

# Certification Practice Statement der D-TRUST-Root PKI

Version 1.2

Erscheinungsdatum  
Datum des Inkrafttretens

01.06.2009  
01.06.2009



## Vermerk zum Copyright

### **Certification Practice Statement der D-TRUST-Root PKI ©2009 D-TRUST GMBH, alle Rechte vorbehalten.**

Ohne Einschränkung der vorstehenden vorbehaltenen Rechte und über den im Folgenden gestatteten Rahmen hinaus darf kein Teil dieser Veröffentlichung auf irgend eine Weise oder mittels irgend eines Verfahrens (elektronisch, mechanisch, durch Fotokopie, Aufzeichnung oder auf sonstige Weise) ohne vorherige schriftliche Zustimmung der D-TRUST GMBH reproduziert, gespeichert oder in ein Speichersystem geladen oder übertragen werden.

Unbeschadet des Voranstehenden ist es gestattet, dieses CPS auf nicht-exklusiver, gebührenfreier Basis zu reproduzieren und zu verteilen, sofern (i) der vorstehende Copyright-Vermerk und die einleitenden Absätze an deutlicher Stelle zu Beginn jeder Kopie erscheinen und (ii) dieses Dokument wortgetreu und vollständig wiedergegeben wird, beginnend mit der Nennung der D-TRUST GMBH als Verfasser des Dokuments.

Anträge auf jede sonstige Genehmigung zur Reproduktion oder anderweitige Verwendung 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](mailto:info@d-trust.net)

## Dokumentenhistorie

| Version | Datum      | Beschreibung   |
|---------|------------|--|
| 1.0     | 18.06.2008 | Initialversion   |
| 1.1     | 01.11.2008 | <ul style="list-style-type: none"><li>- Änderung der Bedingungen zur Berechtigung zur Antragstellung bezüglich der Volljährigkeit</li><li>- Anpassung der Prüfverfahren für SSL-Zertifikate mit <i>dNSNames</i></li><li>- Generalisierung OCSP-Pfad</li><li>- Anpassung Prüfverfahren von Class-1-Zertifikaten</li><li>- Anpassungen für SSL-Zertifikate</li></ul> |
| 1.2     | 01.06.2009 | <ul style="list-style-type: none"><li>- Erweiterung Sperrgründe von Code-Signing Zertifikaten</li><li>- editorische Änderungen</li><li>- Anpassung aufgrund WebTrust Audit</li></ul>   |

## Inhaltsverzeichnis

|      |  |    |
|------|--|----|
| 1.   | Einleitung .....   | 5  |
| 1.1  | Überblick .....  | 5  |
| 1.2  | Name und Kennzeichnung des Dokuments .....   | 7  |
| 1.3  | PKI-Teilnehmer .....   | 7  |
| 1.4  | Verwendung von Zertifikaten.....   | 8  |
| 1.5  | Pflege der CP/des CPS .....  | 9  |
| 1.6  | Begriffe und Abkürzungen.....  | 9  |
| 2.   | Verantwortlichkeit für Verzeichnisse und Veröffentlichungen.....                         | 13 |
| 2.1  | Verzeichnisse .....  | 13 |
| 2.2  | Veröffentlichung von Informationen zu Zertifikaten .....                                 | 13 |
| 2.3  | Häufigkeit von Veröffentlichungen .....  | 13 |
| 2.4  | Zugriffskontrollen auf Verzeichnisse .....   | 14 |
| 3.   | Identifizierung und Authentifizierung .....  | 15 |
| 3.1  | Namensregeln .....   | 15 |
| 3.2  | Initiale Überprüfung der Identität .....   | 17 |
| 3.3  | Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) . | 20 |
| 3.4  | Identifizierung und Authentifizierung von Sperranträgen.....                             | 20 |
| 4.   | Betriebsanforderungen .....  | 21 |
| 4.1  | Zertifikatsantrag und Registrierung .....  | 21 |
| 4.2  | Verarbeitung des Zertifikatsantrags .....  | 21 |
| 4.3  | Ausstellung von Zertifikaten .....   | 24 |
| 4.4  | Zertifikatsübergabe .....  | 25 |
| 4.5  | Verwendung des Schlüsselpaars und des Zertifikats.....                                   | 26 |
| 4.6  | Zertifikatserneuerung (certificate renewal).....   | 26 |
| 4.7  | Zertifikatserneuerung mit Schlüsselerneuerung .....                                      | 27 |
| 4.8  | Zertifikatsänderung .....  | 28 |
| 4.9  | Sperrung und Suspendierung von Zertifikaten .....  | 28 |
| 4.10 | Statusabfragedienst für Zertifikate .....  | 32 |
| 4.11 | Austritt aus dem Zertifizierungsdienst .....   | 32 |
| 4.12 | Schlüsselhinterlegung und –wiederherstellung .....                                       | 32 |
| 5.   | Nicht-technische Sicherheitsmaßnahmen .....  | 33 |
| 5.1  | Bauliche Sicherheitsmaßnahmen .....  | 33 |
| 5.2  | Verfahrensvorschriften .....   | 33 |
| 5.3  | Eingesetztes Personal.....   | 34 |
| 5.4  | Überwachungsmaßnahmen.....   | 35 |
| 5.5  | Archivierung von Aufzeichnungen.....   | 35 |
| 5.6  | Schlüsselwechsel beim ZDA.....   | 36 |
| 5.7  | Kompromittierung und Geschäftweiterführung beim ZDA.....                                 | 37 |
| 5.8  | Schließung des ZDA.....  | 38 |
| 6.   | Technische Sicherheitsmaßnahmen.....   | 39 |
| 6.1  | Erzeugung und Installation von Schlüsselpaaren.....                                      | 39 |
| 6.2  | Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module.....      | 41 |
| 6.3  | Andere Aspekte des Managements von Schlüsselpaaren.....                                  | 43 |
| 6.4  | Aktivierungsdaten .....  | 43 |
| 6.5  | Sicherheitsmaßnahmen in den Rechneranlagen .....   | 44 |
| 6.6  | Technische Maßnahmen während des Life Cycles.....  | 44 |
| 6.7  | Sicherheitsmaßnahmen für Netze .....   | 45 |
| 6.8  | Zeitstempel .....  | 45 |
| 7.   | Profile von Zertifikaten, Sperrlisten und OCSP .....                                     | 46 |
| 7.1  | Zertifikatsprofile.....  | 46 |
| 7.2  | Sperrlistenprofile.....  | 49 |
| 7.3  | Profile des Statusabfragedienstes (OCSP).....  | 49 |

|    |  |    |
|----|--|----|
| 8. | Überprüfungen und andere Bewertungen .....           | 51 |
| 9. | Sonstige finanzielle und rechtliche Regelungen ..... | 52 |
|    | Annex A Sperrgründe bei Class 3 EV-Zertifikaten..... | 53 |

## 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

Der Zertifizierungsdiensteanbieter (kurz ZDA) ist die

D-TRUST GMBH  
Kommandantenstr. 15  
10969 Berlin.

Der ZDA kann Teilaufgaben an Partner oder externe Anbieter auslagern, mit denen der ZDA ordnungsgemäß dokumentierte Vereinbarung und ein etabliertes vertragliches Verhältnis bei Bereitstellung der Dienste unterhält.

#### 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 (EA-Zertifikate). Es werden Mindestmaßnahmen konstatiert, die von allen PKI-Teilnehmern<sup>1</sup> zu erfüllen sind.

Sowohl in CA- als auch in EA-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.

---

<sup>1</sup> Im Interesse einer leichteren Lesbarkeit wird in diesem Dokument auf die weibliche Form der PKI-Teilnehmer und sonstigen genannten Personengruppen verzichtet. Es wird gebeten, die weibliche Form jeweils als eingeschlossen anzusehen.

### 1.1.3 Eigenschaften der PKI

Die Hierarchie der D-TRUST-Root-PKI ist mehrstufig. Abbildung 1 zeigt eine mögliche Konstellation der D-TRUST-Root-PKI.

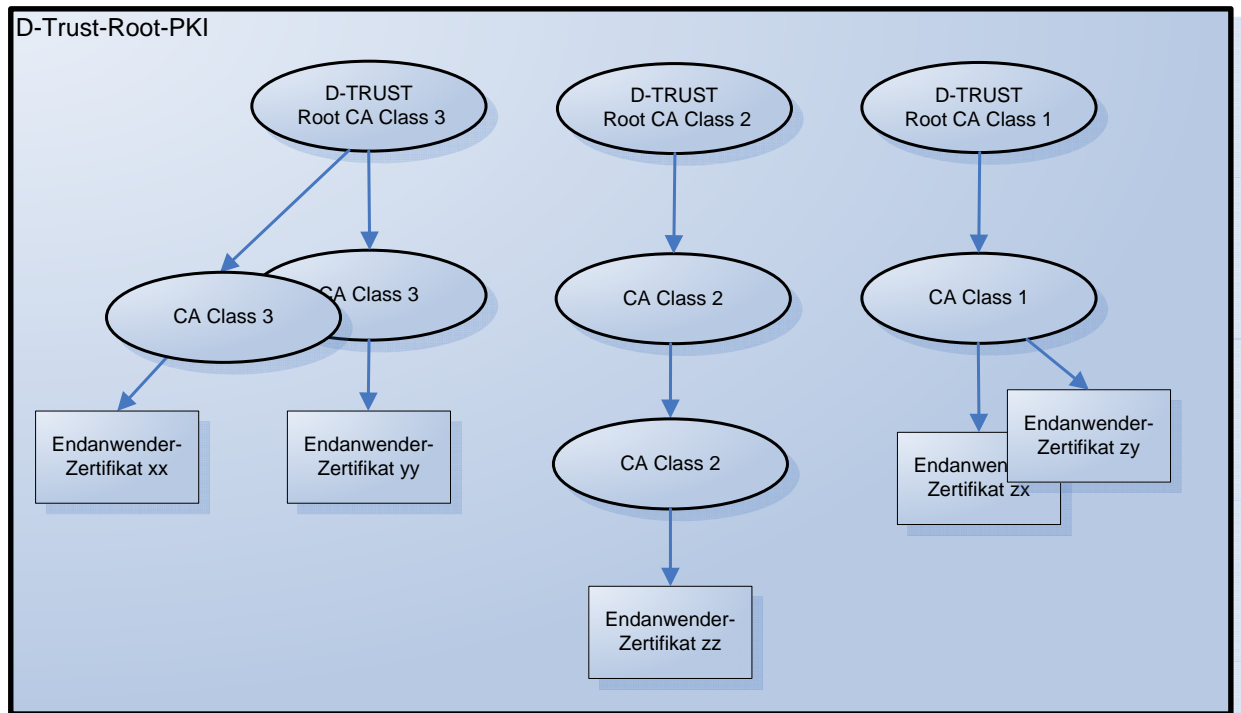


Abbildung 1 Beispielkonstellation der D-TRUST-Root-PKI

Die EA- und CA-Zertifikate lassen sich einer von drei Klassen (Class 3, Class 2 oder Class 1) zuordnen. Je höher die Klasse, desto höher ist auch die Qualität der Zertifikate, so haben Class-3-Zertifikate annähernd die Qualität qualifizierter Zertifikate gemäß [SigG]. Soweit in diesem Dokument nicht zwischen den Klassen unterschieden wird oder bestimmte Klassen explizit ausgeschlossen werden, sind die Anforderungen oder Bestimmungen der jeweiligen Abschnitte auf alle drei Klassen anwendbar.

#### Class 3

Class-3-Zertifikate sind besonders hochwertige, aber nicht qualifizierte Zertifikate, die in vielen Bereichen den Anforderungen qualifizierter Zertifikate nach [SigG] entsprechen und die Anforderungen von [ETSI-F] „NCP“ bzw. „NCP+“ erfüllen. SSL-Zertifikate werden ausschließlich für juristische Personen ausgestellt.

#### Class 3 EV-Zertifikate

Ein Sonderfall unter den Class-3-Zertifikaten sind Class 3 SSL-EV-Zertifikate. Es handelt sich um SSL-Zertifikate, die den Vorgaben der [GL-BRO] unterliegen und die Anforderungen von [ETSI-F] „EVCP“ erfüllen. Dass es sich um EV-Zertifikate handelt, ist in den EA-Zertifikaten an der EV-Policy-OID (entsprechend Abschnitt 1.2) erkennbar. Class 3 EV-Zertifikate bilden keine selbstständige Klasse. Alle für die Klasse „Class 3“ aufgeführten Erläuterungen haben für Class 3 EV-Zertifikate ebenfalls Gültigkeit, sofern Abweichungen bestehen, werden diese für Class 3 EV-Zertifikate zusätzlich aufgeführt.

#### Class 2

Class-2-Zertifikate sind hochwertige, nicht qualifizierte Zertifikate, die die Anforderungen von [ETSI-F] „LCP“ erfüllen.

#### Class 1

Class-1-Zertifikate sind einfache Zertifikate, bei denen der ZDA nur wenige Inhalte prüft. Class-1-Zertifikate entsprechen nicht den Anforderungen von [ETSI-F].

## 1.2 Name und Kennzeichnung des Dokuments

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

Version 1.2

## 1.3 PKI-Teilnehmer

### 1.3.1 Zertifizierungsstellen (CA)

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

- Personenzertifikate für natürliche und juristische Personen (EA-Zertifikat),
- Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EA-Zertifikat),
- Zertifizierungsinstanzen (nachgeordnete CA-Zertifikate des ZDA).

Die Wurzelinstanzen (D-TRUST Root Class 3/2/1 CA) stellen Zertifikate ausschließlich mit der Erweiterung *basicConstraints: cA=TRUE* (CA-Zertifikat) aus. Untergeordnete CAs stellen EA-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 identifiziert und authentifiziert Antrag stellende Personen, erfasst und prüft Anträge für verschiedene Zertifizierungsdienstleistungen. Der ZDA stellt geeignete Soft- und Hardware sowie Verfahrensanweisungen zur Verfügung, die für die Tätigkeit der RA bindend sind. Diese Verfahrensanweisungen beinhalten strikte Vorgaben für die Erfüllung der RA-Aufgaben und beschreiben detailliert Abläufe und Verhaltensvorgaben im Fehlerfall.

### 1.3.3 Zertifikatnehmer (ZNE)

Antragsteller sind natürliche Personen, die für sich (Antragsteller ist mit Zertifikatnehmer identisch) oder andere Zertifikatsnehmer Zertifikate beantragen.

Zertifikatnehmer sind natürliche oder juristische Personen, die EA-Zertifikate inne haben. Der Zertifikatnehmer muss nicht mit dem im Zertifikat genannten *subject* identisch sein.

Endanwender (EA, *subject*) verwenden die privaten Endanwenderschlüssel (EA-Schlüssel). Der Endanwender muss nicht mit dem Zertifikatnehmer identisch sein. Zulässige Endanwender sind:

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

#### Class 3

Class-3-Zertifikate für natürliche Personen werden nur dann ausgestellt, wenn Antragsteller, Zertifikatnehmer und Endanwender identisch sind. SSL-Zertifikate werden für juristische Personen ausgestellt.

#### Class 3 EV

EV-Zertifikate werden derzeit nicht an Einzelunternehmer ausgegeben.

#### Class 2

Class-2-Zertifikate, für natürliche Personen werden auch dann ausgestellt, wenn Antragsteller, Zertifikatnehmer und Endanwender nicht identisch sind.

#### Class 3-2 (Class 3 und Class 2)

Die Verantwortung für Schlüssel und Zertifikat trägt der Zertifikatnehmer. Zertifikatnehmer nehmen diverse Pflichten wahr. Bei Antragstellung muss sich der Antragsteller (als Zertifikatnehmer oder in dessen Vertretung) mit diesen Pflichten vertraut machen und zu deren Einhaltung verpflichten.

#### Class 1

In Class 1 wird nicht zwischen Antragsteller, Zertifikatnehmer und Endanwender unterschieden. Hier nimmt derjenige, der den Antrag stellt alle drei Rollen ein und trägt somit die alleinige Verantwortung für Schlüssel und Zertifikate.

### 1.3.4 Zertifikatsnutzer (ZNU)

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

## 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

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

D-TRUST GMBH  
 Redaktion CP und CPS  
 Kommandantenstr. 15  
 10969 Berlin, Germany

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

## 1.6 Begriffe und Abkürzungen

### 1.6.1 Deutsche Begriffe und Namen

|                       |  |
|-----------------------|--|
| Antragsteller         | <i>Subscriber</i> , natürliche Personen, die für sich oder andere Zertifikatnehmer Zertifikate beantragen.                             |
| CA-Zertifikat         | das für eine Zertifizierungsinstanz ausgestellte Zertifikat zum Signaturschlüssel der CA   |
| Cross-Zertifikat      | Zertifikat, das verwendet wird, um andere CAs für vertrauenswürdig zu bestätigen.  |
| D-TRUST Root CA       | Wurzelzertifizierungsstelle, existiert in den Classen 3-1, siehe Abschnitt 1.3.1.  |
| D-TRUST-Root-PKI      | Von der D-TRUST GMBH betriebene PKI.   |
| EA-Zertifikat         | Siehe Endanwenderzertifikat.   |
| Endanwender           | <i>Subject</i> , Endanwender verwenden die privaten Endanwenderschlüssel, müssen jedoch nicht mit dem Zertifikatnehmer identisch sein. |
| Endanwenderzertifikat | Zertifikat, das nicht zum Zertifizieren anderer Zertifikate oder CRLs verwendet werden darf.   |
| Postident Basic       | Verfahren zur Identifizierung, angeboten von der Deutschen Post AG. Siehe auch:  |
| Registrierungsstelle  | Registration Authority - (RA), Einrichtung der PKI, die die Teilnehmeridentifizierung vornimmt, siehe Abschnitt 1.3.2.                 |
| Signaturkarte         | Prozessorchipkarte, die für die Erzeugung elektronischer Signaturen und für andere PKI-Anwendungen benutzt werden kann.                |

|                                |   |
|--------------------------------|---|
| Soft-PSE                       | Software Personal Security Environment, auch Software-Token genannt, enthalten das EA-Schlüsselpaar, das EA-Zertifikat sowie das Zertifikat der ausstellenden CA-Instanz. |
| Sperrberechtigter (Dritter)    | Natürliche oder juristische Person, die zur Sperrung eines Zertifikats berechtigt ist.  |
| Statusabfragedienst            | PKI-Dienstleistung zur Online-Abfrage über den Status eines Zertifikats (OCSP)  |
| Token                          | Trägermedium für Zertifikate und Schlüsselmaterial.   |
| Trustcenter                    | Der Sicherheitsbereich in den Räumen der D-TRUST GMBH.  |
| Verzeichnisdienst              | PKI-Dienstleistung zum Online-Abrufen von Informationen, wie Zertifikaten und Sperrlisten, erfolgt i. d. R. über das LDAP-Protokoll.                                      |
| Zertifikatnehmer               | natürliche oder juristische Personen, die EA-Zertifikate inne haben, siehe Abschnitt 1.3.3.   |
| Zertifikatsnutzer              | Relying Party, natürliche oder juristische Personen, die Zertifikate nutzen, siehe Abschnitt 1.3.4.   |
| Zertifikatsrichtlinie          | Certificate Policy - (CP), siehe Abschnitt 1.1.   |
| Zertifizierungsdiensteanbieter | Anbieter von Zertifizierungsdiensten.   |
| Zertifizierungsstelle          | Certification Authority - (CA), Instanz der Root PKI, siehe Abschnitt 1.3.1.  |

## 1.6.2 Englische Begriffe

|                              |   |
|------------------------------|---|
| Certificate Policy (CP)      | Zertifikatsrichtlinie.  |
| Certification Authority (CA) | Instanz der Root PKI, siehe Abschnitt 1.3.1.  |
| Distinguished Name           | Ein aus mehreren Namensbestandteilen bestehender technischer Name, der in Zertifikaten die ausstellende CA und/oder den Zertifikatnehmer innerhalb der Root PKI eindeutig beschreibt. Der Distinguished Name ist im Standard [X.501] definiert. |
| Registration Authority (RA)  | Registrierungsstelle, Einrichtung der PKI, die die Teilnehmeridentifizierung vornimmt, siehe Abschnitt 1.3.2  |

### 1.6.3 Abkürzungen

|      |  |
|------|--|
| CA   | Certification Authority                        |
| CN   | Common Name                                    |
| CP   | Certificate Policy                             |
| CPS  | Certification Practice Statement               |
| CRL  | Certificate Revocation List                    |
| DN   | Distinguished Name                             |
| FIPS | Federal Information Processing Standard        |
| HSM  | Hardware Security Module                       |
| ISO  | International Organization for Standardization |
| LDAP | Lightweight Directory Access Protocol          |
| OCSP | Online Certificate Status Protocol             |
| OID  | Object Identifier                              |
| PIN  | Personal Identification Number                 |
| PKI  | Public Key Infrastructure                      |
| PUK  | Personal Unblocking Key                        |
| RA   | Registration Authority                         |
| RFC  | Request for Comment                            |
| SSCD | Secure Signature Creation Device               |
| SUD  | Secure User Device                             |
| URL  | Uniform Resource Locator                       |
| UTF8 | Unicode Transformation Format-8                |
| ZDA  | Zertifizierungsdiensteanbieter                 |

### 1.6.4 Referenzen

|           |  |
|-----------|--|
| [AGB]     | Allgemeine Geschäftsbedingungen der D-TRUST GmbH, D-TRUST GmbH, aktuelle Version   |
| [ALG-KAT] | Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, in der aktuellen Version |
| [Co-PKI]  | Common PKI Specification, Version 2.0 vom 20. Januar 2009  |
| [CP]      | Zertifikatsrichtlinie der D-TRUST-Root-PKI, D-TRUST GMBH, aktuelle Version   |
| [CPS]     | Certification Practice Statement der D-TRUST-Root-PKI, D-TRUST GMBH, aktuelle Version  |

- [ETSI-ALG] ETSI, Algorithms and Parameters for Secure Electronic Signatures, TS 102 176-1 V2.0.0, Nov. 2007
- [ETSI-F] ETSI, Technical Specification Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI TS 102 042 V2.1.1, May 2009
- [GL-BRO] Guidelines for Extended Validation Certificates, CA/Browser Forum, Version 1.1 April 2008
- [ISO 3166] ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions - Part 1: Country codes
- [RFC 2247] Using Domains in LDAP/X.500 Distinguished Names, January 1998
- [RFC 2560] X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, June 1999
- [RFC 3647] Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003
- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008
- [SigÄndG] Erstes Gesetz zur Änderung des Signaturgesetzes vom 04. Januar 2005 (BGBl. I S. 2)
- [SigG] Signaturgesetz (Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007, (BGBl. I S. 179)
- [SigV] Verordnung zur elektronischen Signatur vom 16. November 2001 (BGBl. I., S. 3074) , zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)
- [SiKo-DTR] Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GMBH
- [WebTrustEV] WEBTRUST<sup>SM/TM</sup> for Certification Authorities – Extended Validation Audit Criteria, Canadian Institute of Chartered Accountants (Version 1.1, 2008)
- [WebTrustCA] WebTrust CA - WebTrust Program for Certification Authorities (Version 1.0; August 25, 2000)
- [X.501] ITU-T RECOMMENDATION X.501, Information technology – Open Systems Interconnection – The Directory: Models, Version August 2005
- [X.509] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997

## 2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

### 2.1 Verzeichnisse

Der ZDA veröffentlicht CRLs und Zertifikate im LDAP-Verzeichnis unter:  
ldap://directory.d-trust.net

Der vollständige zertifikatsspezifische Link ist dem Zertifikat selbst zu entnehmen.

Der ZDA stellt einen Online-Dienst (OCSP) zur Abfrage des Sperrstatus von Zertifikaten der D-TRUST-Root-PKI zur Verfügung. Der Link ist dem Zertifikat zu entnehmen.

Der Status der Zertifikate kann dort bis mindestens ein Jahr nach Ablauf der Gültigkeit der Zertifikate abgerufen werden.

Die [CP], dieses CPS und die Verpflichtungserklärung (Subscribers Obligation) können im PDF-Format von den Webseiten des ZDA herunter geladen werden (<http://www.d-trust.net/repository>).

### 2.2 Veröffentlichung von Informationen zu Zertifikaten

Der ZDA veröffentlicht folgende Informationen zur D-TRUST-Root-PKI:

- EA-Zertifikate, so dies vom Antragsteller gewünscht wurde,
- CA-Zertifikate (Trust-Anchor),
- Sperrlisten (CRLs) und Statusinformationen,
- dieses CPS,
- die [CP],
- Cross-Zertifikate.

### 2.3 Häufigkeit von Veröffentlichungen

EA-Zertifikate werden veröffentlicht, falls dies vom Antragsteller so beantragt wurde. Veröffentlichte EA-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für ein weiteres Jahr und bis zum Jahresende abrufbar.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und:

- mindestens 5 Jahre (Class 3) bzw.
- mindestens 1 Jahr (Class 1 und 2)

nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig und bis zum Ende der Gültigkeit des ausstellenden CA-Zertifikats ausgestellt. Sperrlisten werden unmittelbar nach Sperrungen erstellt und veröffentlicht. Auch wenn keine Sperrungen erfolgen, stellt der ZDA täglich Sperrlisten aus. Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vorgehalten.

Die [CP] und dieses CPS werden – wie unter Abschnitt 2.1 genannt – veröffentlicht und bleiben dort mindestens so lange abrufbar, wie Zertifikate, die auf Basis dieser CP ausgestellt wurden, gültig sind. Die Verfügbarkeit beträgt 99,5%.

## **2.4 Zugriffskontrollen auf Verzeichnisse**

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

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

### 3. Identifizierung und Authentifizierung

#### 3.1 Namensregeln

##### 3.1.1 Arten von Namen

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

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

##### 3.1.2 Notwendigkeit für aussagefähige Namen

Class 3-2

*DistinguishedNames* sind stets eindeutig und sind immer demselben Zertifikatnehmer zugeordnet.

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

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

##### 3.1.3 Anonymität oder Pseudonyme von Zertifikatnehmern

Diese Regelungen sind in der [CP] festgehalten.

##### 3.1.4 Regeln für die Interpretation verschiedener Namensformen

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

| DN-Bestandteil | Interpretation  |
|----------------|---|
| G              | <i>Vorname(n)</i> der natürlichen Person entsprechend <ul style="list-style-type: none"> <li>- Class 2-3 dem zur Identifizierung vorgelegten Dokument</li> <li>- Class 1 den Angaben des Antragstellers.</li> </ul>   |
| SN             | <i>Familiennamen</i> der natürlichen Person entsprechend <ul style="list-style-type: none"> <li>- Class 2-3 dem zur Identifizierung vorgelegten Dokument</li> <li>- Class 1 den Angaben des Antragstellers.</li> </ul> Bei der Verwendung von Pseudonymen entspricht der SN dem CN. |

| DN-Bestandteil                                       | Interpretation   |
|--|--|
| CN   | <p><i>Gebräuchlicher Name:</i> Folgende Varianten werden verwendet:</p> <ul style="list-style-type: none"> <li>- Natürlichen Personen ohne Pseudonym: „Familiename, Rufname“.</li> <li>- Natürliche Personen mit Pseudonym: „Pseudonym:PN“.</li> <li>- Juristischen Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.<br/>Sonderfall: ein oder mehrere Domainnamen können ebenfalls in den CN aufgenommen werden. Wildcards sind nicht zulässig bei EV-Zertifikaten.</li> <li>- Funktion oder Personengruppe: Name der Funktion oder Personengruppe mit dem vorangestellten Abkürzung „GRP:“ als Hinweis, dass es sich um ein Gruppenzertifikat handelt</li> <li>- Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.</li> </ul> |
| PN   | <i>Pseudonym:</i> ist identisch zu CN.   |
| serialNumber   | <p><i>Seriennummer:</i> Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer).<br/>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</p>  |
| O  | Offizielle Bezeichnung der <i>Organisation</i> , 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   | <i>Organisationseinheit</i> (Abteilung, Bereich oder andere Unterteilung) der Organisation.  |
| C  | Das aufzuführende <i>Land</i> wird gemäß [ISO 3166] notiert und ergibt sich wie folgt: Ist eine Organisation O im DistinguishedName aufgeführt, 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 <i>Titel</i> oder Grad kann aufgenommen werden.  |
| Street   | Postalische Adresse <i>Straße</i>  |
| Locality   | Postalische Adresse <i>Ort</i>   |
| State  | Postalische Adresse ( <i>Bundes-</i> ) <i>Land</i>   |
| PostalCode   | Postalische Adresse <i>Postleitzahl</i>  |
| BusinessCategory                                     | Business Category (2.5.4.15) gemäß [GL-BRO]  |
| Jurisdiction Of Incorporation Locality               | Gerichtsstand der Organisation gemäß [GL-BRO]: <i>Ort</i> (1.3.6.1.4.1.311.60.2.1.1)   |
| Jurisdiction Of Incorporation State Or Province Name | Gerichtsstand der Organisation: ( <i>Bundes-</i> ) <i>Land</i> (1.3.6.1.4.1.311.60.2.1.2)  |

| DN-Bestandteil                                  | Interpretation   |
|---|--|
| Jurisdiction<br>Of Incorporation<br>CountryName | Gerichtsstand der Organisation gemäß [GL-BRO]: <i>Land</i><br>(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 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.

|                | Class 3   | Class 2   | Class 1   |
|----------------|---|---|---|
| CN             | Register/   | Register/   | Register/   |
| O              | Non-Register/   | Non-Register/   | Domain  |
| C              | Domain <sup>2</sup>                                   | Domain <sup>3</sup>                                   |   |
| OU             | Z-Bestätigung/  | A-Bestätigung/  | Keine Prüfung   |
| STREET         | Register/   | Register/   |   |
| L              | Non-Register  | Non-Register/   |   |
| State          |   | out-of-band-  |   |
| PostalCode     |   | Mechanismen/  |   |
|                | Domain  | Domain  |   |
| E-Mail-Adresse | Keine Prüfung<br>(Bestätigung durch<br>Antragsteller) | Keine Prüfung<br>(Bestätigung durch<br>Antragsteller) | Keine Prüfung<br>(Bestätigung durch<br>Antragsteller) |

<sup>2</sup> Zusätzliche Prüfung des Domainnamens im CN gemäß Abschnitt 4.2.1

<sup>3</sup> Zusätzliche Prüfung des Domainnamens im CN gemäß Abschnitt 4.2.1

|                                      | Class 3  | Class 2   | Class 1       |
|--------------------------------------|--|---|---------------|
| Alle weiteren Attribute <sup>4</sup> | Z-Bestätigung/ 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 Authentifizierung natürlicher Personen

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

#### Class 2

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

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 1       |
|---------------------------------|-----------------------|---|---------------|
| G                               | Pers-Ident            | HR-DB/<br>Dok-Ident/<br>Z-Bestätigung/<br>A-Bestätigung/<br>Körperschaften/ out-of-band-Mechanismen | Keine Prüfung |
| SN                              |                       |   |               |
| CN                              |                       |   |               |
| C                               |                       |   |               |
| STREET                          |                       |   |               |
| L                               |                       |   |               |
| S                               |                       |   |               |
| PostalCode                      |                       |   |               |
| Titel                           | Pers-Ident/ Dok-Ident |   |               |
| O (Organisationszugehörigkeit)  | Z-Bestätigung         | A-Bestätigung/<br>Z-Bestätigung/<br>Körperschaften/ out-of-band-Mechanismen/<br>HR-DB               |               |
| OU (Organisationszugehörigkeit) |                       |   |               |

<sup>4</sup> Für Class 3 EV-Zertifikate gelten die Richtlinien [GL-BRO].

|                                      | Class 3   | Class 2  | Class 1       |
|--------------------------------------|---|--|---------------|
| E-Mail-Adresse                       | Keine Prüfung<br>(Bestätigung durch<br>Antragsteller)                           | Keine Prüfung<br>(Bestätigung durch<br>Antragsteller)                  | E-Mail        |
| Alle weiteren Attribute <sup>5</sup> | Z-Bestätigung/ A-<br>Bestätigung/ Dok-<br>Ident/<br>out-of-band-<br>Mechanismen | A-Bestätigung/ Dok-<br>Ident/<br>out-of-band-<br>Mechanismen/<br>HR-DB | Keine Prüfung |

Bei Antrag auf Zertifikate für Gruppen, Funktionen oder IT-Prozesse, werden alle in der Tabelle aufgeführten Attribute zum Antragsteller (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

Die Angaben des Antragstellers werden entsprechend den Abschnitten 3.2.2, 3.2.3 und 4.2.1 Klassen-spezifisch geprüft bzw. nicht geprüft. Bei *Alternativen Namen* werden generell nur die E-Mail-Adressen geprüft. Andere alternative Namen wie Adressen beispielsweise LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (*AdditionalInformation, monetaryLimit, etc.*) werden nicht auf Korrektheit geprüft (siehe hierzu auch Abschnitt 4.9.1). Eine Ausnahme bilden hierbei Class 3-2-SSL-Zertifikate, bei denen der *Alternative Name* für die Aufnahme weiterer URLs genutzt wird. In diesen Fällen werden auch dNSNames geprüft.

### 3.2.5 Prüfung der Berechtigung zur Antragstellung

Class 3 – 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.

<sup>5</sup> Für Class 3 EV-Zertifikate gelten die Richtlinien [GL-BRO].

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

Eine Schlüsselerneuerung ist gleichbedeutend mit der erneuten Produktion von Zertifikaten ggf. Token und Schlüsseln für denselben Antragsteller. Schlüsselerneuerungen werden nur für Class 3-2, aber **nicht** für Class 1 und Class 3 EV-Zertifikate angeboten. Bei Class 3 EV-Zertifikate muss der gesamte Identifizierungs- und Registrierungsprozess wie bei einem Erstantrag durchlaufen werden, ggf. können aber bereits vorliegende Nachweisdokumente wiederverwendet werden, wenn sie nach Abschnitt D 8 (b) [GL-BRO] noch verwertbar sind (Gültigkeit ein Jahr).

#### 3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

Diese Regelungen sind in der [CP] festgehalten.

#### 3.3.2 Schlüsselerneuerung nach Sperrungen

Schlüsselerneuerung nach Sperrungen erfolgen bei EA-Zertifikaten gemäß Abschnitt 3.3.1, sofern keine Zweifel an Identifizierungsdaten bestehen und ggf. die Organisationszugehörigkeit nicht widerrufen wurde.

### 3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

- Class 3-1 (Class 3, Classe 2 und Class 1)  
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 3-2  
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 3-2  
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 Antragsteller 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 3-2

Dem Antragsteller liegen vor Beginn des Registrierungsprozesses CP, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Antragsteller bei Antragstellung verpflichten muss. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [ETSI-F]. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Antragstellers 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 E 12 [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 (Personalausweis, Reisepass oder Dokumente mit vergleichbarer Sicherheit) persönlich identifizieren und authentifizieren lassen. Zulässige Dokumente sind Personalausweis oder Reisepass bei Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes, oder Dokumenten mit gleichwertiger Sicherheit. Elektronische oder papierbasierte Kopien des Ausweisdokuments 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-, Ernennungsurkunden sowie Dokumente vergleichbaren

Ranges. Elektronische oder papierbasierte Kopien des Ausweisdokuments 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. Elektronische oder papierbasierte Kopien der Nachweise werden hinterlegt.

### **Non-Register**

Staatliche Einrichtungen/öffentlich-rechtliche Institutionen bestätigen zertifikatsrelevante Informationen mit Dienstsiegel und Unterschrift. Elektronische oder papierbasierte Kopien der Nachweise werden hinterlegt.

### **HR-DB**

Der ZDA schließt vertragliche Vereinbarungen mit einer Organisation und vereinbart, dass nur Daten übermittelt werden, die die Vorgaben der [CP] erfüllen. Ein autorisierter Mitarbeiter oder Funktionsträger einer Organisation übermittelt dem ZDA über einen sicheren Kommunikationskanal einen Auszug aus der Personaldatenbank (Human-Resource DB) der Organisation bzw. Antragsformulare, die auf Basis dieser Daten entstanden sind. Die anwendbaren Datenschutzerfordernisse sind seitens der Organisation zu beachten. Der ZDA vertraut auf die Richtigkeit und Eindeutigkeit der übermittelten Daten. Gleiches gilt für an den ZDA gestellte Zertifikats-Requests. Spätestens bei Übergabe der Token erklären Antragsteller oder Zertifikatsnehmer die Anerkennung ihrer Pflichten nach Abschnitt 9.6.3. Es werden

- 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 Antragsteller bzw. Zertifikatsnehmer ihre Pflichten nach Abschnitt 9.6.3 [CP] anerkennen
- hinterlegt.

### **Z-Bestätigung**

Ein Zeichnungsberechtigter der Organisation bestätigt zertifikatsrelevante Informationen. Dies geschieht schriftlich, in Einzelfällen können elektronisch signierte Bestätigungen akzeptiert werden. Die Zeichnungsberechtigung muss entweder aus dem Existenznachweis für die Organisation ersichtlich sein oder anderweitig nachgewiesen werden. Elektronische oder papierbasierte Kopien der Nachweise werden hinterlegt.

### **A-Bestätigung**

Autorisierte Mitarbeiter oder Funktionsträger innerhalb einer Organisation oder vertrauenswürdige Dritte (z. B. Partner des ZDA oder staatliche Institutionen, wie IHK) bestätigen bestimmte zertifikatsrelevante Informationen, die in ihrer Bestätigungskompetenz liegen. Dies geschieht schriftlich, in Einzelfällen können elektronisch signierte Bestäti-

gungen akzeptiert werden. Elektronische oder papierbasierte Kopien der 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 Antragsteller 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 Antragsteller versendet werden, die Unterschrift auf dem Rückschein wird mit der Unterschrift auf der Passkopie oder den Antragsunterlagen verglichen.

Die Organisationszugehörigkeit des Antragstellers kann ebenfalls mittels Testpost per "Einschreiben mit Rückschein" an die Organisation zu Händen des Antragstellers 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 geprüft. Class 3-2: Die Ergebnisse der Abfrage werden hinterlegt. Nicht registrierungspflichtige Domainnamen (keine Top-Level-Domain) werden nicht geprüft. Der Zertifikatsnehmer ist verpflichtet diese nur intern zu verwenden.

### **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 Antragstellers 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 Antragsteller nicht zeitnah und restlos ausräumt, wird der Antrag abgelehnt.

Class 3-2

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.

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

#### **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**

Nach der positiven Prüfung des Antrags/Requests werden im Hochsicherheitsbereich des Trustcenters die entsprechenden Zertifikate ausgefertigt. Eine vom ZDA beauftragte Person der laut Sicherheitskonzept entsprechenden Rolle stellt gemäß der Verfahrensanweisung diese Zertifikate aus.

Die vollständigen Antragsunterlagen werden entweder vom ZDA gemäß Abschnitt 5.5 abgelegt oder der ZDA schließt vertragliche Vereinbarungen mit Partnern (z. B. Körperschaften, siehe Abschnitt 4.2.1), dass die Antragsunterlagen und/oder Requests sicher und vollständig bis zum Ablauf der Frist nach Abschnitt 5.5.2 zu verwahren sind.

#### **4.3.2 Benachrichtigung des Zertifikatnehmers über die Ausstellung des Zertifikats**

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

## 4.4 Zertifikatsübergabe

### 4.4.1 Verhalten bei der Zertifikatsübergabe

#### Class 3-2

Chipkarten werden (analog zu Verfahren, die bei qualifizierten Signaturkarten eingesetzt werden) entweder an die angegebene Adresse per Briefdienstleister oder Kurier versendet oder persönlich durch die RA oder einen autorisierten Mitarbeiter oder Funktionsträger innerhalb einer Organisation an den Antragsteller ausgehändigt. Soft-PSEs werden je nach Wunsch des Antragstellers auf einem Speichermedium (mit der Post an die im Antrag benannte Adresse) versandt, zum zugriffsgeschützten und SSL-verschlüsselten Download bereitgestellt oder per E-Mail gesendet (die PKCS#12-Datei ist mit einer PIN von mindestens 8 Stellen – Ziffern und Buchstaben – geschützt). Wird ein Zertifikat zu einem beim Antragsteller vorhandenen Schlüsselpaar ausgestellt, wird das Zertifikat entweder zum Download bereitgestellt (z. B. im Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

#### Class 1

Chipkarten werden entweder an die angegebene Adresse per Briefdienstleister der Kurier versendet oder persönlich durch die RA an den Antragsteller ausgehändigt. Soft-PSEs werden entweder zum zugriffsgeschützten und SSL-verschlüsselten Download bereitgestellt oder per E-Mail gesendet (die PKCS#12-Datei ist mit einer PIN von mindestens 8 Stellen – Ziffern und Buchstaben – geschützt). Wird ein Zertifikat zu einem vorhandenen Schlüsselpaar ausgestellt, wird es entweder zum Download bereitgestellt (z. B. im Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

Erhält der ZDA Reklamationen, über die Funktion der Schlüssel und Token wird der Ursache nachgegangen. Zurückgesendete Chipkarten werden überprüft.

Bestätigt sich die Vermutung des Zertifikatnehmers bzw. wird der Verdacht nicht ausgeräumt, werden die Zertifikate gesperrt.

### 4.4.2 Veröffentlichung des Zertifikats durch den ZDA

Hat der Antragsteller im Zertifikatsantrag der Veröffentlichung der Zertifikate zugestimmt, werden die Zertifikate nach der Produktion<sup>6</sup> online über das Protokoll LDAP zur Verfügung gestellt. Hat der Antragsteller die Veröffentlichung abgelehnt, wird das Zertifikat nicht veröffentlicht.

### 4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Diese Regelungen sind in der [CP] festgehalten.

---

<sup>6</sup> Sind auf dem Token zusätzlich zu den fortgeschrittenen Zertifikaten der Root-PKI weitere Endnutzerzertifikate (qualifizierte oder qualifizierte mit Anbieterakkreditierung), erfolgt die Freischaltung gemäß den für diese Zertifikate vorgeschriebenen Verfahren.

## **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)**

Eine Zertifikatserneuerung ist die erneute Ausstellung eines Zertifikats, das auf den Inhaltsdaten und Schlüsseln des ursprünglichen Zertifikats beruht und dessen Gültigkeitszeitraum verändert wird. Bei einem Antrag auf Zertifikatserneuerung können grundsätzlich alle Felder verändert werden. Nachweise sind entsprechend beizufügen. Für die erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle CP. Eine Zertifikatserneuerung wird ausschließlich zu EA-Schlüsseln, die sich auf Chipkarten befinden durchgeführt.

Bei CA-Schlüsseln wird generell keine Zertifikatserneuerung durchgeführt.

### **4.6.1 Bedingungen für eine Zertifikatserneuerung**

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

Diese 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 3-2

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, produziert die entsprechende Rolle neue Zertifikate.

Class 1

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

### **4.6.4 Benachrichtigung des Antragstellers 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**

Im Rahmen der Zertifikatserneuerung liegt das Schlüsselpaar dem Zertifikatnehmer bereits vor. Das erzeugte Zertifikat wird entweder analog zu Verfahren, die bei qualifizierten Signaturkarten Anwendung finden, über eine sichere Datenverbindung auf die Chipkarte geschrieben oder über den LDAP-Verzeichnisdienst zur Verfügung gestellt. Weiterhin gelten die in Abschnitt 4.4.1 festgelegten anwendbaren Regelungen.

#### **4.6.6 Veröffentlichung der Zertifikatserneuerung durch den ZDA**

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

#### **4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats**

Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

### **4.7 Zertifikatserneuerung mit Schlüsselerneuerung**

Eine Schlüsselerneuerung ist die erneute Ausstellung eines Zertifikats, das auf den Inhaltsdaten des ursprünglichen Zertifikats beruht, für das aber neue Schlüssel verwendet werden und dessen Gültigkeitszeitraum verändert wird. Bei einem Antrag auf Schlüsselerneuerung können grundsätzlich alle Felder verändert werden. Nachweise sind entsprechend beizufügen. Eine Ausnahme bilden Personenzertifikate ohne Pseudonym, bei denen das Feld CN des Distinguished Names unverändert bleiben muss, siehe Abschnitt 3.1.1. Für die erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle CP. Schlüsselerneuerungen werden nur für Class 3-2 angeboten. Bei CA-Schlüsseln kann unabhängig von der Klasseneinstufung eine Schlüsselerneuerung durchgeführt werden, sofern diese nicht gesperrt sind.

Class 3 EV-Zertifikate

Zertifikatserneuerung mit Schlüsselerneuerung wird für EV-Zertifikate nicht angeboten. Für Class 3 EV-Zertifikate gelten die Vorgaben aus Abschnitt D 8.3 und F 25 [GL-BRO].

#### **4.7.1 Bedingungen für Zertifikate mit Schlüsselerneuerung**

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

Diese 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 3-2

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, produziert die entsprechende Rolle neue Zertifikate.

#### 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**

Es gelten die in Abschnitt 4.3.2 festgelegten Regelungen.

### **4.7.5 Verhalten für die Ausgabe von Zertifikaten nach Schlüsselerneuerungen**

Es gelten die in Abschnitt 4.4.1 festgelegten Regelungen.

### **4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen durch den ZDA**

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen. Der Antragsteller kann seine Entscheidung zur Veröffentlichung ändern.

### **4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats**

Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

## **4.8 Zertifikatsänderung**

Zertifikatsänderungen werden nicht angeboten.

## **4.9 Sperrung und Suspendierung von Zertifikaten**

### **4.9.1 Bedingungen für eine Sperrung**

Die 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 28 [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 28 (b) [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](mailto: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

Ein Sperrantrag kann grundsätzlich per Briefpost eingereicht werden. Soweit ein Sperrpasswort vereinbart wurde, können Sperrberechtigte Sperranträge per E-Mail oder telefonisch an bundeseinheitlichen Arbeitstagen in der Zeit von 9 - 17 Uhr stellen.

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

E-Mail-Adresse: sperren@d-trust.net

Anschrift für Sperranträge: D-TRUST GMBH  
Kommandantenstr. 15  
10969 Berlin

##### Class 3 EV-Zertifikate

Soweit ein Sperrpasswort vereinbart wurde, können Sperrberechtigte telefonisch sperren, an 24 Stunden am Tag und 7 Tagen der Woche.

Sperrnummer: +49 (0)30 / 25 93 91 – 601

Andere Sperrverfahren können vereinbart werden.

Ein Antrag zur Sperrung eines Zertifikats muss folgende Angaben enthalten:

- Name des Sperrantragstellers,
- Name des Zertifikatnehmers,
- Subject-/Antragsteller-Seriennummer (im Falle von EV Zertifikaten die Registernummer),
- Zertifikatsseriennummer (wenn möglich als Dezimalzahl), damit das Zertifikat eindeutig identifiziert werden kann.

Sperrungen finden im Verantwortungsbereich des ZDA statt. Ungeachtet dessen kann der ZDA Teilaufgaben an vertraglich gebundene Dritte weiter geben. Die Sperrdienstleistung kann von Dritten übernommen werden, die nach den Maßgaben des ZDA handeln. Der ZDA stellt geeignete Soft- und Hardware sowie Verfahrensanweisungen zur Verfügung. Die Verfahrensanweisungen beinhalten strikte Vorgaben für die Erfüllung der Sperrdienstleistung und beschreiben detailliert Abläufe und Verhaltensvorgaben im Fehlerfall.

Die vom Sperrantragsteller angegebenen Sperrgründe werden dokumentiert. Nach erfolgter Sperrung wird der Zertifikatsnehmer bzw. der Antragsteller über die Sperrung informiert.

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

#### **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**

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

Class 3 EV-Zertifikate

Die Sperrung erfolgt umgehend nach erfolgreicher Authorisierung des Sperrantragstellers per Telefon.

#### **4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen**

Aktuelle Sperrinformationen werden in Sperrlisten vorgehalten, die über das Protokoll LDAP oder über den in Abschnitt 2.1 angegebenen Link abgerufen werden können. Zusätzlich steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieser Dienste wird in Form von URLs in den Zertifikaten angegeben. Ferner können Sperrinformationen über die Webseite des ZDA (siehe Abschnitt 2.1) bezogen werden. Delta-CRLs werden nicht genutzt.

Integrität und Authentizität der Sperrinformationen wird 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 OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieses Dienstes wird in Form eines URL in den Zertifikaten angegeben.

#### **4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen**

Diese Regelungen sind in der [CP] festgehalten.

#### **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 wird nicht angeboten.

### **4.10 Statusabfragedienst für Zertifikate**

#### **4.10.1 Funktionsweise des Statusabfragedienstes**

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

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

#### **4.10.2 Verfügbarkeit des Statusabfragedienstes**

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

#### **4.10.3 Optionale Leistungen**

keine

### **4.11 Austritt aus dem Zertifizierungsdienst**

Diese Regelungen sind in der [CP] festgehalten.

### **4.12 Schlüsselhinterlegung und –wiederherstellung**

Das Hinterlegen privater EA-Schlüssel kann beantragt werden.

Class 3-2

Signatur Schlüssel von EA-Zertifikaten werden nicht hinterlegt.

Class 3 EV-Zertifikate

Schlüssel zu Class 3 EV-Zertifikaten werden nicht hinterlegt.

#### **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**

Sitzungsschlüssel werden nicht angeboten.

## 5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die CAs Class 3-2, 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“ 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 einen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

Die CAs der 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.

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 H 29 [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 Sicherheitskonzeptes 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.

## 5.5.2 Aufbewahrungsfristen für archivierte Daten

### Class 3-2

Dokumente zur Antragstellung und Prüfung sowie die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden mindestens fünf Jahre und bis zum Jahresende aufbewahrt<sup>7</sup>. Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

### Class 3 EV-Zertifikate

Dokumente zur Antragstellung und Prüfung sowie die Zertifikate selbst werden mindestens sieben Jahre und bis zum Jahresende aufbewahrt. 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 erfolgt 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.

## 5.6 Schlüsselwechsel beim ZDA

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

---

<sup>7</sup> 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.

## **5.7 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 bzw. Antragsteller 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 Disaster**

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 EA-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 3-2, 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 3-2 und deren Sub-CAs) und
- Endanwenderzertifikate (EA-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.

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

Class 3-2

Werden EA-Schlüssel und EA-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.

#### 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 EA-Schlüsselpaare, die im Verantwortungsbereich des ZDA erzeugt werden, liegen dem ZDA vor. Zertifikatsanforderungen können von Antragstellern 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.

#### 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 Antragsteller 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 3-2

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

Für EA-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 EA-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 1024 Bit verwendet.

#### 6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

Class 3-2

CA- und EA-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG] in der aktuell gültigen Fassung entsprechen.

Class 3 EV-Zertifikate

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

Class 1

Der ZDA legt Schlüsselparameter für CA-Zertifikate und EA-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 EA-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 Extensions eingeschränkt (siehe Abschnitt 7.1.2).

## **6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module**

### **6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module**

Die vom 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 EA-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 EA-Schlüssel besteht nur im Fall von Schlüssel hinterlegung gemäß Abschnitt 6.2.3.

### **6.2.3 Hinterlegung privater Schlüssel (key escrow)**

Private CA-Schlüssel werden nicht hinterlegt.

Das Hinterlegen privater EA-Schlüssel kann beantragt werden. Die Schlüssel werden verschlüsselt im Hochsicherheitsbereich des Trustcenters gehalten und können nur von autorisierten Personen wieder entschlüsselt werden.

Class 3-2

Signaturschlüssel von EA-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 EA-Schlüssel wird kein Backup angeboten, eine Sicherung erfolgt nur im Rahmen der Hinterlegung (key escrow).

### 6.2.5 Archivierung privater Schlüssel

Private CA- und EA-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 EA-Schlüssel aus dem kryptographischen Modul kann erfolgen, wenn der Antragsteller nachweist, dass er nach Abschnitt 4.12.1 berechtigt 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.

EA-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 EA-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 EA-Schlüssel, spätestens aber das Ziehen der Karte aus dem Kartenleser bzw. das Deaktivieren oder Löschen des Soft-PSEs.

Eine dauerhafte Deaktivierung der privaten EA-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 EA-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 EA-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 EA-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 EA-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt

Class 3-2  
5 Jahre,

Class 3 EV-Zertifikate  
27 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.

Zertifikatsnehmer: Wird das Schlüsselpaar vom Zertifikatsnehmer erzeugt, wird das Aktivierungsgeheimnis bei dieser Prozedur ebenfalls produziert und steht dem Zertifikatsnehmer 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 Zertifikatsnehmer 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.

Zertifikatsnehmer: Beim Transport-PIN-Verfahren ist die Unversehrtheit der Karte über die Transport-PIN erkennbar. Andernfalls werden die PINs einmalig in einen besonders gesicherten PIN-Brief gedruckt und an den Zertifikatsnehmer 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], [ETSI-F] und im Fall von Class 3 EV-Zertifikaten [GL-BRO] stehen.

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 re-

agieren 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 werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Änderungen an Systemen 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 relevanten Ereignisse, die den Life-Cycle der CA sowie der ausgestellten Zertifikate und generierten Schlüssel beeinflussen und werden auf langlebigen Medien revisionssicher gespeichert.

Class 3 EV

Es werden mindestens die unter I 31 (b) [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. 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  |
|-------------------------|-----------|--|
| <i>KeyUsage</i>         | 2.5.29.15 | <i>keyCertSign</i> ,<br><i>cRLSign</i>           |
| <i>BasicConstraints</i> | 2.5.29.19 | <i>Ca=TRUE</i> ,<br>( <i>pathLenConstraint</i> ) |

CA-Zertifikate können folgende *unkritische* Erweiterungen enthalten:

| Erweiterung                   | OID               | Parameter  |
|-------------------------------|-------------------|--|
| <i>AuthorityKeyIdentifier</i> | 2.5.29.35         | 160-bit SHA-1 Hash des Ausstellerschlüssels                                |
| <i>SubjectKeyIdentifier</i>   | 2.5.29.14         | 160-bit SHA-1 Hash des Subject Public Key                                  |
| <i>CRLDistributionPoints</i>  | 2.5.29.31         | Adresse der CRL-Ausgabestelle  |
| <i>AuthorityInfoAccess</i>    | 1.3.6.1.5.5.7.1.1 | <i>accessMethod=OCSP</i><br>{1.3.6.1.5.5.7.48.1},<br><i>accessLocation</i> |
| <i>certificatePolicies</i>    | 2.5.29.32         | OID zu unterstützten CPs   |
| <i>SubjectAltName</i>         | 2.5.29.17         | Alternativer Ausstellernamen   |

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

EA-Zertifikate enthalten folgende *kritische* Erweiterungen:

| <b>Erweiterung</b> | <b>OID</b> | <b>Parameter</b>  |
|--------------------|------------|---|
| <i>KeyUsage</i>    | 2.5.29.15  | Möglich sind:<br><i>digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly</i><br>und Kombinationen |

EA-Zertifikate können folgende *unkritische* Erweiterungen enthalten:

| <b>Erweiterung</b>            | <b>OID</b>        | <b>Parameter</b>  |
|-------------------------------|-------------------|---|
| <i>ExtKeyUsage</i>            | 2.5.29.37         | Entsprechend [RFC 5280]                                       |
| <i>AuthorityKeyIdentifier</i> | 2.5.29.35         | 160-bit SHA-1 Hash des Ausstellerschlüssels                   |
| <i>SubjectKeyIdentifier</i>   | 2.5.29.14         | 160-bit SHA-1 Hash des Subject Public Key                     |
| <i>CRLDistributionPoints</i>  | 2.5.29.31         | CRL-Ausgabestelle als ldap-Adresse                            |
| <i>AuthorityInfoAccess</i>    | 1.3.6.1.5.5.7.1.1 | <i>accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation</i> |
| <i>certificatePolicies</i>    | 2.5.29.32         | OID zu unterstützten CPs<br><i>cpsURI</i>                     |
| <i>SubjectAltName</i>         | 2.5.29.17         | Alternativer Ausstellername                                   |

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

### 7.1.3 Algorithmen-OIDs

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

- RSA mit OID 1.2.840.113549.1.1.1.

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

- SHA1 RSA mit OID 1.2.840.113549.1.1.5,
- 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 *Issuer-AltName* (Alternativer Ausstellername) können Namen gemäß RFC [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. Dieses CPS entspricht den Vorgaben von [ETSI-F].

##### Class 3

Zertifikate der Klasse 3 können den OID der in [ETSI-F] definierten NCP bzw. NCP+ enthalten. Unabhängig davon können weitere CPs referenziert werden.

##### Class 3 EV

Class 3 EV Zertifikate können den OID der in [ETSI-F] definierten EVCP enthalten. Unabhängig davon können weitere CPs referenziert werden.

##### Class 2

Zertifikate der Klasse 2 können den OID der in [ETSI-F] definierten LCP enthalten. Unabhängig davon können weitere CPs referenziert werden.

##### Class 1

Zertifikate der Klasse 1 enthalten keine OID nach [ETSI-F]. Weitere CPs können 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 EA-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                                   |
|-------------------------------|-----------|---|
| <i>cRLNumber</i>              | 2.5.29.20 | Nummer der Sperrliste                       |
| <i>AuthorityKeyIdentifier</i> | 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  |
|--------------------------|--|
| <i>RetrieveIfAllowed</i> | Falls gesetzt, wird Zertifikat in der Antwort mitgeliefert (optional). |

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

| Erweiterung           | Parameter   |
|-----------------------|---|
| <i>ArchiveCutoff</i>  | Zeitraum, für den der OCSP-Responder nach Ausstellung des Zertifikats die Statusinformationen bereitstellt. |
| <i>CertHash</i>       | Bei Status good oder revoked wird der SHA-1 Hash-Wert des Zertifikats eingetragen.                          |
| <i>CertInDirSince</i> | Zeitpunkt der Veröffentlichung des Zertifikats im zentralen Verzeichnisdienst.                              |

| Erweiterung                 | Parameter   |
|-----------------------------|---|
| <i>RequestedCertificate</i> | Enthält das Zertifikat, falls <i>RetrieveIfAllowed</i> gesetzt war. |

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

## 8. Überprüfungen und andere Bewertungen

Die CAs der D-TRUST-Root-PKI werden vom ZDA in den gleichen Räumen betrieben wie die CA der D-TRUST GMBH zur Ausstellung qualifizierter Zertifikate mit Anbieterakkreditierung nach deutschem Signaturgesetz. Revisionen, Revisionsgegenstände und Prozesse sind detailliert im Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GMBH [SiKo-DTR] beschrieben. Der Teil Rollenkonzept desselben Sicherheitskonzepts [SiKo-DTR] dokumentiert die Qualifikation und die Stellung des Revisors. Das Sicherheitskonzept wurde durch die TÜV Informationstechnik GmbH geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden. Des Weiteren finden im Zuge des Genehmigungsverfahrens zur freiwilligen Akkreditierung des ZDAs gemäß §15 SigG und §11 SigV regelmäßig alle drei Jahre Kontrollen durch externe Prüfer der Prüf- und Bestätigungsstelle TÜV Informationstechnik GmbH statt. Das bestätigte Vorgehen nach deutschem Signaturgesetz bescheinigt der D-TRUST GMBH einen hohen Sicherheitsstandard.

### Class 3-2

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

[CP] und CPS erfüllen für Class 3 Zertifikate die Anforderungen von „NCP“ bzw. „NCP+“, für Class 3 EV Zertifikate die Anforderungen von „EVCP“ und für Class 2 Zertifikate die Anforderungen für „LCP“ gemäß [ETSI-F]. Ein regelmäßiges Assessment durch eine „competent independent party“ gemäß TS 102 042 [ETSI-F] (Abschnitt 5.4.1) belegt die Kompatibilität.

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

### Class 3 EV-Zertifikate

Der ZDA gibt EV-Zertifikate nur dann aus, wenn durch einen nach J 35 [GL-BRO] unabhängigen externen Wirtschaftsprüfer mit WebTrust-Lizenzierung bestätigt wurde, dass die Verfahren des ZDA den Richtlinien von [GL-BRO] entsprechen. Alternativ könnte entsprechend [ETSI-F] "EVCP" eine Zertifizierung erfolgen. Sollten sich die Verfahren hernach als nicht mehr konform zu den aktuellen Richtlinien von [GL-BRO] erweisen, unterlässt der ZDA das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde. Die 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 die AGB verwiesen.

## **Annex A** Sperrgründe bei Class 3 EV-Zertifikaten

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

### **G 27 [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.*