Certification Practice Statement der D-TRUST-Root PKI

Version 1.10

Erscheinungsdatum	01.05.2014
Datum des Inkrafttretens	01.05.2014

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	18.06.2008	Initialversion
1.1	01.11.2008	- Änderung der Bedingungen zur Berechtigung zur Antragstellung bezüglich der Volljährigkeit - Anpassung der Prüfverfahren für SSL-Zertifikate mit *dNSNames* - Generalisierung OCSP-Pfad - Anpassung Prüfverfahren von Class-1-Zertifikaten - Anpassungen für SSL-Zertifikate
1.2	01.06.2009	- Erweiterung Sperrgründe von Code-Signing Zertifikaten - editorische Änderungen - Anpassung aufgrund WebTrust Audit
1.3	25.02.2010	- Konkretisierung: für SSL-Zertifikate wird weder Zertifikatserneuerung (renewal) noch Zertifikatserneuerung mit Schlüsselerneuerung angeboten
1.4	21.09.2010	Update aufgrund neuer Version [ETSI-F] und [GL-BRO]
1.5	02.02.2011	Beschränkung der SSL-Zertifikate auf registierungspflichtige Domains
1.6	14.09.2011	Begrenzung der Laufzeit bei SSL-Zertifikaten auf 39 Monate
1.7	26.07.2012	Erweiterung der Gültigkeitszeiträume Class 2 Entkoppelung Class 2 von „LCP“
1.8	07.02.2013	Anpassung aufgrund Änderung der [ETSI-F] einschließlich Baseline Requirements des CA/Browser Form [BRG] und der Network and Certificate Systems Security Requirements [NetSec-CAB].
1.9	30.10.2013	Angleichung der Definitionen von subject und subscriber an [ETSI-F]. Einführung des Niveaus LCP und damit verbundener Verfahren. Redundanzen im Verhältnis zur CP wurden durch Streichungen / Verweise beseitigt. Ergänzungen um technische und organisatorische Maßnahmen entsprechend [ETSI-F] - Kap. 7.4.5: operations management - Kap. 7.4.6: system access management
1.10	01.05.2014	Anpassung Zertifikatsprofile Kapitel 7.1.2 und 7.1.3; formale Anpassung der Klassennotation

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

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

1.1.1 Zertifizierungsdiensteanbieter

Diese Regelungen sind in der [CP] festgehalten.

1.1.2 Über dieses Dokument

Dieses CPS definiert mögliche 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.

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

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.

Das CPS erläutert bzw. erweitert die in der zugehörigen CP beschriebenen Verfahren, bei identischen Formulierungen werden Referenzen auf die CP eingesetzt.

1.1.3 Eigenschaften der PKI

Diese Regelungen sind in der [CP] festgehalten.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Certification Practice Statement der D-TRUST-Root-PKI
Version	1.10

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Diese Regelungen sind in der [CP] festgehalten.

1.3.2 Registrierungsstellen (RA)

Diese Regelungen sind in der [CP] festgehalten.

1.3.3 Zertifikatnehmer (ZNE)

Diese Regelungen sind in der [CP] festgehalten.

1.3.4 Zertifikatsnutzer (ZNU)

Diese Regelungen sind in der [CP] festgehalten.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Diese Regelungen sind in der CP festgehalten.

1.4.2 Verbotene Verwendungen von Zertifikaten

Diese Regelungen sind in der CP festgehalten.

1.5 Pflege der CP/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.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Diese Regelungen sind in der CP festgehalten.

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

Diese Regelungen sind in der CP festgehalten.

2.3 Häufigkeit von Veröffentlichungen

Diese Regelungen sind in der CP festgehalten.

2.4 Zugriffskontrollen auf Verzeichnisse

Diese Regelungen sind in der CP festgehalten.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Diese Regelungen sind in der CP festgehalten.

3.1.2 Notwendigkeit für aussagefähige Namen

Diese Regelungen sind in der CP festgehalten.

3.1.3 Anonymität oder Pseudonyme von Zertifikatnehmern

Diese Regelungen sind in der CP 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 entsprechend - Class 3 und Class 2 dem zur Identifizierung vorgelegten Dokument - Class 1 den Angaben des Zertifikatnehmers.
SN	*Familienname* der natürlichen Person entsprechend - Class 3 und Class 2 dem zur Identifizierung vorgelegten Dokument - Class 1 den Angaben des Zertifikatnehmers. 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.

DN-Bestandteil	Interpretation
PN	*Pseudonym*: ist identisch zu CN.
serialNumber	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Sonderfall bei Class 3 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].
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, das das Dokument ausgestellt hat, mit dem der Zertifikatnehmer identifiziert wurde.
Titel	Ein *Titel* kann aufgenommen werden.
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)

3.1.5 Eindeutigkeit von Namen

Diese Regelungen sind in der [CP] festgehalten.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Diese Regelungen sind in der [CP] festgehalten.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Diese Regelungen sind in der [CP] festgehalten.

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.

In den verschiedenen Klassen werden 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.

<table>
<tr><th></th><th>Class 3</th><th>Class 2</th><th>Class 2 LCP</th><th>Class 1</th></tr>
<tr><td>CN
O
C</td><td>Register/
Non-Register/
Domain</td><td>Register/
Non-Register/
Domain</td><td>HR-
DB/Register/
Non-Register/
Domain</td><td>Register/
Domain</td></tr>
<tr><td>OU
STREET
L
State
PostalCode</td><td>Z-Bestätigung/
Register/
Non-Register</td><td>A-
Bestätigung/
Register/
Non-Register/
out-of-band-
Mechanis-
men/ Domain</td><td>A-
Bestätigung/
Register/
Non-Register/
out-of-band-
Mechanis-
men/ Domain</td><td>Keine
Prüfung</td></tr>
</table>

	Class 3	Class 2	Class 2 LCP	Class 1
E-Mail-Adresse	Keine Prüfung (Bestätigung durch Zertifikatnehmer)	Keine Prüfung (Bestätigung durch Zertifikatnehmer)	Keine Prüfung (Bestätigung durch Zertifikatnehmer)	Keine Prüfung (Bestätigung durch Zertifikatnehmer)
Alle weiteren Attribute[1]	**Z-Bestätigung**/ A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen	Keine Prüfung

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

Class 2

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

In den verschiedenen Klassen werden 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.

	Class 3	**Class 2**	**Class 2 LCP**	**Class 1**
G	Pers-Ident	HR-DB/ Dok-Ident/ **Z-Bestätigung**/ A-Bestätigung/ Körperschaften/ out-of-band-Mechanismen	HR-DB/ Dok-Ident/ **Z-Bestätigung**/ A-Bestätigung/ Körperschaften/ out-of-band-Mechanismen	
SN				
CN				
C				
STREET				
L				
S				
PostalCode				
Titel	Pers-Ident/ Dok-Ident			
O (Organisationszugehörigkeit)	**Z-Bestätigung**	A-Bestätigung/ **Z-Bestätigung**/ Körperschaften/ out-of-band-Mechanismen/ HR-DB	A-Bestätigung/ **Z-Bestätigung**/ Körperschaften/ out-of-band-Mechanismen/ HR-DB	
OU (Organisationszugehörigkeit)				
E-Mail-Adresse	Keine Prüfung (Bestätigung durch Zertifikatnehmer)	Keine Prüfung (Bestätigung durch Zertifikatnehmer)	Keine Prüfung (Bestätigung durch Zertifikatnehmer)	E-Mail

	Class 3	Class 2	Class 2 LCP	Class 1
Alle weiteren Attribute[2]	**Z-Bestätigung** / A-Bestätigung/ Dok-Ident/ out-of-band-Mechanis-men	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanis-men/ HR-DB	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanis-men/ HR-DB	

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) Klassen-spezifisch geprüft. Für die Aufnahme von Namen für Gruppen, Funktionen oder IT-Prozesse im CN gelten die Klassen-spezifischen Verfahren analog zu Zeile „Alle weiteren Attribute“.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatnehmer

Diese Regelungen sind in der CP festgehalten.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Class 3, Class 2

Bei natürlichen Personen werden Identitätsnachweis und ggf. die Organisationszugehörigkeit mittels der Klassen-spezifischen Verfahren gemäß Abschnitt 3.2.3 ermittelt und geprüft bzw. bestätigt.

Bei Organisationen wird der Existenznachweis sowie die Vertretungsberechtigung des Antragstellers Klassen-spezifisch nach Abschnitt 3.2.2 geprüft bzw. bestätigt.

Class 1

Abgesehen von wirtschaftlichen Verifikationen findet keine Prüfung der Berechtigung zur Antragstellung statt.

3.2.6 Kriterien für die Interoperabilität

Diese Regelungen sind in der [CP] festgehalten.

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

Diese Regelungen sind in der [CP] festgehalten.

3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

Diese Regelungen sind in der [CP] festgehalten.

3.3.2 Schlüsselerneuerung nach Sperrungen

Diese Regelungen sind in der [CP] festgehalten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

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 ZDA vorliegen muss.

- Class 3, Class 2
  Bei einem Sperrantrag mit handschriftlich unterschriebener *Briefpost* muss aus dem Unterschriftenvergleich erkennbar sein, dass der die Sperrung Beantragende entweder der Zertifikatnehmer selbst oder ein benannter Sperrberechtigter Dritter ist.
- Class 3, Class 2
  Bei *telefonischem* Sperrantrag oder einem Antrag per *E-Mail* ohne Signatur muss der Sperrberechtigte das entsprechende Sperrpasswort korrekt nennen.
- Class 1
  Bei einem Sperrantrag mit handschriftlich unterschriebener Briefpost muss der die Sperrung Beantragende der Zertifikatnehmer selbst sein.

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

Diese Regelungen sind in der [CP] festgehalten.

4.1.2 Registrierungsprozess und Zuständigkeiten

Class 3, Class 2

Dem Zertifikatnehmer liegen vor Beginn des Registrierungsprozesses CP, 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.

Class 3 EV-Zertifikate

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

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

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

Der ZDA 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 der [CP] 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.

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 Handel-register- oder vergleichbare Auszüge, die nicht älter als ein halbes Jahr alt sind, Promotions-, Habilitations-, Ernennungs-

urkunden sowie Dokumente vergleichbaren Ranges. Nachweise werden hinterlegt.

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.

Non-Register
Staatliche Einrichtungen/öffentlich-rechtliche Institutionen bestätigen zertifikatsrelevante Informationen mit Dienstsiegel und Unterschrift. Nachweise werden hinterlegt.

HR-DB
Der ZDA schließt vertragliche Vereinbarungen mit einer Organisation (Zertifikatnehmer) und vereinbart, dass nur valide Daten übermittelt werden, die die Vorgaben der [CP] erfüllen. Ein autorisierter Mitarbeiter oder Funktionsträger einer Organisation übermittelt dem ZDA 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 ZDA 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 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.

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 Existenznach-weis für die Organisation ersichtlich sein oder anderweitig nachgewiesen werden. Nachweise werden hinterlegt.

A-Bestätigung
Autorisierte Mitarbeiter oder Funktionsträger innerhalb einer Organisation oder vertrauenswürdige Dritte (z. B. Partner des ZDA oder staatliche Institutionen) bestätigen bestimmte zertifikatsrelevante Informationen, die in ihrer Bestätigungs-

kompetenz liegen. Dies geschieht schriftlich, in Einzelfällen können elektronisch signierte Bestätigungen akzeptiert werden. Nachweise werden hinterlegt.

out-of-band-Mechanismen
Der ZDA 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 ZDA kann beispielsweise mittels Banküberweisung, Lastschrift- oder Kreditkarteneinzug erfolgen. Der ZDA 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 ZDA.

Zur Identifizierung natürlicher Personen kann eine postalische Sendung mittels "Einschreiben mit Rückschein" vom ZDA 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 weiteren zertifikatsrelevanten Daten können auch mittels telefonischer Nachfrage über ein öffentliches Telefonverzeichnis seitens des ZDA bestätigt werden.

Körperschaften
Der ZDA schließt vertragliche Vereinbarungen mit Körperschaften des öffentlichen Rechts und vereinbart, dass nur Daten übermittelt werden, die die Vorgaben der [CP] erfüllen. Ein autorisierter Mitarbeiter oder Funktionsträger dieser Körperschaft des öffentlichen Rechts übermittelt dem ZDA 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.

Domain
Die Domain einer Organisation und ggf. weitere Attribute wie E-Mail-Adressen werden durch eine Domain-Abfrage in offiziellen Registern (WHOIS) geprüft. Class 3 und Class 2: Dabei wird hinterfragt, ob der Zertifikatnehmer über die exklusive Kontrolle der Domain verfügt. Die Ergebnisse der Abfrage werden hinterlegt. 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.

E-Mail
Der ZDA schickt 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 [CP] statt.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Eine vom ZDA beauftragte "unabhängige zweite" Person der laut Sicherheitskonzept entsprechenden Rolle prüft die Antragsunterlagen nach folgenden Kriterien:

- wurde die Authentifizierung des Zertifikatnehmers korrekt durchlaufen und dokumentiert,
- wurden alle notwendigen Nachweise erbracht,
- liegen Gründe vor, die eine Ablehnung des Antrags nahe legen.

Mögliche Ablehnungsgründe sind in der [CP] festgehalten.

Treten bei der Prüfung der Identität oder der Prüfung auf Korrektheit der Daten im Zertifikatsantrag oder den Ausweis- und Nachweisdokumenten Unstimmigkeiten auf, die der Zertifikatnehmer nicht zeitnah und restlos ausräumt, wird der Antrag abgelehnt.

Nach eingehender Prüfung entsprechend der Verfahrensanweisung entscheidet der Prüfende nach Sachlage, ob der Antrag abgeleht oder weiterverarbeitet wird.

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

Erhält der ZDA vorab Zertifikatsdaten über eine mandantenfähige Onlineschnittstelle, kann eine Vorabprüfung der Zertifikatsdaten erfolgen. Wird dann die eigentliche Zertifikatsanforderung nach der Prüfung 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 ZDA 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 ZDA gemäß Abschnitt 5.5 revisionssicher abgelegt oder der ZDA schließt vertragliche Vereinbarungen 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

Diese Regelungen sind in der [CP] festgehalten.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Diese Regelungen sind in der [CP] festgehalten.

4.4.2 Veröffentlichung des Zertifikats durch den ZDA

Diese Regelungen sind in der [CP] festgehalten.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Diese Regelungen sind in der [CP] festgehalten.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer

Diese Regelungen sind in der [CP] festgehalten.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Diese Regelungen sind in der [CP] festgehalten.

4.6 Zertifikatserneuerung (certificate renewal)

Diese Regelungen sind in der [CP] festgehalten.

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.

Detaillierte Regelungen sind in der [CP] festgehalten.

4.6.2 Berechtigung zur Zertifikatserneuerung

Diese Regelungen sind in der [CP] festgehalten.

4.6.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Class 3, Class 2
Eine vom ZDA beauftragte Person der entsprechenden Rolle prüft die Berechtigung zur Antragsstellung sowie die Signatur gemäß Verfahrensanweisung. Nach eingehender Prüfung entscheidet der Prüfende nach Sachlage, ob der Antrag abgelehnt oder weiterverarbeitet wird. Wird der Antrag zur Weiterverarbeitung weitergegeben, stellt die entsprechende Rolle neue Zertifikate aus. Die Prüfung sowie Ausstellung kann unter Beibehaltung der Prüfschritte teilweise oder vollständig automatisiert erfolgen.

Class 1
Anträge werden teils automatisiert, teils manuell geprüft und entweder abgelehnt oder weiterverarbeitet.

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

Diese Regelungen sind in der [CP] festgehalten.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch den ZDA

Diese Regelungen sind in der [CP] festgehalten.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Diese Regelungen sind in der [CP] festgehalten.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Diese Regelungen sind in der [CP] festgehalten.

4.7.1 Bedingungen für Zertifikate mit Schlüsselerneuerung

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

Die weiteren Regelungen sind in der [CP] festgehalten.

4.7.2 Berechtigung zur Schlüsselerneuerung

Diese Regelungen sind in der [CP] festgehalten.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Class 3, Class 2
Eine vom ZDA beauftragte Person der entsprechenden Rolle prüft die Berechtigung zur Antragsstellung sowie die Signatur gemäß Verfahrensanweisung. Nach eingehender Prüfung entscheidet der Prüfende

nach Sachlage, ob der Antrag abgelehnt oder weiterverarbeitet wird. Wird der Antrag zur Weiterverarbeitung gegeben, stellt die entsprechende Rolle neue Zertifikate aus. Die Prüfung sowie Ausstellung kann unter Beibehaltung der Prüfschritte teilweise oder vollständig automatisiert erfolgen.

Class 1
Anträge werden teils automatisiert, teils manuell geprüft und entweder abgelehnt oder weiterverarbeitet.

4.7.4 Benachrichtigung des Zertifikatnehmers über die Ausgabe eines Nachfolgezertifikats

Diese Regelungen sind in der [CP] festgehalten.

4.7.5 Verhalten für die Ausgabe von Zertifikaten nach Schlüsselerneuerungen

Diese Regelungen sind in der [CP] festgehalten.

4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen durch den ZDA

Diese Regelungen sind in der [CP] festgehalten.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Diese Regelungen sind in der [CP] festgehalten.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Die Sperrung eines Zertifikats wird bei folgenden Ereignissen durchgeführt:

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

Unabhängig davon kann der ZDA Sperrungen veranlassen, wenn:

- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- das Schlüsselpaar sich auf einer Signaturkarte befindet, auf der gleichzeitig ein Schlüsselpaar liegt, das zu einem qualifizierten Zertifikat gehört, welches gesperrt wird,
- 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.

Class 3 EV-Zertifikate
[GL-BRO] sieht für EV-Zertifikate zwingende Sperrgründe vor (Annex A).

Der ZDA 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 ZDA 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.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zur Sperrung

Diese Regelungen sind in der [CP] festgehalten.

4.9.3 Verfahren für einen Sperrantrag

Diese Regelungen sind in der [CP] festgehalten.

4.9.4 Fristen für einen Sperrantrag

Diese Regelungen sind in der [CP] festgehalten.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den ZDA

Diese Regelungen sind in der [CP] festgehalten.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Diese Regelungen sind in der [CP] festgehalten.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Diese Regelungen sind in der [CP] festgehalten.

4.9.8 Maximale Latenzzeit für Sperrlisten

Diese Regelungen sind in der [CP] festgehalten.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

Diese Regelungen sind in der [CP] festgehalten.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Diese Regelungen sind in der [CP] festgehalten.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Diese Regelungen sind in der [CP] festgehalten.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Diese Regelungen sind in der [CP] festgehalten.

4.9.13 Bedingungen für eine Suspendierung

Diese Regelungen sind in der [CP] festgehalten.

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

Diese Regelungen sind in der [CP] festgehalten.

4.10.3 Optionale Leistungen

Keine.

4.11 Austritt aus dem Zertifizierungsdienst

Diese Regelungen sind in der [CP] festgehalten.

4.12 Schlüsselhinterlegung und –wiederherstellung

Diese Regelungen sind in der [CP] festgehalten.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Diese Regelungen sind in der [CP] festgehalten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Diese Regelungen sind in der [CP] festgehalten.

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die CAs Class 3 und Class 2 die bei der D-TRUST GMBH 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 die von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle TÜV Informationstechnik GmbH 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“ (TUVIT-TSI66184.13 vom 22.03.2013) 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 Root-PKI werden vom ZDA 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 [Siko-DTR], in dem Mitarbeiter einer oder mehreren Rollen zugeordnet werden und entsprechende Berechtigungen erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zuordnung der Berechtigungen wird regelmäßig 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 ZDA 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 ZDA 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 ZDA 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 ZDA 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 ZDA 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 ZDA schult Personen, die im Zertifizierungsdienst tätig sind.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Der ZDA 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 ZDA 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 ZDA 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 Besucher 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 ZDA sein.

Ein weiterer Bestandteil des Sicherheitskonzepts ist eine Risikoanalyse, die Bedrohung für den Betrieb des ZDA 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

Class 3, Class 2

Dokumente zur Antragstellung und Prüfung sowie die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden mindestens fünf Jahre und bis zum Jahresende aufbewahrt[3]. Für alle SSL Zertifikate einschließlich Class 3 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 ZDA.

5.5.4 Datensicherung des Archivs

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

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Der ZDA betreibt einen Zeitstempeldienst gemäß [SigG].

5.5.6 Archivierung (intern / extern)

Die Archivierung erfolgt intern beim ZDA, 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 ZDA.

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

5.6 Schlüsselwechsel beim ZDA

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

5.7 Kompromittierung und Geschäftsweiterführung beim ZDA

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Der ZDA 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 Insuffizienz von Algorithmen oder assoziierten Parametern durch die Herausgeber der maßgeblichen Kataloge nach Abschnitt 6.1.6, veranlasst der ZDA 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 ZDA 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 ZDA 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 ZDA

Bei Beendigung der Dienste von CAs informiert der ZDA alle Zertifikatnehmer und beendet alle Zugriffsmöglichkeiten von Unterauftragnehmern des ZDA 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 ZDA oder der Bundesdruckerei GmbH übergeben.

Der ZDA 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 Class 3 und Class 2, die bei der D-TRUST GMBH betrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

An dieser Stelle wird zwischen Schlüsselpaaren für die

- CA-Zertifikate (D-TRUST Root CA Class 3 und Class 2 und deren Sub-CAs) 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.

EE-Schlüssel werden vom ZDA oder dem Zertifikatnehmer kryptographisch sicher erzeugt und entsprechen den Vorgaben von [CP] und [CPS].

Class 3, Class 2
: Werden EE-Schlüssel und EE-Zertifikate auf Chipkarten (Secure User Device (SUD) gemäß [ETSI-F], D-TRUST GMBH verwendet eine bestätigte SSCD als SUD) aufgebracht, verfährt der ZDA bei der Beschaffung, Lagerung, Personalisierung und beim PIN-Handling wie im qualifizierten Betrieb SigG-konform und gemäß Sicherheitskonzept des ZDA. Der ZDA kann Dritte mit der Schlüsselgenerierung und Personalisierung der Chipkarte beauftragen, die ein SigG-konformes Sicherheitskonzept vorweisen. Der ZDA betreibt seinerseits eine SigG-konforme Schnittstelle zu diesen externen Personalisierern.

Class 2 LCP
: Schlüsselpaare für Zertifikate, die als Soft-PSE produziert werden, entstehen im Rahmen einer sichereren Einsatzumgebung auf Basis von vertrauenswürdigen kryptographischen Anwendungen.

6.1.2 Lieferung privater Schlüssel an Zertifikatnehmer

Werden die privaten Schlüssel beim ZDA erzeugt, werden sie gemäß Abschnitt 4.4.1 zugestellt.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

CA-Schlüsselpaare werden im Trustcenter erzeugt.

Die EE-Schlüsselpaare, die im Verantwortungsbereich des ZDA erzeugt werden, liegen dem ZDA 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

Class 3, Class 2

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.

Class 1

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 1024 Bit verwendet.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

Class 3, Class 2

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.

Class 3 EV-Zertifikate

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

Class 1

Der ZDA legt Schlüsselparameter für CA-Zertifikate und EE-Zertifikate fest.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 7.1.3 CPS genannt.

6.1.7 Schlüsselverwendungen

Private CA-Schlüssel werden ausschließlich zum Signieren von 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 *ExtKeyUsage* im Zertifikat definiert und ggf. durch weitere Extentions eingeschränkt (siehe Abschnitt 7.1.2).

6.2 Sicherung des privaten Schlüssels und Anforderungen an krytographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die vom ZDA 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 ZDA 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)

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-Schlüssel werden nicht hinterlegt.

Das Hinterlegen privater EE-Schlüssel kann beantragt werden. Die Schlüssel werden verschlüsselt im Hochsicherheitsbereich des Trustcenters gehalten und können nur von autorisierten Personen wieder entschlüsselt werden. Sonstige Optionen auf Schlüsselhinterlegung werden mit dem Kunden individuell vereinbart.

Class 3, Class 2
Signaturschlüssel von EE-Zertifikaten werden nicht hinterlegt.

Class 3 EV-Zertifikate
Schlüssel zu Class 3 EV-Zertifikaten werden 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).

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 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 das Ziehen der Karte aus dem Kartenleser bzw. das Deaktivieren oder Löschen des Soft-PSEs.

Eine dauerhafte Deaktivierung der privaten EE-Schlüssel auf Chipkarten erfolgt, wenn die PIN-Eingabe aufeinander folgend mehrfach fehlerhaft ist. Die Anzahl der Reaktivierungsvorgänge der Karte durch Eingabe der PUK ist begrenzt. Mehrfachsignaturkarten verfügen nicht über eine PUK.

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

Wird der Chip der Karte zerstört oder werden die Dateien, die den privaten EE-Schlüssel enthalten, gelöscht, so ist der private Schlüssel zerstört. Die Zerstörung beim ZDA hinterlegter Schlüssel (nach Abschnitt 4.12.1) kann beantragt werden.

6.2.11 Beurteilung kryptographischer Module

Der ZDA 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

Class 3, Class 2
61 Monate (SSL-Zertifikate maximal 39 Monate),

Class 3 EV-Zertifikate
27 Monate,

Class 2 LCP
60 Monate

Class 1
15 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.

Zertifikatnehmer: Wird das Schlüsselpaar vom Zertifikatnehmer erzeugt, wird das Aktivierungsgeheimis bei dieser Prozedur ebenfalls produziert und steht dem Zertifikatnehmer somit zur Verfügung. Erzeugt der ZDA 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: Beim Transport-PIN-Verfahren ist die Unversehrtheit der Karte über die Transport-PIN erkennbar. In anderen Verfahren werden die PINs einmalig in einen besonders gesicherten PIN-Brief gedruckt und an den Zertifikatnehmer versandt oder übergeben.

6.4.3 Andere Aspekte von Aktivierungsdaten

Produktspezifisch wird Zertifikatnehmern mit Signaturkarte zusätzlich zu der PIN eine Personal Unblocking Key-Nummer (PUK) zum Entsperren der Signaturkarte (nach dreimaliger Fehleingabe der PIN) angeboten. Mehrfachsignaturkarten verfügen nicht über eine PUK.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom ZDA eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die nicht im Widerspruch zu [CP] und [ETSI-F] und im Fall von Class 3 EV-Zertifikaten zu [GL-BRO] stehen.

Die Computersicherheit des ZDA 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 die von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle TÜV Informationstechnik GmbH geprüft.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Bei der Entwicklung aller vom ZDA oder im Auftrag des ZDA 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 ZDAs 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 ZDA-Leiter gemeldet. Um kurzfristig und koordiniert auf eventuelle sicherheitsrelevante Vorfälle reagieren zu können, definiert der ZDA 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 ZDA zuverlässig vor Schaden, Entwendung, Verlust oder Kompromittierung geschützt.

Class 3 EV
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 ZDAs D-TRUST GMBH – Netzwerkkonzept [Siko-DTR]), die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Zum Schutz der Prozesse des ZDA werden beispielsweise Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt. Der ZDA 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 ZDA geschützten Netzwerke, für den Integrität oder Vertraulichkeit sichergestellt werden muss, wird durch kryptographische Mechanismen geschützt.

Die physische Sicherheit der durch den ZDA 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 ZDA 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:

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:

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:

- SHA1 RSA mit OID 1.2.840.113549.1.1.5 (nur noch in Ausnahmefällen),
- 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.

Class 3
Zertifikate der Class 3 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].

Class 3 EV
Class 3 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

Diese Regelungen sind in der [CP] festgehalten.

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 Class 3 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.