Certification Practice Statement der D-TRUST Device PKI

Version 1.0

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement der D-TRUST Device PKI

Anfragen zu einer sonstigen, in der vorgenannten Lizenz nicht enthaltenen Nutzungsart dieses CPS der D-Trust GmbH sind zu richten an:

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	13.11.2019	▪ Initialversion
		▪
		▪
		▪
		▪
		▪
		▪
		▪
		▪
		▪
		▪
		▪
		▪

Inhaltsverzeichnis

1. Einleitung 6
1.1 Überblick 6
1.2 Name und Kennzeichnung des Dokuments 7
1.3 PKI-Teilnehmer 8
1.4 Verwendung von Zertifikaten 8
1.5 Administration der Policy 9
1.6 Begriffe und Abkürzungen 9
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen 10
2.1 Verzeichnisse 10
2.2 Veröffentlichung von Informationen zu Zertifikaten 10
2.3 Häufigkeit von Veröffentlichungen 10
2.4 Zugriffskontrollen auf Verzeichnisse 11
2.5 Zugang und Nutzung von Diensten 11
3. Identifizierung und Authentifizierung 11
3.1 Namensregeln 11
3.2 Initiale Überprüfung der Identität 13
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) 13
3.4 Identifizierung und Authentifizierung von Sperranträgen 13
4. Betriebsanforderungen 14
4.1 Zertifikatsantrag und Registrierung 14
4.2 Verarbeitung des Zertifikatsantrags 14
4.3 Ausstellung von Zertifikaten 14
4.4 Zertifikatsübergabe 14
4.5 Verwendung des Schlüsselpaars und des Zertifikats 15
4.6 Zertifikatserneuerung (certificate renewal) 15
4.7 Zertifikatserneuerung mit Schlüsselerneuerung 15
4.8 Zertifikatsänderung 15
4.9 Widerruf und Suspendierung von Zertifikaten 15
4.10 Statusabfragedienst für Zertifikate 17
4.11 Austritt aus dem Zertifizierungsdienst 17
4.12 Schlüsselhinterlegung und –wiederherstellung 17
5. Nicht-technische Sicherheitsmaßnahmen 18
5.1 Bauliche Sicherheitsmaßnahmen 18
5.2 Verfahrensvorschriften 18
5.3 Eingesetztes Personal 19
5.4 Überwachungsmaßnahmen 20
5.5 Archivierung von Aufzeichnungen 21
5.6 Schlüsselwechsel beim TSP 22
5.7 Kompromittierung und Geschäftsweiterführung beim TSP 22
5.8 Schließung des TSP bzw. die Beendigung der Dienste 23
6. Technische Sicherheitsmaßnahmen 23
6.1 Erzeugung und Installation von Schlüsselpaaren 23
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module 24
6.3 Andere Aspekte des Managements von Schlüsselpaaren 26
6.4 Aktivierungsdaten 26
6.5 Sicherheitsmaßnahmen in den Rechneranlagen 26
6.6 Technische Maßnahmen während des Life Cycles 27
6.7 Sicherheitsmaßnahmen für Netze 28
6.8 Zeitstempel 28
7. Profile von Zertifikaten und Sperrlisten 28

7.1 Zertifikatsprofile 28
7.2 Sperrlistenprofile 31
7.3 Profile des Statusabfragedienstes (OCSP) 31
8. Auditierungen und andere Prüfungen 31
9. Sonstige finanzielle und rechtliche Regelungen 32

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Certification Practice Statement (CPS) der von D-Trust GmbH betriebenen Dienste für Maschinenzertifikate, die über den Certificate Service Manager (CSM) bereitgestellt werden.

1.1.1 Diensteanbieter

Der Diensteanbieter (Trust Service Provider, im Folgenden TSP genannt) ist – auch im juristischen Sinne – die

D TRUST GmbH

Kommandantenstr. 15

10969 Berlin.

Der TSP kann Teilaufgaben an Partner oder externe Anbieter auslagern.

Für die Einhaltung der Verfahren im Sinne dieses Dokuments bzw. etwaiger gesetzlicher oder zertifizierungstechnischer Anforderungen an den TSP, bleibt der TSP, vertreten durch die Geschäftsführung oder deren Beauftragte, verantwortlich.

Die D-Trust GmbH stellt auch Zertifikate für eigene Zwecke aus. Hierbei werden ebenfalls die entsprechenden gesetzlichen bzw. zertifizierungstechnischen Anforderungen eingehalten.

1.1.2 Über dieses Dokument

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

Dieses CPS nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-Trust GmbH mit der OID 1.3.6.1.4.1.4788.2.200.1 und die Technische Richtlinie des BSI [TR-03145-1]. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

Das gesamte CPS ist rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist. Es enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit Garantien oder Zusicherungen betroffen sind, enthält dieses CPS ausschließlich die für diesen Bereich ausdrücklich eingeräumten Garantien oder Zusicherungen.

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

Die Struktur dieses Dokuments folgt dem Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework".

1.1.3 Eigenschaften der PKI

Die Dienste, die über den CSM bereitgestellt werden, beruhen auf einer mehrstufigen PKI. Abbildung 1 zeigt die schematische Konstellation der PKI. Sie besteht immer aus einer Kette, die angeführt wird von einer Root-CA (Wurzelinstanz oder Vertrauensanker), 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.

Der Dienst der Device PKI ist im eigentlichen Sinne kein Vertrauensdienst im Sinne der eIDAS sondern ein Dienst für technische Verfahren.

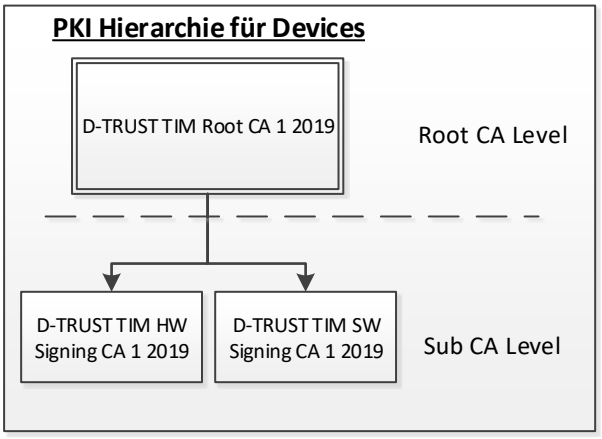

Abbildung 1 PKI-Hierarchie der Device PKI

CA-Zertifikate

D-TRUST TIM Root CA 1 2019 http://www.d-trust.net/cgi-bin/D-TRUST TIM Root CA 1 2019.crt Fingerprint: SHA1: df 21 5f e3 19 df 5e c7 7e 8a 70 d4 30 01 a5 05 91 27 d9 61
D-TRUST TIM HW Signing CA 1 2019 http://www.d-trust.net/cgi-bin/D-TRUST TIM HW Signing CA 1 2019.crt Fingerprint: SHA1: 76 bb e0 db c6 0f 0d 90 89 b0 b7 dd 9a 0a 64 ed 4b b0 8a 05
D-TRUST TIM SW Signing CA 1 2019 http://www.d-trust.net/cgi-bin/D-TRUST TIM SW Signing CA 1 2019.crt Fingerprint: SHA1: 34 7f ea 29 4b 0b 70 34 74 da 87 e7 37 96 c6 7f 16 c4 8d cd

Sowohl in CA- als auch in EE-Zertifikaten können CPs oder OIDs referenziert werden, die detailliert Anforderungen und Beschränkungen definieren.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Certification Practice Statement der D-TRUST Device PKI
Kennzeichnung (OID):	Dieses Dokument erhält die Policy-OID: 1.3.6.1.4.1.4788.2.400.1
Version	1.0

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Zertifizierungsstellen (Certification Authority – CA) werden vom Diensteanbieter betrieben und stellen Zertifikate sowie Sperrlisten aus. Möglich sind folgende Arten von Zertifikaten:

- Zertifikate für Geräte oder Maschinen(EE-Zertifikat)
- Zertifizierungsinstanzen (untergeordnete CA-Zertifikate des TSP).

Die Wurzelinstanzen stellen Zertifikate ausschließlich mit der Erweiterung basicConstraints: 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.

1.3.2 Registrierungsstellen (RA)

Die RA ist im Rahmen der Device PKI automatisiert.

Die RA erzeugt die Schlüsselpaare, legt den Common Name (in Form einer eindeutigen ID) fest, formuliert daraus einen Zertifikatsantrag und sendet diesen an die CMP-Schnittstelle des CSM. Die erhaltenen Zertifikate werden den privaten Schlüsseln zugeordnet und diese werden für die TSE Hersteller bereitgestellt.

1.3.3 Zertifikatsnehmer (ZNE) und Endanwender (EE)

Zertifikatsnehmer (*subscriber*) und Endanwender sind identisch. Endanwender (*subject*; End-Entity (EE)) ist in diesem Fall ein Gerät, auf dem die privaten Endanwenderschlüssel (EE-Schlüssel) verwendet werden.

1.3.4 Zertifikatsnutzer (ZNU)

Zertifikatsnutzer (englisch relying parties) sind natürliche oder juristische Personen, die die Zertifikate dieser 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.

Weiterhin gelten die Regelungen der CP der D-Trust GmbH.

1.4.2 Verbotene Verwendungen von Zertifikaten

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

Weiterhin gelten die Regelungen der CP der D-Trust GmbH.

1.4.3 Verwendung von Dienstezertifikaten

Dienstezertifikate werden durch den TSP selbst und zur eigenen Verwendung ausgestellt. Sie unterliegen den Anforderungen der jeweilig anwendbaren Zertifizierung.

Zu den Verwendungsarten zählen:

- CA-Zertifikate zur CA- und Zertifikatserstellung
- Signatur von Sperrauskünften

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird durch die D-Trust GmbH gepflegt und aktualisiert. Der Beauftragte der Geschäftsführung 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.

Kontaktdaten:

D-Trust GmbH
Redaktion CP und CPS
Kommandantenstr. 15

10969 Berlin, Germany

Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

D-TRUST stellt folgende E-Mail-Adresse für die Meldung von Sicherheitsvorfällen bereit:

security.incident@d-trust.net.

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 die Kompatibilität der Zertifizierungspraktiken mit der referenzierten CP.

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Diese Regelungen sind in der CP festgehalten.

1.6.2 Abkürzungen

Certificate Policy (CP)	Zertifikatsrichtlinie.
CMP	CMP-Schnittstelle des DTR CSM
CSM	Certificate Service Management: Dienst der DTR für die automatische Zertifikatsverwaltung
CSR	Certificate Signing Request

Weitere Regelungen sind in der CP festgehalten.

1.6.3 Referenzen

BSI [TR-03145-1]	Secure CA operation, Part 1 Teil 1 Generelle Anforderungen: Die TR-03145-1 beinhaltet generelle Anforderungen an Trust Center, die eine Certification Authority mit Sicherheitslevel "hoch" betreiben.
[X9.62]	ANS X9.62: "Public Key Cryptography for the Financial Service Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)", 2005

Weitere Regelungen sind in der CP festgehalten.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die Sperrliste (CRL) kann nur über HTTP abgerufen werden.

Weitere Regelungen sind in der CP festgehalten.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- CA-Zertifikate,
- Sperrlisten (CRLs),
- die CP,
- dieses CPS,

2.3 Häufigkeit von Veröffentlichungen

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und mindestens zehn Jahre nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig ausgestellt und können bis zum Ende des Bereitstellungszeitraumes des ausstellenden CA-Zertifikats und 24x7 abgerufen werden. Sperrlisten werden unmittelbar nach dem Widerruf von Zertifikaten erstellt und veröffentlicht. Auch wenn kein Widerruf von Zertifikaten erfolgt, stellt der TSP sicher, dass mindestens alle 24 Std. eine neue Sperrliste ausgestellt wird.

CA-Sperrlisten, die von Root-CAs ausgestellt werden, werden mindestens alle 12 Monate erstellt und veröffentlicht, auch wenn kein Widerruf von Zertifikaten vorgenommen wurde.

Dieses CPS wird veröffentlicht und bleibt mindestens so lange abrufbar, wie Zertifikate, die auf Basis dieses CPS ausgestellt wurden, gültig sind.

Die Webseiten des TSP können öffentlich und unentgeltlich 24x7 abgerufen werden (siehe CP 2.1).

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten und dieses CPS können öffentlich und unentgeltlich 24x7 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.

2.5 Zugang und Nutzung von Diensten

Diese Regelungen sind in der CP festgehalten.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

CA- und EE-Zertifikate enthalten grundsätzlich Angaben zu Aussteller (issuer) und. Endanwender (subject). Bei Maschinenzertifikaten (EE-Zertifikate) ist im subject eine eindeutige ID vergeben. Diese Namen werden entsprechend dem Standard [X.509] als DistinguishedName vergeben.

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 dieser PKI.

Eine eindeutige Zuordnung des Zertifikats zum Endanwender ist nicht gegeben.

Bei alternativen Namen (subjectAltName) gibt es keine Notwendigkeit für aussagefähige Namen. IP-Adressen sind nicht zugelassen.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern

Nicht anwendbar, da Pseudonyme ausschließlich für natürliche Personen benutzt werden.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

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

DN-Bestandteil	Interpretation
G (GivenName)	Feld wird nicht verwendet.
SN (Surname)	Feld wird nicht verwendet.
CN (commonName) (2.5.4.3)	Technische Komponente: Name oder ID des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.

DN-Bestandteil	Interpretation
PN (Pseudonym)	Feld wird nicht verwendet.
Serial Number (serialNumber) (2.5.4.5)	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt. Produktspezifisch kann das Feld anderweitig verwendet werden.
O (organizationName) (2.5.4.10)	Feld wird nicht verwendet.
OU (organizationalUnitName) (2.5.4.11)	Feld wird nicht verwendet.
OrgID (organizationIdentifier) (2.5.4.97)	Feld wird nicht verwendet.
C (countryName) (2.5.4.6)	DE
Street (streetAddress) (2.5.4.9)	Feld wird nicht verwendet.
Locality (localityName) (2.5.4.7)	Feld wird nicht verwendet.
State (stateOrProvinceName) (2.5.4.8)	Feld wird nicht verwendet.
PostalCode (postalCode) (2.5.4.17)	Feld wird nicht verwendet.

Es müssen nicht alle genannten DN-Bestandteile verwendet werden. Weitere können ergänzt werden. Ergänzende DN-Bestandteile müssen [RFC 5280], [RFC 6818] und BSI [TR-03145-1] entsprechen.

3.1.5 Eindeutigkeit von Namen

Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer (serialNumber) erzielt.

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

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Die RA haftet für die Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten (siehe Zertifikatsrichtlinie der D-Trust GmbH, Abschnitt 9.5).

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Die RA-Software erstellt auf Basis der Schlüsselpaare einen passenden CSR und übergibt diesen über eine definierte Schnittstelle (CMP) an den CSM. In dieser Schnittstelle garantiert die RA-Software die Kenntnis des privaten Schlüssels in Parameter „proof of possession".

3.2.2 Identifizierung und Authentifizierung von Organisationen

Nicht anwendbar.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

Nicht anwendbar.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Nicht anwendbar.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Nicht anwendbar.

3.2.6 Kriterien für die Interoperabilität

Nicht anwendbar.

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.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

Sperrberechtigt ist ausschließlich D-TRUST. D-TRUST kann Sperranträge von Zertifikatsempfängern sowie Geschäftspartnern über die RA annehmen und ausführen, sofern diese ihre Sperrberechtigung nachweisen und ihr Sperrinteresse ausreichend begründen können. Die Authentifizierung erfolgt in Abhängigkeit der vertraglichen Geschäftsbeziehung über einen abgestimmten Kommunikationsweg.

Sperrverfahren werden in Abschnitt 4.9 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

Der Prozess für die Zertifikatserstellung für Geräte erfolgt automatisiert. Eine formale Antragsstellung bzw. eine Registrierung beim TSP ist nicht erforderlich.

Das CSM erwartet einen gültigen Certificate Signing Request (CSR) auf Basis dessen der Prozess der Zertifikatserstellung gestartet wird. Der CSR muss an eine definierte Schnittstelle (CMP) des CSM gerichtet sein. Es werden nur CSR von authentifizierten Systemen akzeptiert. Die Verwaltung der Schlüssel der EE-Zertifikate obliegt der RA.

4.1.1 Berechtigung zur Antragstellung

Die RA kann über die CMP-Schnittstelle Zertifikatsanträge stellen, sofern sie sich gegenüber CSM authentifiziert.

4.1.2 Registrierungsprozess und Zuständigkeiten

Nicht anwendbar

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Nicht anwendbar.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Der TSP erhält die Antragsdaten über die CMP-Schnittstelle des CSM und überprüft die Qualität des öffentlichen Schlüssels (vgl. [X9.62, A.4.2]).

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Nicht anwendbar.

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.

Gemäß dem "Standardprozess CSM" werden Zertifikate erzeugt und über die definierte CMP-Schnittstelle zurückgegeben.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats.

Es erfolgt keine Benachrichtigung nach der Fertigstellung des Zertifikats.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Gemäß dem "Standardprozess CSM" werden Zertifikate erzeugt und über die definierte CMP-Schnittstelle an die RA zurückgegeben.

Werden Fehler in Zertifikaten oder bei der Funktion der Schlüssel und Token entdeckt, so ist dies dem TSP unverzüglich mitzuteilen. Die betroffenen Zertifikate werden widerrufen.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

Die Zertifikate werden nach der Produktion nicht veröffentlicht.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Es gibt keine Dritten, die über die Erstellung und Ausgabe eines Zertifikats unterrichtet werden.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Endanwender ist in diesem Fall ein Gerät und die privaten Schlüssel sind ausschließlich für die dafür vorgesehenen Anwendungen zu nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Zertifikate 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 und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifischen Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

4.6 Zertifikatserneuerung (certificate renewal)

Die Erstellung von Zertifikaten kann auf Basis bereits bestehender Schlüssel erfolgen, sofern die kryptografischen Eigenschaften der zu zertifizierenden Schlüssel noch vom TSP akzeptiert werden.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Eine Zertifikatserneuerung wird für Zertifikate der Device PKI angeboten. Bei gleichlautendem Subject DistinguishedName wird das serialNumber Attribut angepasst, um dessen Eindeutigkeit zu gewährleisten.

Bei CA-Schlüsseln wird keine Zertifikatserneuerung durchgeführt.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Widerruf und Suspendierung von Zertifikaten

4.9.1 Bedingungen für einen Widerruf von Zertifikaten

Die Verfahren des TSP erfüllen die Bedingungen aus [TR-03145].

Betroffene Dritte oder eine sonstige dritte Partei sind aufgefordert, den Widerruf unverzüglich zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden oder Inhaltsdaten des Zertifikats nicht mehr korrekt sind.

Der Widerruf eines Zertifikats wird bei folgenden Ereignissen durchgeführt:

- wenn zur Antragsstellung gültige Zertifikatsinhalte während des Gültigkeitszeitraums ungültig werden,
- wenn der TSP seine Tätigkeit beendet und diese nicht von einem anderen TSP fortgeführt wird.

Unabhängig davon kann der TSP Zertifikate widerrufen, 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,
- ein Zertifikat anderweitig missbraucht wurde,
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde.

Der Widerruf enthält eine Angabe des Zeitpunkts des Widerrufs und wird nicht rückwirkend erstellt. Weiterhin kann ein Widerruf nicht rückgängig gemacht werden.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zur Sperrung bzw. zum Widerruf

Der TSP ist sperrberechtigt.

Die RA kann über die CMP-Schnittstelle Sperranträge stellen, sofern sie sich gegenüber CSM authentifiziert.

4.9.3 Verfahren für einen Sperrantrag

Die RA stellt Sperranträge über die CMP-Schnittstelle an das CSM.

Der TSP kann ein Zertifikat auf allen ihm verfügbaren Wegen sperren.

Der Widerruf eines Zertifikats wird in der Verantwortung des TSP durchgeführt.

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.

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

4.9.4 Fristen für einen Sperrantrag

Nicht anwendbar.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Über die RA eingehende Sperranträge werden automatisch und unmittelbar ausgeführt.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten (CRL) vorgehalten. Die Erreichbarkeit des Sperrdienstes wird in Form von URLs in den Zertifikaten angegeben. Delta-CRLs werden nicht genutzt.

Integrität und Authentizität der Sperrinformationen wird durch eine Signatur der CRL gewährleistet.

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 die Sperrliste (CRL) 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

Nicht anwendbar. Der OCSP Dienst wird nicht angeboten.

4.11 Austritt aus dem Zertifizierungsdienst

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Termin.

Der Sperrauftrag zu einem Zertifikat löst den Widerruf des Zertifikats durch den TSP aus.

4.12 Schlüsselhinterlegung und –wiederherstellung

Schlüsselhinterlegung wird nicht vom TSP angeboten.

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 [TR-03145] betrieben werden.

Die D-Trust betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Information Security Policy regelt die verbindlichen Vorgaben für den Betrieb. Diese wurde von der Geschäftsführung der D-TRUST freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Führen prozess- bzw. betriebsbedingte Änderungen zu einem Update der Security Policy, sind die daraus resultierenden Änderungen für den TSP Betrieb von der Geschäftsführung zu genehmigen. Die aktualisierte und genehmigte Security Policy ist zeitnah durch die Führungskräfte an alle davon betroffenen Mitarbeiter zu kommunizieren bzw. bei Bedarf muss die Führungskraft Schulungsmaßnahmen einleiten.

Bis auf vereinzelte Identifizierungsdienstleistungen findet eine Auslagerung von Tätigkeiten an externe Dienstleister im Anwendungsbereich nicht statt. Soweit anwendbar werden notwendige Aspekte der Security Policy für Dienstleister ebenfalls verpflichtend.

5.1 Bauliche Sicherheitsmaßnahmen

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine anerkannte Konformitätsbewertungsstelle geprüft. Die Konformitätsbewertung wird gemäß [TR-03145] regelmäßig wiederholt.

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 bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Das genannte Zertifikat bestätigt der D-Trust GmbH diesen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Teil der Dokumentation ist ein Rollenkonzept, in dem Mitarbeiter einer oder mehreren Rollen durch das Management des TSP 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.

Rollen mit Sicherheitsverantwortung für den Betrieb des TSP, genannt „Trusted Roles", (mit unter anderem den Aufgaben des Sicherheitsbeauftragten, System Administrator, System Operator, System Auditor, Registration Officer, Revocation Officer und Validation Specialist) werden in den Berechtigungskonzepten der D-TRUST festgelegt. Diese Rollen dürfen nur von fachkundigen und zuverlässigen Mitarbeitern übernommen werden.

Mitarbeiter werden regelmäßig geschult, um ihre Rollen und damit verbundenen Verantwortlichkeiten zu erfüllen und bezüglich der Einhaltung geltender Sicherheitsvorgaben sensibilisiert. Die Anforderungen an die jeweiligen Rollen sind dokumentiert und können von den

Mitarbeitern jederzeit eingesehen werden. Bevor Mitarbeiter ihre zugewiesenen Rollen ausüben, müssen sie diesen zustimmen. Im Falle von sich ausschließenden Rollen, kann eine Person nur eine dieser Rollen übernehmen (Vier-Augen-Prinzip).

Eine Risikobewertung findet regelmäßig statt.

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

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.

Sicherheitskritische Systeme zur Zertifikatsausstellung sind zusätzlich durch eine Multi-Faktor-Authentisierung geschützt.

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, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Handeln vorzubeugen.

5.3 Eingesetztes Personal

Der TSP erfüllt die Anforderungen an das Personal aus BSI [TR-03145-1].

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.

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.

Insbesondere Führungskräfte werden nach speziellen Kriterien ausgewählt. Sie müssen nachweisen, dass sie in Bezug auf den bereitgestellten Vertrauensdienst über Kenntnisse der Sicherheitsverfahren für Mitarbeiter mit Sicherheitsverantwortung und über ausreichende Erfahrung in Bezug auf Informationssicherheit und Risikobewertung verfügen. Nachweise können in Form von Zertifikaten und Lebensläufen erbracht werden. Kann die erforderliche Qualifikation nicht ausreichend nachgewiesen werden, muss diese durch eine entsprechende Schulungsmaßnahme erworben werden bevor der Mitarbeiter im TSP Betrieb Managementfunktionen übernehmen darf.

5.3.2 Sicherheitsprüfungen

Personen, die in sicherheitsrelevanten Bereichen des TSP tätig sind, müssen unter anderem regelmäßig polizeiliche Führungszeugnisse vorlegen.

Übergreifend betreibt der TSP ein nach ISO 27001 zertifiziertes ISMS. Hierdurch werden den Mitarbeitern entsprechend sicherheitsrelevante Vorgaben bzw. Verhaltensregeln zugänglich gemacht.

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.

5.3.6 Maßnahmen bei unerlaubten Handlungen

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

Verstöße von Mitarbeitern gegen die Richtlinien oder die Prozesse des TSP-Betriebs werden analysiert und bewertet. Kann das Vertrauensverhältnis nicht sichergestellt werden, werden diese Mitarbeiter von sicherheitsrelevanten Tätigkeiten ausgeschlossen.

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 GmbH ist gewährleistet, dass von diesen definierten Verfahren im Produktionsbetrieb nicht abgewichen werden kann.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts

Der TSP betreibt umfangreiche Überwachungsmaßnahmen (beispielsweise durch Videoüberwachung) zur Absicherung der Zertifizierungsdienstleistungen und deren zugrundeliegenden IT-Systemen und Dokumenten.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besucher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des TSP sein.

5.4.2 Überwachung von organisatorischen Maßnahmen

Ein weiterer Bestandteil ist die Überwachung von organisatorischen Maßnahmen.

Hierzu gehört eine regelmäßige Risikoanalyse, die die Bedrohung für den Betrieb des TSP umfassend analysiert sowie Anforderungen und Gegenmaßnahmen sowie deren Umsetzung definiert. Ferner ist eine Restrisikoanalyse enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt und ggf. akzeptiert wird.

Weiterhin werden relevante Assets angemessen erfasst, sowie entsprechende Änderungen dieser Assets überprüft bzw. wenn anwendbar durch das vom Management beauftragte Personal des TSP freigegeben.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden.

Archiviert werden Dokumente zu Verfahrensrichtlinien (CP, CPS), Zertifikate, Sperrdokumentation, elektronische Dateien und Protokolle zum Zertifikatslebenszyklus. Dabei werden die Vorgänge zeitlich erfasst. Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird über DCF77 täglich gegen die offizielle Zeit synchronisiert.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Antragsrelevante Aufzeichnungen und Prüfungen werden mindestens zehn Jahre und bis zum Jahresende aufbewahrt.

Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird über DCF77 täglich gegen die offizielle Zeit synchronisiert.

5.5.3 Archivierung (intern / extern)

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

5.5.4 Sicherung des Archivs

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

5.5.5 Datensicherung des Archivs

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

5.5.6 Anforderungen zum Zeitstempeln von Aufzeichnungen

Der TSP betreibt einen Zeitstempeldienst gemäß [eIDAS].

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.

Sollte eine System Recovery erforderlich sein, sind die Verantwortlichkeiten und entsprechenden „Trusted Roles" im Berechtigungskonzept der D-TRUST deklariert und den jeweiligen Mitarbeitern bekannt. Siehe Abschnitt 5.2.1.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren für die Wiederherstellung der Betriebsfähigkeit des TSP. Es erfolgt ein tägliches Backup und ein Backup nach Veränderungen. Backups werden in einem anderen Brandabschnitt aufbewahrt. Die Wiederherstellungen von kritischen CA-Systemen werden im Rahmen von Notfallübungen regelmäßig getestet.

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 0, veranlasst der TSP folgendes:

- betroffene CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden widerrufen,
- involvierte Zertifikatsnehmer werden über den Vorfall und dessen Auswirkungen informiert,
- die zuständige Aufsichtsstelle wird informiert und der Vorfall wird auf den Webseiten des TSP veröffentlicht mit dem Hinweis, dass Zertifikate, die von dieser CA ausgestellt wurden, ihre Gültigkeit verlieren und der Sperrstatus verifiziert werden kann.

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 bzw. die Beendigung der Dienste

D-TRUST verfügt über einen fortlaufend aktualisierten Beendigungsplan.

Bei Beendigung der Dienste von CAs informiert der TSP alle Zertifikatsnehmer 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 widerrufen. Betroffene private CA-Schlüssel werden zerstört.

Im Fall einer geplanten Betriebseinstellung informiert der TSP alle Endanwender, Zertifikatsnehmer und Dritte vorab.

Der Verzeichnisdienst und Dokumente zur Antragstellung sowie das Repository (CP, CPS und CA-Zertifikate) werden an die Bundesdruckerei GmbH übergeben und unter äquivalenten 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 eine entsprechende Zusicherung der Bundesdruckerei für die Erfüllung dieser Mindestanforderungen.

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 PKI-Dienste, die in diesem CPS behandelt werden und bei der D-Trust GmbH betrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

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. Die Key-Ceremony erfolgt nach festgelegten Verfahren. In Abhängigkeit der CA erfolgt die Key-Ceremony durch dafür vorgesehen Trusted Roles im Beisein des Security Officers und falls erforderlich unter Aufsicht eines unabhängigen Dritten. Die Tätigkeiten während der Key Ceremony werden mittels Checkliste geprüft und protokolliert. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip erzwungen. Bei der Erzeugung von CA-Schlüsseln ist gegebenenfalls ein unabhängiger Auditor anwesend oder der Auditor kann sich nach der Schlüsselerzeugung durch eine Videoaufzeichnung vom ordnungsgemäßen Ablauf der Schlüsselerzeugung überzeugen. Weiterhin wird die Erstellung von CA-Schlüsseln gemäß BSI [TR-03145-1] dokumentiert.

Es werden keine EE-Schlüssel vom TSP erzeugt [TR-03145-1].

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Nicht anwendbar, da keine EE-Schlüssel vom TSP erzeugt werden.

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

Der öffentliche Schlüssel werden nur in Form von CSRs an den TSP geliefert.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Die Lieferung öffentlicher CA-Schlüssel für Zertifikatsnutzer erfolgt über die RA an die TSE Hersteller und Geschäftspartner.

6.1.5 Schlüssellängen

Für CA-Zertifikate werden derzeit ECC-Schlüssel mit einer Schlüssellänge von mindestens 384 Bit mit Nist-Kurve (secp384r1) verwendet.

Für EE-Zertifikate werden derzeit ECC-Schlüssel mit einer Schlüssellänge von mindestens 256 Bit mit Nist-Kurve (secp256r1) verwendet.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

CA- und EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die die Vorgaben aus [X9.62, A.4.2] erfüllen.

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 und Sperrlisten verwendet. Alle anderen privaten CA-Schlüssel werden zum Signieren von CA-Zertifikaten, EE-Zertifikaten und Sperrlisten benutzt (siehe Abschnitt7.1.2).

Die EE-Schlüssel dürfen nur für die im Zertifikat benannten Nutzungsarten verwendet werden. Die Nutzungsarten werden in den Feldern *KeyUsage* und *ExtKeyUsage* im Zertifikat definiert und ggf. durch weitere Extentions eingeschränkt (siehe Abschnitt7.1.2).

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.

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

Das HSM, auf dem die CA-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die Aktivierung des privaten Schlüssels erfolgt automatisiert in der RA-Software.

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)

Nicht anwendbar, da keine EE-Schlüssel vom TSP erzeugt werden und damit auch nicht hinterlegt werden.

6.2.4 Backup privater Schlüssel

Es ist ein Backup der privaten CA-Schlüssel vorhanden. Ein CA-Schlüssel-Backup erfordert für diese Tätigkeit am HSM zwei 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, da vom TSP keine EE-Schlüssel erzeugt werden.

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.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten CA-Schlüssel liegen verschlüsselt im HSM vor.

Für EE-Schlüssel nicht anwendbar, da vom TSP keine EE-Schlüssel erzeugt werden.

6.2.8 Aktivierung privater Schlüssel

Nicht anwendbar.

6.2.9 Deaktivieren privater Schlüssel

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

Für EE-Schlüssel nicht anwendbar, da vom TSP keine EE-Schlüssel erzeugt werden.

6.2.10 Zerstörung privater Schlüssel

Die privaten CA-Schlüssel werden gelöscht, wenn ihre geplante Nutzungsdauer abgelaufen ist. Die Nutzungsdauer ist gemäß ETSI ALGO Paper TS 119 312 und SOG-IS festgelegt. Dies erfolgt durch Löschen auf dem HSM und gleichzeitigem Löschen der auf Datenträgern 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 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 8 Jahre.

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.

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.

6.4.3 Andere Aspekte von Aktivierungsdaten

Nicht anwendbar.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

Die D-TRUST betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Security Policy regelt die verbindlichen Vorgaben für den IT Betrieb. Diese wurde von der Geschäftsführung der D-TRUST freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Die Bewertung und ggf. die Behebung von identifizierten Schwachstellen erfolgt innerhalb von 48 Stunden. Ist die Behebung innerhalb von 48 Stunden nicht möglich, so enthält die Bewertung einen konkreten Behandlungsplan.

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 [TR-03145] 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.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdates in angemessener Zeit auf den relevanten Systemen installiert werden. Abweichungen hiervon werden vom TSP angemessen dokumentiert und ggf. im Risikomanagement des TSP adressiert.

Zertifikatsnehmer 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 Konformitätsbewertungsstellen regelmäßig geprüft und unterliegen gemäß [EN 319 401] einem entsprechenden Monitoring.

6.5.3 Monitoring

Zur Sicherstellung der Verfügbarkeit erfolgt ein kontinuierliches Monitoring der relevanten Systeme. Jede Störung wird erfasst, dokumentiert und gemäß ihrer Auswirkung mit einem Schweregrad gekennzeichnet und daraufhin priorisiert. Die Behandlung von kritischen Meldungen erfolgt im Rahmen des Prozesses Incident Management. Meldungen zu sicherheitsrelevanten Ereignissen werden an eine zentrale Stelle übermittelt und gemäß Kritikalität ausgewertet.

Bei Störungen mit Verfügbarkeitsverlust eines Services werden die betroffenen Parteien mindestens alle 24 Stunden über einen aktuellen Status zur Störungsbeseitigung informiert.

6.6 Technische Maßnahmen während des Life Cycles

Bereits bei der Planung aller vom TSP oder im Auftrag des TSP betriebener Systeme werden die Anforderungen aus Abschnitt 5 [BRG] und BSI [TR-03145-1] angemessen berücksichtigt.

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 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 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 dokumentierten 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 relevanten 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 Klassifizierung im Rahmen der Dokumentationsrichtlinie des TSP zuverlässig vor Schaden, Entwendung, Verlust oder Kompromittierung geschützt.

Penetrationstests werden durch eine unabhängige und fachkundige Stelle regelmäßig durchgeführt. Weiterhin werden regelmäßig Schwachstellenscans veranlasst.

6.7 Sicherheitsmaßnahmen für Netze

Im Betrieb der CAs wird ein Netzkonzept realisiert, welches sicherstellt, dass die relevanten CA-Systeme in besonders gesicherten Netzwerkzonen betrieben werden. Die Netzwerkarchitektur des TSP beinhaltet ein mehrstufiges Konzept der Netzwerksicherheitszonen. Die Root CAs werden in der Netzwerksicherheitszone mit dem höchsten Schutzbedarf betrieben. Für das Netzkonzept liegt eine detaillierte Dokumentation vor, 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, die nur explizit erlaubte Verbindungen zulassen. 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.

Die Verfügbarkeit der Internetanbindung ist durch Redundanz abgesichert. Es bestehen zwei ständige Verbindungen zum Provider auf zwei unterschiedlichen Streckenführungen. Beim Ausfall des Zugangspunktes des Providers erfolgt die automatische Umschaltung auf die zweite Anbindung.

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.

6.8 Zeitstempel

Der TSP betreibt einen Zeitstempeldienst. Zeitstempel werden im Rahmen dieses CPS jedoch nicht angeboten.

7. Profile von Zertifikaten und Sperrlisten

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 Ausstellerschlüssels
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
CRLDistributionPoints	2.5.29.31	Adresse(n) der CRL-Ausgabestelle(n)
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=caIssuers {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs
SubjectAltName	2.5.29.17	Alternativer Inhabername

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280] und [RFC 6818] 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], [RFC 6818]
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellerschlüssels
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
CRLDistributionPoints	2.5.29.31	CRL-Ausgabestelle
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod= caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs *cpsURI*
SubjectAltName	2.5.29.17	Alternativer Inhabername
QCStatements	*1.3.6.1.5.5.7.1*	Es sind keine QCStatements gesetzt.

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280] und [RFC 6818] entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.3 Algorithmen-OIDs

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

- ECDSA auf Basis der NIST-Kurve "P-384" (secp384r1) mit OID: 1.3.132.0.34.

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

- NIST-Kurve "secp256r1" mit OID: 1.2.840.10045.3.1.7.

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 Zertifikatsnehmername) und *Issuer-AltName* (Alternativer Ausstellername) können Namen gemäß [RFC 5280], [RFC 6818] (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.

Weitere Regelungen sind in der CP enthalten.

7.1.7 Nutzung der Erweiterung „PolicyConstraints"

„PolicyConstraints" wird nicht benutzt.

7.1.8 Syntax und Semantik von „PolicyQualifiers"

„PolicyQualifiers" können benutzt werden.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung von CertificatePolicies

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

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Es werden Sperrlisten v2 gemäß [RFC 5280], [RFC 6818] erstellt. Delta-CRLs sind nicht vorgesehen.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Sperrlisten 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)

Ein OCSP-Responder wird nicht angeboten.

8. Auditierungen und andere Prüfungen

Revisionen, Revisionsgegenstände und Prozesse sind detailliert in der Dokumentation der D TRUST GmbH beschrieben. Das Rollenkonzept dokumentiert die Qualifikation und die Stellung des Revisors.

Die Dokumentation wird regelmäßig durch eine unabhängige Konformitätsbewertungsstelle geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

CP und CPS erfüllen für Zertifikate die Anforderungen gemäß BSI [TR-03145-1]. Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten („competent independent party" gemäß [TR-03145] belegt die Kompatibilität.

Der TSP gibt Zertifikate erst nach der initialen und erfolgreich abgeschlossenen Prüfung durch einen unabhängigen externen Zertifizierer aus. Es finden regelmäßige Wiederholungsprüfungen statt. Sollten sich die Verfahren als nicht mehr konform zu den aktuellen Richtlinien erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität 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.