröffentlichung ändern.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Eine Zertifikatserneuerung mit Schlüsselerneuerung ist die erneute Ausstellung eines Zertifikats, das auf den Inhaltsdaten des ursprünglichen Zertifikats beruht, für das aber neue Schlüssel verwendet werden.

Für die erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle CP und CPS.

Bei CA-Schlüsseln kann eine Schlüsselerneuerung durchgeführt werden, sofern diese nicht gesperrt sind.

EVCP
Für EV-Zertifikate gelten die Vorgaben aus Abschnitt 11.14 [GL-BRO].

4.7.1 Bedingungen für Zertifikate mit Schlüsselerneuerung

Bei einem Antrag auf die Schlüsselerneuerung kann – im Gegensatz zu einem neuen Antrag auf Zertifikate – der Vorgang der initialen Identifizierung entfallen.

Voraussetzung ist, dass das Zertifikat für denselben Endanwender ausgestellt wird.

Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Schlüsselerneuerung noch gültig sein.

Zertifikatnehmer müssen ggf. entsprechend der Vorgaben aus Abschnitt 3.2.1 nachweisen, dass sie im Besitz des privaten Schlüssels sind, wenn der Schlüssel nicht durch den TSP erzeugt wurde.

Die Zertifikatnehmer müssen bestätigen, dass sich die Zertifikatsinhalte nicht verändert haben. Wurde die Organisationszugehörigkeit widerrufen, muss sie ggf. erneut nachgewiesen werden, andernfalls wird die Organisation nicht wieder ins Zertifikat auf genommen.

Haben sich grundsätzliche Änderungen an den Nutzungsbedingungen ergeben, wird der Zertifikatnehmer darüber informiert. Der Zertifikatnehmer muss die neuen Bedingungen bestätigen.

Das Schlüsselmaterial und der kryptographische Algorithmus müssen den Mindestanforderungen des zum Zeitpunkt der Antragstellung gültigen CPS entsprechen, siehe Abschnitte 3.2.1, 6.1.1 und 6.1.5 und dürfen nicht kompromittiert sein.

4.7.2 Berechtigung zur Schlüsselerneuerung

Jeder Zertifikatnehmer, der (nach Abschnitt 4.1.1) berechtigt ist, einen erneuten Zertifikatsantrag zu stellen, kann eine Zertifikatserneuerung beantragen, wenn die Bedingungen nach Abschnitt 4.7.1 erfüllt sind und der TSP ein entsprechendes Verfahren für das gewählte Produkt anbietet.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Zertifikatnehmer, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, nutzen eine produktspezifisch bereitgestellte Onlineschnittstelle des TSP zur Antragstellung.

Über die entsprechenden Schnittstellen gestellte Anträge werden automatisiert auf Berechtigung und Inhalt geprüft.

4.7.4 Benachrichtigung des Zertifikatnehmers über die Ausgabe eines Nachfolgezertifikats

Zertifikatnehmer, die berechtigt sind, Anträge auf Schlüsselerneuerungen zu stellen, nutzen eine produktspezifisch bereitgestellte Onlineschnittstelle des TSP zur Antragstellung.

4.7.5 Verhalten für die Ausgabe von Zertifikaten nach Schlüsselerneuerungen

Es gelten die in Abschnitt 4.3.2 festgelegten Regelungen.

4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen durch den TSP

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Die Verfahren des TSP erfüllen die Bedingungen aus [ETSI-F] und [GL-BRO].

Zertifikatnehmer oder betroffenen Dritte sind aufgefordert, die Sperrung zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden oder Inhaltsdaten des Zertifikats nicht mehr korrekt sind (z. B. der Wegfall der Zugehörigkeit des Zertifikatnehmers zu einer Organisation).

Die Sperrung eines Zertifikats wird bei folgenden Ereignissen durchgeführt:

- auf Verlangen des Zertifikatnehmers bzw. betroffenen Dritten (z.B. die im Zertifikat genannte Organisation),
- Ungültigkeit von Angaben im Zertifikat,
- wenn der TSP seine Tätigkeit beendet und diese nicht von einem anderen TSP fortgeführt wird,
- nur bei Code-Signing Zertifikaten:
  - wenn dem TSP bekannt wird, dass das Zertifikat an einen Herausgeber von Schadsoftware ausgegeben wurde oder
  - wenn dem TSP bekannt wird, dass das Zertifikat, wenn es nicht gesperrt wird, den Vertrauensstatus schädigen würde.

Unabhängig davon kann der TSP Sperrungen veranlassen, wenn:

- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- Schwächen im verwendeten Kryptoalgorithmus bekannt werden, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eingesetzte Hard- und Software Sicherheitsmängel aufweist, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eindeutige Zuordnung des Schlüsselpaars zum Zertifikatnehmer nicht mehr gegeben ist,
- ein Zertifikat aufgrund falscher Angaben erwirkt wurde,
- der Kunde nach zweimaliger Mahnung mit dem Entgelt in Verzug ist,
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde.

EVCP

[GL-BRO] sieht für EV-Zertifikate zwingende Sperrgründe vor (Annex A).

Der TSP hält den Betrieb einer EV-Reportingstelle gemäß Abschnitt 11.3 [GL-BRO] vor. PKI-Teilnehmer oder Software-Hersteller können dort an 24 Stunden am Tag und 7 Tagen der Woche Beschwerden mitteilen, Verdacht über die Kompromittierung privater Schlüssel von EV-Zertifikaten äußern, den Missbrauch von EV-Zertifikaten melden, Betrug, regelwidriges Verhalten von EV-Zertifikaten melden.
Innerhalb von 24 Stunden beginnt der TSP mit der Bearbeitung der Vorfälle gemäß Abschnitt 11.3.2 [GL-BRO], was die Sperrung der betroffenen EV-Zertifikate auslösen kann.
Missbrauchsverdacht von D-Trust-EV-Zertifikaten kann unter der E-Mail-Adresse:
ev-support@d-trust.net gemeldet werden.

Sperrungen enthalten eine Angabe des Zeitpunkts der Sperrung und werden nicht rückwirkend erstellt. Weiterhin kann eine Sperrung nicht rückgängig gemacht werden.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zur Sperrung

Der TSP ist sperrberechtigt. Der TSP muss gemäß [GL-BRO] Abschnitt 11.2.2 bzw. 11.3.3 sperren.

Der Zertifikatnehmer hat stets die Berechtigung zur Sperrung seiner Zertifikate. Es können Vereinbarungen getroffen werden, in denen der Zertifikatnehmer auf dieses Recht verzichtet.

Enthält ein Zertifikat Angaben über die Vertretungsmacht des Zertifikatnehmers für eine dritte Person, so kann auch die dritte Person eine Sperrung des betreffenden Zertifikates verlangen. Die für sonstige Angaben zur Person (z.B. die Angabe „Steuerberater“) zuständige Stelle (z.B. zuständige Kammer) kann ebenfalls eine Sperrung des betreffenden Zertifikates verlangen, wenn die Voraussetzungen für die Angaben zur Person nach Aufnahme in das Zertifikat entfallen. Zusätzliche Sperrberechtigte Dritte können benannt werden und haben dann stets die Berechtigung zur Sperrung dieser Zertifikate.

Im Übrigen gilt jede Person als sperrberechtigt gegenüber dem TSP, soweit sie das zutreffende Sperrpasswort mitteilt.

4.9.3 Verfahren für einen Sperrantrag

Sperrungen können grundsätzlich über die vereinbarte Online-Schnittstelle durch den Zertifikatnehmer bzw. seinen autorisierten Vertreter durchgeführt werden.

Sperranträge eines Endanwenders sind grundsätzlich an den technischen Ansprechpartner der RA zu richten. Dieser löst dann einen Sperrauftrag beim TSP über die vereinbarte Online-Schnittstelle aus. Der technische Ansprechpartner der RA muss sich zwingend gegenüber der Online-Schnittstelle des TSPs eindeutig authentifizieren.

Soweit ein Sperrpasswort vereinbart wurde, können Sperranträge telefonisch an bundeseinheitlichen Arbeitstagen in der Zeit von 9 - 17 Uhr gestellt werden.

Sperrnummer: +49 (0)30 / 25 93 91 - 602

OVCP, EVCP
Sperrberechtigte können telefonisch sperren, an 24 Stunden am Tag und 7 Tagen der Woche und müssen sich mit ihrem vereinbarten Sperrpasswort authentifizieren.
Sperrnummer: +49 (0)30 / 25 93 91 – 601

Andere Sperrverfahren können vereinbart werden.

Ein Antrag per E-Mail zur Sperrung eines Zertifikats muss eindeutig das zu sperrende Zertifikat beschreiben und muss daher folgende Angaben enthalten:

- Name des Sperrantragstellers,
- Name des Zertifikatnehmers,

- Zertifikatsseriennummer (wenn möglich als Dezimalzahl), damit das Zertifikat eindeutig identifiziert werden kann.

Sperrungen finden im Verantwortungsbereich des TSP statt. Ungeachtet dessen kann der TSP Teilaufgaben an vertraglich gebundene Dritte weiter geben. Die Sperrdienstleistung kann von Dritten übernommen werden, die nach den Maßgaben des TSP handeln. Der TSP stellt geeignete Soft- und Hardware sowie Verfahrensanweisungen zur Verfügung.

Die Verfahrensanweisungen beinhalten strikte Vorgaben für die Erfüllung der Sperrdienstleistung und beschreiben detailliert Abläufe und Verhaltensvorgaben im Fehlerfall.

Die vom Sperrantragsteller angegebenen Sperrgründe werden dokumentiert. Nach erfolgter Sperrung wird der Zertifikatnehmer bzw. der Endanwender über die Sperrung informiert. Die Information des Endanwenders kann durch den Zertifikatnehmer erfolgen, wenn dies vereinbart wurde.

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

4.9.4 Fristen für einen Sperrantrag

Der Endanwender oder Zertifikatnehmer muss in eigener Verantwortung dafür sorgen, dass er oder eine für ihn sperrberechtigte Person unverzüglich die Sperrung beantragt, sobald Gründe zur Sperrung bekannt werden. Dabei ist dasjenige Verfahren zu nutzen, welches die schnellste Bearbeitung des Sperrantrags erwarten lässt.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Sperranträge werden vom TSP an bundeseinheitlichen Arbeitstagen in der Zeit von 9 - 17 Uhr bearbeitet. Telefonisch eintreffende Sperranträge werden unmittelbar ausgeführt. Per E-Mail und per Briefpost eintreffende Sperranträge werden spätestens am folgenden Arbeitstag bearbeitet.

EVCP
Die Sperrung erfolgt umgehend nach erfolgreicher Autorisierung des Sperrantragstellers per Telefon.

LCP
Ein Sperrverlangen wird innerhalb von 72h umgesetzt.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten vorgehalten, die über das Protokoll LDAP oder über den in Abschnitt 2.1 angegebenen Link abgerufen werden

können. Zusätzlich steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieser Dienste wird in Form von URLs in den Zertifikaten angegeben. Ferner können Sperrinformationen über die Webseite des TSP (siehe Abschnitt 2.1) bezogen werden. Delta-CRLs werden nicht genutzt.

Integrität und Authentizität der Sperrinformationen wird durch eine Signatur der CRL bzw. der OCSP-Antwort gewährleistet.

Sperreinträge in Sperrlisten verbleiben mindestens bis zum Ablauf der Zertifikatsgültigkeit enthalten.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Siehe Abschnitt 2.3.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden unmittelbar nach ihrer Erzeugung veröffentlicht.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

Zur Onlineprüfung steht ein OSCP-Dienst zur Verfügung. Die Erreichbarkeit dieses Dienstes wird in Form eines URL in den Zertifikaten angegeben.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Es gibt keine Pflicht zur Online-Prüfung von Sperrinformationen, es gilt jedoch Abschnitt 4.5.2.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine.

4.9.13 Bedingungen für eine Suspendierung

Suspendierungen von Zertifikaten werden nicht angeboten.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

Der Statusabfragedienst ist über das Protokoll OCSP verfügbar. Die Erreichbarkeit des Dienstes wird als URL in den Zertifikaten angegeben.

Die Formate und Protokolle der Dienste sind in den Abschnitten 7.2 und 7.3 beschrieben.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst ist permanent (24 Stunden an 7 Tagen der Woche) verfügbar.

4.10.3 Optionale Leistungen

Keine.

4.11 Austritt aus dem Zertifizierungsdienst

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Termin. Schlüsselerneuerung kann gemäß Abschnitt 3.3.1 beantragt werden. Der Sperrauftrag zu einem Zertifikat durch Zertifikatnehmer oder Sperrberechtigte Dritte löst die Sperrung durch den TSP aus. Die vertraglichen Hauptleistungspflichten des TSP sind damit vollständig erfüllt.

4.12 Schlüsselhinterlegung und –wiederherstellung

Schlüsselhinterlegung wird nicht vom TSP angeboten. Dem *subscriber* steht es frei, Schlüssel im eigenen Verantwortungsbereich zu hinterlegen.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Schlüsselhinterlegung wird nicht vom TSP angeboten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Schlüsselhinterlegung wird nicht vom TSP angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die CAs, die bei der D-TRUST GMBH im Rahmen von [ETSI-F] betrieben werden.

5.1 Bauliche Sicherheitsmaßnahmen

Die D-TRUST GMBH ist akkreditierter Zertifizierungsdiensteanbieter nach deutschem Signaturgesetz. Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor (Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters [SiKo-DTR]), die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle geprüft. Die Prüfung und Bestätigung wird nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen wiederholt.

Teil des Sicherheitskonzepts ist eine detaillierte Dokumentation der baulichen Sicherheits- und Überwachungsmaßnahmen, die im Einzelfall und bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Ferner wurde dem Sicherheitsbereich des Trustcenters der D-TRUST GMBH durch den TÜV-IT die Anwendung und Umsetzung der „Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3“ beurkundet (gemäß Prüfkriterienkatalog für „Trusted Site Infrastructure“). Mit diesem TÜV-IT-Zertifikat „Trusted Site Infrastructure“ werden alle Infrastruktur-relevanten Aspekte untersucht und bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Die genannten Zertifikate bestätigen der D-TRUST GMBH diesen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

Die CAs der hier behandelten CSM-PKI werden vom TSP unter den gleichen Bedingungen betrieben wie die CAs der D-TRUST GMBH zur Ausstellung qualifizierter Zertifikate mit Anbieterakkreditierung nach deutschem Signaturgesetz.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Teil des Sicherheitskonzeptes ist ein Rollenkonzept, in dem Mitarbeiter einer oder mehreren Rollen zugeordnet werden und entsprechende Berechtigungen durch einen gesteuerten Prozess erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zuordnung der Berechtigungen wird regelmäßig durch das Sicherheitsmanagement revisioniert und umgehend nach Entfall des Bedarfs entzogen.

Mitarbeiter, die im Bereich der Zertifizierungs- und Sperrdienste tätig sind, agieren unabhängig und sind frei von kommerziellen/finanziellen Zwängen, die ihre Entscheidungen und Handlungen beeinflussen könnten. Die organisatorische Struktur des TSP berücksichtigt und unterstützt die Mitarbeiter in der Unabhängigkeit ihrer Entscheidungen.

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft. Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit. Schulungen und Leistungsnachweise werden dokumentiert. Der TSP erfüllt somit die Forderungen aus Abschnitt 12.1 [GL-BRO].

5.2.2 Mehraugenprinzip

Besonders sicherheitskritische Vorgänge müssen mindestens im Vier-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen durchgesetzt.

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen, durchgesetzt. Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

5.2.4 Rollenausschlüsse

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, die verhindern, dass eine Person allein ein Zertifikat ausstellen und in den Verzeichnisdienst einstellen kann.

5.3 Eingesetztes Personal

Der TSP erfüllt die Anforderungen an das Personal aus dem [SigG] und [SigV] und beschreibt sie im Sicherheitskonzept [SiKo-DTR].

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Der TSP gewährleistet, dass die im Bereich des Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen.

5.3.2 Sicherheitsprüfungen

Der TSP erfüllt die Anforderungen gemäß § 5 (5) SigG und beschreibt sie in seinem Sicherheitskonzept [SiKo-DTR]. So müssen unter anderem regelmäßig Führungszeugnisse vorgelegt werden.

5.3.3 Schulungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind zu Beginn ihres Einsatzes und bei Bedarf.

5.3.5 Häufigkeit und Folge von Job-Rotation

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult. Rollenwechsel finden unter Berücksichtigung des Sicherheitskonzeptes [SiKo-DTR] statt (Zugriffsrecht, Zugriffskontrolle).

5.3.6 Maßnahmen bei unerlaubten Handlungen

Der TSP schließt unzuverlässige Mitarbeiter von den Tätigkeiten im Zertifizierungsdienst aus.

5.3.7 Anforderungen an freie Mitarbeiter

Entfällt; freie Mitarbeiter werden nicht eingesetzt.

5.3.8 Ausgehändigte Dokumentation

Umfangreiche Verfahrensanweisungen definieren für alle Produktionsschritte die zuständigen Mitarbeiterrollen und -rechte sowie entsprechende manuelle und maschinelle Prüfungen. Durch die sicherheitstechnische Infrastruktur der D-TRUST ist gewährleistet, dass von diesen definierten Verfahren im Produktionsbetrieb nicht abgewichen werden kann.

5.4 Überwachungsmaßnahmen

Der TSP betreibt umfangreiche Überwachungsmaßnahmen (beispielsweise durch Videoüberwachung) zur Absicherung der Zertifizierungsdienstleistungen und deren zugrunde liegenden IT-Systemen und Dokumenten. Diese Maßnahmen sind im Sicherheitskonzept [SiKo-DTR] beschrieben.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besu-

cher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen und während ihres Besuchs die Personaldokumente abgeben. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des TSP sein.

Ein weiterer Bestandteil des Sicherheitskonzepts ist eine Risikoanalyse, die Bedrohung für den Betrieb des TSP umfassend analysiert sowie Anforderungen und Gegenmaßnahmen definiert. Ferner ist eine Restrisikoanalyse enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt wird.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden.

Archiviert werden die vollständigen Antragsunterlagen (auch Folgeanträge), Dokumente zu Verfahrensrichtlinien (CP, CPS), Zertifikate, Sperrdokumentation, elektronische Dateien und Protokolle zum Zertifikatslebenszyklus. Dabei werden die Vorgänge zeitlich erfasst.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Dokumente zur Antragstellung und Prüfung sowie die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden mindestens fünf Jahre und bis zum Jahresende aufbewahrt[2]. Für alle SSL Zertifikate einschließlich EV Zertifikate gilt eine Frist von sieben Jahren. Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

5.5.3 Sicherung des Archivs

Das Archiv befindet sich in gesicherten Räumen und unterliegt dem Rollen- und Zutrittskontrollkonzept des TSP.

5.5.4 Datensicherung des Archivs

Vertraulichkeit und Integrität der Daten werden gewahrt. Die Dokumentation erfolgt unverzüglich, so dass sie nachträglich nicht unbemerkt verändert werden kann. Die Bundesdeutschen Datenschutzanforderungen werden eingehalten.

[2] Sind auf dem Token zusätzlich zu den nicht-qualifizierten Zertifikaten der CSM PKI weitere Endnutzerzertifikate (qualifizierte oder qualifizierte mit Anbieterakkreditierung), ist gelten die in Aufbewahrungsfristen dieser Zertifikate.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Der TSP betreibt einen Zeitstempeldienst gemäß [SigG].

5.5.6 Archivierung (intern / extern)

Die Archivierung erfolgt intern beim TSP, sowie extern in gleichwertig gesicherten Räumen.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Das Verfahren zur Beschaffung und Verifikation von Archivinformationen unterliegt dem Rollenkonzept des TSP.

5.6 Schlüsselwechsel beim TSP

Eine angemessene Zeit vor Ablauf einer CA werden neue CA-Schlüssel generiert, neue CA-Instanzen aufgesetzt und veröffentlicht.

5.7 Kompromittierung und Geschäftsweiterführung beim TSP

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Der TSP verfügt über ein Notfallkonzept sowie einen Wiederanlaufplan, die den beteiligten Rollen bekannt sind und von ihnen im Bedarfsfall umgesetzt werden. Die Verantwortlichkeiten sind klar verteilt und bekannt.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren.

5.7.3 Kompromittierung des privaten CA-Schlüssels

Im Fall einer Kompromittierung oder der Bekanntgabe von Unsicherheit von Algorithmen oder assoziierten Parametern durch die Herausgeber der maßgeblichen Kataloge nach Abschnitt 6.1.6, veranlasst der TSP folgendes:

- betroffenen CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden gesperrt,
- involvierte Zertifikatnehmer werden über den Vorfall und dessen Auswirkungen informiert,
- der Vorfall wird auf den Webseiten des TSP veröffentlicht mit dem Hinweis, dass Zertifikate, die von dieser CA ausgestellt wurden, ihre Gültigkeit verlieren.

Aus der Analyse der Gründe für die Kompromittierung werden, wenn möglich, Maßnahmen ergriffen, um zukünftige Kompromittierungen zu vermeiden. Unter Berücksichtigung der Gründe für die Kompromittierung werden neue CA-Signaturschlüssel generiert und neue CA-Zertifikate ausgestellt.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach Kompromittierung und Desaster

In einem Notfall entscheidet der TSP je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 6.2.4 beschriebene Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 5.7.3 verfahren wird.

5.8 Schließung des TSP

Bei Beendigung der Dienste von CAs informiert der TSP alle Zertifikatnehmer und beendet alle Zugriffsmöglichkeiten von Unterauftragnehmern des TSP in Bezug auf die betroffenen CAs. Alle noch gültigen und von den betroffenen CAs ausgestellten Zertifikate werden gesperrt. Betroffene private CA-Schlüssel werden zerstört.

Der Verzeichnisdienst und Dokumente zur Antragstellung werden an die Bundesdruckerei GmbH übergeben und unter equivalenten Bedingungen weitergeführt. Die Aufrechterhaltung des Verzeichnisdienstes wird bis Ablauf der EE-Zertifikatsgültigkeit zugesichert und entweder einem anderen TSP oder der Bundesdruckerei GmbH übergeben.

Der TSP verfügt über einen entsprechenden „Letter of Comfort“, für die Übernahme der Kosten für die Erfüllung dieser Mindestanforderungen für den Fall, dass die Zertifizierungsstelle zahlungsunfähig wird oder aus anderen Gründen die Kosten nicht selbst decken kann.

Mit Beendigung des Betriebes wird alle Funktionalität der CAs eingestellt, so dass eine Zertifizierung nicht mehr möglich ist.

6. Technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die CAs, die bei der D-TRUST GMBH im Rahmen von [ETSI-F] betrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

An dieser Stelle wird zwischen Schlüsselpaaren für die

- CA-Zertifikate und
- Endanwenderzertifikate (EE-Zertifikate)

unterschieden.

6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel werden in einem „FIPS 140-2 Level 3“ konformen Hardware Security Module (HSM) erzeugt. Das HSM befindet sich im Hochsicherheitsbereich des Trustcenters. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip erzwungen. Bei der Erzeugung von CA-Schlüsseln ist stets ein unabhängiger Auditor anwesend oder der Auditor kann sich nach der Schlüsselerzeugung durch eine Videoaufzeichnung vom ordnungsgemäßen Ablauf der Schlüsselerzeugung überzeugen.

EE-Schlüssel werden vom Zertifikatnehmer kryptographisch sicher erzeugt, entsprechen den Vorgaben von CP, CPS und entstehen im Rahmen einer sichereren Einsatzumgebung auf Basis von vertrauenswürdigen kryptographischen Anwendungen oder im Falle der Schlüsselgenerierung durch den TSP mit der Hilfe eines HSMs. Weiterhin wird durch entsprechende Maßnahmen eine Verfälschung der Informationen verhindert.

6.1.2 Lieferung privater Schlüssel an Zertifikatnehmer

Werden die privaten Schlüssel beim TSP erzeugt, werden sie gemäß Abschnitt 4.4.1 zugestellt. In diesem Fall erfolgt die Speicherung der privaten Schlüssel beim TSP bis zur Auslieferung in einer sicheren Umgebungen.

Da keine Schlüsselhinterlegung angeboten wird, wird der private Schlüssel nach der Auslieferung an den Zertifikatnehmer beim TSP gelöscht.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

CA-Schlüsselpaare werden im Trustcenter erzeugt.

Die EE-Schlüsselpaare, die im Verantwortungsbereich des TSP erzeugt werden, liegen dem TSP vor. Zertifikatsanforderungen können von Zertifikatnehmern zu einem vorhandenem Schlüsselpaar per PKCS#10-Request gestellt werden, der mit dem entsprechenden privaten Schlüssel signiert werden muss. Der PKCS#10-Request enthält den öffentlichen Schlüssel. Die entsprechende PKCS#10-Response gibt das vollständige Zertifikat zurück.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Der öffentliche Schlüssel der CA ist im CA-Zertifikat enthalten. Dieses Zertifikat befindet sich i. d. R. auf dem Token, das dem Zertifikatnehmer übergeben wird. Darüber hinaus können die CA-Zertifikate aus dem öffentlichen Verzeichnis (siehe Abschnitt 2.1) bezogen werden, in dem sie nach ihrer Erstellung veröffentlicht werden.

6.1.5 Schlüssellängen

Für CA-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit verwendet.

Für EE-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit verwendet.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

EVCP, OVCP , LCP
: CA- und EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG] in der aktuell gültigen Fassung entsprechen, soweit Kompatibilität im Verwendungsumfeld gewährleistet ist.

EVCP
: CA- und EE-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die [ETSI-F] und [GL-BRO] in der aktuell gültigen Fassung entsprechen.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 7.1.3 genannt.

6.1.7 Schlüsselverwendungen

Private Root-CA-Schlüssel werden ausschließlich zum Signieren von CA-Zertifikaten verwendet. Alle anderen privaten CA-Schlüssel werden zum Signieren von CA-Zertifikaten, EE-Zertifikaten und Sperrlisten benutzt (siehe Abschnitt 7.1.2).

Die EE-Schlüssel dürfen nur für die im Zertifikat benannten Nutzungsarten verwendet werden. Die Nutzungsarten werden in den Feldern *KeyUsage* und *Ext-*

KeyUsage im Zertifikat definiert und ggf. durch weitere Extentions eingeschränkt (siehe Abschnitt 7.1.2).

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die vom TSP eingesetzten kryptographischen Module funktionieren einwandfrei. Während des gesamten Lebenszyklus (einschließlich Lieferung und Lagerung) werden die Module durch technische und organisatorische Maßnahmen vor unbefugter Manipulation geschützt.

Zur Sicherung der CA-Schlüssel wird ein HSM eingesetzt, das entsprechend FIPS 140-2 Level 3 evaluiert wurde.

Der TSP betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren um die Qualität der EE-Schlüssel zu sichern. Werden die privaten EE-Schlüssel im Verantwortungsbereich des Zertifikatnehmers erstellt, so hat dieser ebenfalls dafür zu sorgen, dass eine ausreichende Qualität bei der Schlüsselerzeugung gewährleistet ist.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Der HSM, auf dem die CA-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die Aktivierung des privaten Schlüssels erfordert zwei autorisierte Personen. Nach der Aktivierung kann der HSM beliebig viele Zertifikate signieren.

Ein Zugriff auf private EE-Schlüssel besteht nur im Fall von Schlüsselhinterlegung gemäß Abschnitt 6.2.3.

6.2.3 Hinterlegung privater Schlüssel (key escrow)

Private CA- und EE-Schlüssel werden vom TSP nicht hinterlegt.

6.2.4 Backup privater Schlüssel

Es ist ein Backup der privaten CA-Schlüssel vorhanden. Ein CA-Schlüssel-Backup erfordert zwei für diese Tätigkeit am HSM autorisierte Personen und findet in der sicheren Umgebung des Trustcenters statt. Für das Backupsystem gelten die gleichen Voraussetzungen und Sicherungsmaßnahmen wie für das Produktivsystem. Eine Wiederherstellung privater Schlüssel erfordert ebenfalls zwei autorisierte Personen. Weitere Kopien der privaten CA-Schlüssel existieren nicht.

Für private EE-Schlüssel wird kein Backup angeboten, eine Sicherung erfolgt nur im Rahmen der Hinterlegung (key escrow), wenn diese vereinbart wurde.

6.2.5 Archivierung privater Schlüssel

Private CA- und EE-Schlüssel werden nicht archiviert.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Ein Transfer privater CA-Schlüssel in oder aus dem HSM erfolgt nur zu Backup- und Wiederherstellungszwecken. Ein 4-Augen-Prinzip wird erzwungen. Bei Export/Import in ein anderes HSM schützt eine Verschlüsselung den privaten CA-Schlüssel.

Ein Transfer privater EE-Schlüssel aus dem kryptographischen Modul kann erfolgen, wenn der Zertifikatnehmer nachweist, dass er nach Abschnitt 4.12.1 berechtig ist, den Schlüssel wiederzuverwenden und der Transfer technisch möglich ist. Der Schlüssel verlässt das Modul nie im Klartext.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten CA-Schlüssel liegen verschlüsselt im HSM vor.

EE-Schlüssel liegen bis zur Auslieferung verschlüsselt in einer Datenbank des CA-Systems vor.

6.2.8 Aktivierung privater Schlüssel

Die privaten CA-Schlüssel können nur im 4-Augen-Prinzip und von den zuständigen Rollen und für die zulässigen Nutzungsarten (*keyCertSign, cRLSign*) aktiviert werden.

Private EE-Schlüssel werden durch Eingabe der PIN aktiviert.

6.2.9 Deaktivieren privater Schlüssel

Die privaten CA-Schlüssel werden durch Beendigung der Verbindung zwischen HSM und Anwendung deaktiviert.

Die jeweilige Anwendung deaktiviert den privaten EE-Schlüssel, spätestens aber durch das Deaktivieren oder Löschen des Soft-PSEs.

6.2.10 Zerstörung privater Schlüssel

Nach Ablauf der Gültigkeit der privaten CA-Schlüssel werden diese gelöscht. Dies erfolgt durch Löschen auf dem HSM und gleichzeitigem Löschen der auf Daten-

trägern angelegten Backups. Bei Stilllegung des HSMs werden die privaten Schlüssel auf dem Gerät gelöscht.

Werden die Dateien, die den privaten EE-Schlüssel enthalten, gelöscht, so ist der private Schlüssel zerstört.

Schlüssel, die im Bereich des TSPs erstellt wurden, werden nach Auslieferung automatisch gelöscht.

6.2.11 Beurteilung kryptographischer Module

Der TSP betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren um die Qualität der EE-Schlüssel zu sichern. Die eingesetzten HSM sind FIPS 140-2 Level 3 konform.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche CA- und EE-Schlüssel werden gemäß Sicherheitskonzept in Form der erstellten Zertifikate archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer der CA-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt 30 Jahre.

Die Gültigkeitsdauer der EE-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt

OVCP
61 Monate (SSL-Zertifikate maximal 39 Monate),

EVCP
27 Monate,

LCP
60 Monate

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die Aktivierungsdaten der CA-Schlüssel werden durch das HSM abgefragt. PIN-Vergabe erfolgt während der Bootstrap-Prozedur. Ein 4-Augen-Prinzip wird erzwungen.

Zertifikatnehmer: Wird das Schlüsselpaar vom Zertifikatnehmer erzeugt, wird das Aktivierungsgeheimis bei diesem Verfahren ebenfalls produziert und steht dem Zertifikatnehmer unmittelbar zur Verfügung. Erzeugt der TSP die Schlüssel, wird entweder ein Transport-PIN-Verfahren genutzt oder die PINs werden in einen PIN-Brief gedruckt und an den Zertifikatnehmer versandt oder übergeben. Eine Installation ist nicht erforderlich.

6.4.2 Schutz von Aktivierungsdaten

Die Aktivierungsdaten der CA-Schlüssel setzen sich aus zwei Geheimnissen zusammen, von denen jeweils ein berechtigter Mitarbeiter eines kennt. Der Zugriff auf die Aktivierungsdaten ist nur bestimmten vorgesehenen Mitarbeitern möglich.

Zertifikatnehmer: Die PINs werden durch ein Transport-PIN-Varfahren ausgeliefert oder einmalig in einen besonders gesicherten PIN-Brief gedruckt und an den Zertifikatnehmer versandt oder übergeben.

6.4.3 Andere Aspekte von Aktivierungsdaten

Nicht anwendbar.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom TSP eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die nicht im Widerspruch zum CPS und [ETSI-F] und im Fall von EV-Zertifikaten zu [GL-BRO] stehen.

Die Computersicherheit des TSP wird für exponierte Systeme u.a. durch mehrstufige Sicherheitssysteme zum Zwecke des perimetrischen Virenschutzes, Endpoint-Protection und integritätssichernde Werkzeuge sichergestellt.

Zertifikatnehmer und Zertifikatsnutzer müssen vertrauenswürdige Computer und Software verwenden.

6.5.2 Beurteilung von Computersicherheit

Die für die CA-Schlüssel eingesetzten Computer, Netze und andere Komponenten wurden durch anerkannte Prüf- und Bestätigungsstellen regelmäßig geprüft.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Bei der Entwicklung aller vom TSP oder im Auftrag des TSP durchgeführter Systementwicklungsprojekte werden Sicherheitsanforderungen im Entwurfsstadium analysiert. Die gewonnenen Erkenntnisse werden als Anforderungen bei der Entwicklung festgelegt.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich entsprechend dem Rollenkonzept (des Sicherheitskonzepts des signaturgesetzkonformen TSPs D-TRUST GMBH) autorisiertes Personal darf Computer, Netze und andere Komponenten administrieren. Es findet eine regelmäßige Auswertung von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle statt. Überwachungsmaßnahmen beginnen mit Inbetriebnahme eines Gerätes und enden mit dessen Entsorgung.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

Eingesetzte Geräte werden gemäß Herstellerangaben betrieben. Vor Inbetriebnahme werden sie eingehend geprüft und kommen nur zum Einsatz, wenn zweifelsfrei feststeht, dass sie nicht manipuliert wurden. Durch Versiegelung der Hardware und Softwarechecks beispielsweise werden Manipulationen und Manipulationsversuche bei jeder Aktion oder Revision erkennbar. Bei Verdacht auf Manipulation einer Komponente, wird eine ggf. geplante Aktion an der Komponente nicht durchgeführt und der Vorfall dem TSP-Leiter gemeldet. Um kurzfristig und koordiniert auf eventuelle sicherheitsrelevante Vorfälle reagieren zu können, definiert der TSP klare Eskalationsrichtlinien für die einzelnen Rollen.

Kapazitätsanforderungen und -auslastungen sowie Eignung der beteiligten Systeme werden überwacht und bei Bedarf angeglichen. Ausgetauschte Geräte oder obsolete Datenträger werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Änderungen an Systemen, Software oder Prozessen durchlaufen einen Change-Management-Prozess. Sicherheitskritische Änderungen werden durch den Sicherheitsbeauftragten geprüft. Nach Ablauf der Gültigkeit von CAs werden die privaten Schlüssel vernichtet.

Elektronische Daten oder papiergebundene Protokolle dokumentieren alle relvanten Ereignisse, die den Life-Cycle der CA sowie der ausgestellten Zertifikate und generierten Schlüssel beeinflussen und werden auf langlebigen Medien revisionssicher gespeichert. Die Medien des Unternehmens werden entsprechend ihrer Kassifizierung im Rahmen der Dokumentationsrichtlinie des TSP zuverlässig vor Schaden, Entwendung, Verlust oder Kompromittierung geschützt.

EVCP
Es werden mindesten die unter 13.1 [GL-BRO] geforderten Ereignisse auditierbar geloggt bzw. protokolliert.

6.7 Sicherheitsmaßnahmen für Netze

Im Betrieb der CAs wird ein Netzkonzept realisiert. Für das Netzkonzept liegt eine detaillierte Dokumentation vor (Sicherheitskonzept des signaturgesetzkonformen TSPs D-TRUST GMBH – Netzwerkkonzept [Siko-DTR]), die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Zum Schutz der Prozesse des TSP werden beispielsweise Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt. Der TSP betreibt Netzsegmente unterschiedlichen Schutzbedarfs und trennt dabei Mitarbeiter- und Internet-nahe Netze sorgfältig von Servernetzwerken. Die Systeme unterliegen regelmäßigen Revisionen, die Verantwortlichen sind berichtspflichtig. Auffälligkeiten werden durch technische Systeme und organisatorische Prozesse gemeldet und in einem definierten Incidentverfahren und daran ansetzenden Prozessen behandelt.

Datenverkehr mit hohem Schutzbedarf außerhalb der durch den TSP geschützten Netzwerke, für den Integrität oder Vertraulichkeit sichergestellt werden muss, wird durch kryptographische Mechanismen geschützt.

Die physische Sicherheit der durch den TSP betriebenen und genutzten Netze ist sichergestellt und wird den baulichen Gegebenheiten und ihren Veränderungen angepasst.

Das Sicherheitskonzept wurde durch die von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle TÜV Informationstechnik GmbH geprüft.

6.8 Zeitstempel

Der TSP betreibt einen Zeitstempeldienst gemäß [SigG]. Zeitstempel werden im Rahmen dieses CPS jedoch nicht angeboten.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Es werden Zertifikate im Format X.509v3 ausgegeben.

7.1.2 Zertifikatserweiterungen

Die Wahl der Erweiterung ist weitestgehend produktabhängig.

CA-Zertifikate enthalten folgende *kritische* Erweiterungen („Pflichtfeld“):

Erweiterung	OID	Parameter
KeyUsage	2.5.29.15	*keyCertSign, cRLSign*
BasicConstraints	2.5.29.19	*Ca=TRUE, (pathLenConstraint)*

CA-Zertifikate können folgende *unkritische* Erweiterungen enthalten („optional“):

Erweiterung	OID	Parameter
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
CRLDistributionPoints	2.5.29.31	Adresse der CRL-Ausgabestelle
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation*
certificatePolicies	2.5.29.32	OID zu unterstützten CPs
SubjectAltName	2.5.29.17	Alternativer Ausstellername

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

EE-Zertifikate enthalten folgende *kritische* Erweiterungen:

Erweiterung	OID	Parameter
KeyUsage	2.5.29.15	Möglich sind: *digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly* und Kombinationen

EE-Zertifikate können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
ExtKeyUsage	2.5.29.37	Entsprechend [RFC 5280]
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
CRLDistributionPoints	2.5.29.31	CRL-Ausgabestelle als ldap-Adresse
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation* *accessMethod= Certification Authority Issuer {1.3.6.1.5.5.7.48.2}, accessLocation*
certificatePolicies	2.5.29.32	OID zu unterstützten CPs *cpsURI*
SubjectAltName	2.5.29.17	Alternativer Ausstellername

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.3 Algorithmen-OIDs

In den CA- und EE-Zertifikaten wird derzeit folgender der Verschlüsselungsalgorithmus verwendet:

- RSA mit OID 1.2.840.113549.1.1.1.

Folgende Signaturalgorithmen werden in CA- und EE-Zertifikate derzeit verwendet:

- SHA256 RSA mit OID 1.2.840.113549.1.1.11.

7.1.4 Namensformate

In den Feldern *subject* (hier: Name des Endanwenders) und *issuer* (Name des Ausstellers) werden Namen nach [X.501] als DistinguishedName vergeben. Es können die Attribute aus Abschnitt 3.1.4 vergeben werden. Die Kodierung erfolgt als UTF8-String bzw. PrintableString für das Attribut C (Country).

In den Feldern *SubjectAltName* (Alternativer Zertifikatnehmername) und *IssuerAltName* (Alternativer Ausstellername) können Namen gemäß [RFC 5280] (kodiert als IA5String) stehen.

7.1.5 Name Constraints

„NameConstraints“ wird nicht benutzt.

7.1.6 Certificate Policy Object Identifier

„CertificatePolicies“ kann den OID unterstützter CPs enthalten.

Zertifikate können den OID der in [ETSI-F] definierten NCP, NCP+ bzw. OVCP enthalten. Unabhängig davon können weitere CPs referenziert werden. Dieses CPS entspricht den Vorgaben von [ETSI-F].

EVCP
EV-Zertifikate können den OID der in [ETSI-F] definierten EVCP enthalten. Unabhängig davon können weitere CPs referenziert werden.

7.1.7 Nutzung der Erweiterung „PolicyConstraints“

„PolicyConstraints“ wird nicht benutzt.

7.1.8 Syntax und Semantik von „PolicyQualifiers“

„PolicyQualifier“ können benutzt werden.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung CertificatePolicies

In CA- und EE-Zertifikaten ist die Erweiterung *CertificatePolicies* (Zertifikatsrichtlinie) nicht kritisch. Es liegt im Ermessen der Zertifikatnehmer und Zertifikatsnutzer, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Es werden Sperrlisten v2 gemäß [RFC 5280] erstellt. Delta-CRLs sind nicht vorgesehen.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Sperrlisten der können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
cRLNumber	2.5.29.20	Nummer der Sperrliste
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellerschlüssels

7.3 Profile des Statusabfragedienstes (OCSP)

7.3.1 Versionsnummer(n)

Es wird OCSP v1 gemäß [RFC 2560] eingesetzt.

7.3.2 OCSP-Erweiterungen

Der OCSP-Responder unterstützt bei Anfragen die im Folgenden angegebene Erweiterung (Extension):

Erweiterung	Parameter
RetrieveIfAllowed	Falls gesetzt, wird Zertifikat in der Antwort mitgeliefert (optional).

Der OCSP-Responder verwendet in den Antworten die im Folgenden angegebenen Erweiterungen (Extensions):

Erweiterung	Parameter
ArchiveCutoff	Zeitraum, für den der OCSP-Responder nach Ausstellung des Zertifikats die Statusinformationen bereitstellt.
CertHash	Bei Status good oder revoked wird der SHA-1 Hash-Wert des Zertifikats eingetragen.
CertInDirSince	Zeitpunkt der Veröffentlichung des Zertifikats im zentralen Verzeichnisdienst.
RequestedCertificate	Enthält das Zertifikat, falls *RetrieveIfAllowed* gesetzt war.

Alle Erweiterungen sind nicht kritisch. Weitere unkritische Erweiterungen können enthalten sein.

8. Überprüfungen und andere Bewertungen

Die CAs der D-TRUST CSM PKI werden vom TSP in den gleichen Räumen betrieben wie die CA der D TRUST GmbH zur Ausstellung qualifizierter Zertifikate mit Anbieterakkreditierung nach deutschem Signaturgesetz. Revisionen, Revisionsgegenstände und Prozesse sind detailliert im Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D TRUST GmbH [SiKo-DTR] beschrieben. Der Teil Rollenkonzept desselben Sicherheitskonzepts [SiKo-DTR] dokumentiert die Qualifikation und die Stellung des Revisors.

Das Sicherheitskonzept wird regelmäßig durch eine unabhängige Prüf- und Bestätigungsstelle geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

TSPBereiche, die aufgrund gesetzlicher oder technischer Unterschiede nicht analog zum qualifizierten Betrieb mit Anbieterakkreditierung abgebildet werden (z. B. der Betrieb eines eigenen Root-Zertifikates), werden regelmäßig mindestens einmal im Jahr durch die interne Revision überprüft.

CP und CPS erfüllen für Zertifikate die Anforderungen von NCP, NCP+ bzw. OVCP und für EV-Zertifikate die Anforderungen gemäß [ETSI-F] einschließlich der Anforderungen aus [BRG] und [NetSec-CAB]. Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten („competent independent party“ gemäß TS 102 042 [ETSI-F], Abschnitt 5.4.1) belegt die Kompatibilität.

Der TSP gibt Zertifikate mit der Policy-OID-Referenz auf [ETSI-F] erst nach der initialen und erfolgreich abgeschlossenen Prüfung nach [ETSI-F] durch einen unabhängigen externen und lizenzierten Zertifizierer aus. Es finden regelmäßige Wiederholungsprüfungen statt. Sollten sich die Verfahren hernach als nicht mehr konform zu den aktuellen Richtlinien von [ETSI-F] erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde.

EVCP

Der TSP gibt EV-Zertifikate nur dann aus, wenn entsprechend [ETSI-F] EVCP eine Zertifizierung erfolgt ist. Sollten sich die Verfahren hernach als nicht mehr konform zu den aktuellen Richtlinien von [GL-BRO] erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinien-konformität wiederhergestellt und entsprechend überprüft wurde. Diese Auditierung findet jährlich statt.

Darüber hinaus finden regelmäßig interne Audits statt.

9. Sonstige finanzielle und rechtliche Regelungen

Bezüglich der entsprechenden Regelungen wird auf Kapitel 9 in der CP sowie ergänzend die [AGB] verwiesen.

Annex A Sperrgründe bei EV-Zertifikaten

Auszug aus den aktuellen Guidelines for Extended Validation Certificates, CA/Browser Forum.

11.2 [GL-BRO]Revocation Events *The CA MUST revoke an EV Certificate it has issued upon the occurrence of any of the following events:*

The Subscriber requests revocation of its EV Certificate;

The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;

The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;

The CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;

The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;

The CA receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;

A determination, in the CA's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CA's EV Policies;

The CA determines that any of the information appearing in the EV Certificate is not accurate.

The CA ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;

The CA's right to issue EV Certificates under these Guidelines expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;

The Private Key of the CA's Root Certificate used for issuing that EV Certificate is suspected to have been compromised;

Such additional revocation events as the CA publishes in its EV Policies; or

The CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in Section 23 of these Guidelines.