

Zertifikatsrichtlinie der D-TRUST-Root PKI

Version 1.3

Erscheinungsdatum
Datum des Inkrafttretens

25.02.2010
01.03.2010



Vermerk zum Copyright

Zertifikatsrichtlinie der D-TRUST-Root PKI ©2010 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, diese Zertifikatsrichtlinie 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 dieser Zertifikatsrichtlinie der D-TRUST GMBH sind zu richten an:

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

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	18.06.2008	Initialversion
1.1	18.12.2008	<ul style="list-style-type: none">- Änderung der Bedingungen zur Berechtigung zur Antragstellung bezüglich der Volljährigkeit- Anpassung der Prüfverfahren für SSL-Zertifikate mit <i>dNSNames</i>- Generalisierung OCSP-Pfad- Anpassung Prüfverfahren von Class-1-Zertifikaten- Anpassungen für SSL-Zertifikate
1.3	01.06.2009	<ul style="list-style-type: none">- editorische Änderungen- Anpassung aufgrund WebTrust Audit
1.3	25.02.2010	<ul style="list-style-type: none">- Konkretisierung: für SSL-Zertifikate wird weder Zertifikatserneuerung (renewal) noch Zertifikatserneuerung mit Schlüsselerneuerung angeboten

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	10
2.	Verantwortlichkeit für Verzeichnisse und Veröffentlichungen	14
2.1	Verzeichnisse	14
2.2	Veröffentlichung von Informationen zu Zertifikaten	14
2.3	Häufigkeit von Veröffentlichungen	14
2.4	Zugriffskontrollen auf Verzeichnisse	15
3.	Identifizierung und Authentifizierung	16
3.1	Namensregeln	16
3.2	Initiale Überprüfung der Identität	17
3.3	Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)	19
3.4	Identifizierung und Authentifizierung von Sperranträgen	20
4.	Betriebsanforderungen	21
4.1	Zertifikatsantrag und Registrierung	21
4.2	Verarbeitung des Zertifikatsantrags	22
4.3	Ausstellung von Zertifikaten	23
4.4	Zertifikatsübergabe	23
4.5	Verwendung des Schlüsselpaars und des Zertifikats	24
4.6	Zertifikatserneuerung (certificate renewal)	25
4.7	Zertifikatserneuerung mit Schlüsselerneuerung	26
4.8	Zertifikatsänderung	28
4.9	Sperrung und Suspendierung von Zertifikaten	28
4.10	Statusabfragedienst für Zertifikate	31
4.11	Austritt aus dem Zertifizierungsdienst	31
4.12	Schlüsselhinterlegung und –wiederherstellung	31
5.	Nicht-technische Sicherheitsmaßnahmen	33
6.	Technische Sicherheitsmaßnahmen	34
7.	Profile von Zertifikaten, Sperrlisten und OCSP	35
7.1	Zertifikatsprofile	35
7.2	Sperrlistenprofile	35
7.3	Profile des Statusabfragedienstes (OCSP)	35
8.	Überprüfungen und andere Bewertungen	36
9.	Sonstige finanzielle und rechtliche Regelungen	37
9.1	Preise	37
9.2	Finanzielle Zuständigkeiten	37
9.3	Vertraulichkeit von Geschäftsdaten	38
9.4	Datenschutz von Personendaten	38
9.5	Gewerbliche Schutz- und Urheberrechte	39
9.6	Zusicherungen und Garantien	40
9.7	Haftungsausschlüsse	41
9.8	Haftungsbeschränkungen	41
9.9	Schadensersatz	42
9.10	Gültigkeitsdauer der CP und Beendigung der Gültigkeit	42
9.11	Individuelle Mitteilungen und Absprachen mit PKI-Teilnehmern	42
9.12	Nachträge	42
9.13	Bestimmungen zur Schlichtung von Streitfällen	43
9.14	Gerichtsstand	43

9.15	Einhaltung geltenden Rechts	43
9.16	Sonstige Bestimmungen	43
9.17	Andere Bestimmungen.....	44

1. Einleitung

1.1 Überblick

Dieses Dokument beschreibt die Zertifikatsrichtlinie (engl. *Certificate Policy*, kurz CP) der von D-TRUST GMBH betriebenen D-TRUST Root-PKI.

1.1.1 Zertifizierungsdiensteanbieter

Der Zertifizierungsdiensteanbieter (kurz ZDA) ist – auch im juristischen Sinne – 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

Diese CP stellt Vorgaben und Anforderungen an die Root-PKI und regelt somit den Zertifizierungsprozess während der gesamten Lebensdauer der Endanwenderzertifikate (EA-Zertifikate) sowie das Zusammenwirken, Rechte und Pflichten der PKI-Teilnehmer¹.

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

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

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

¹ 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.

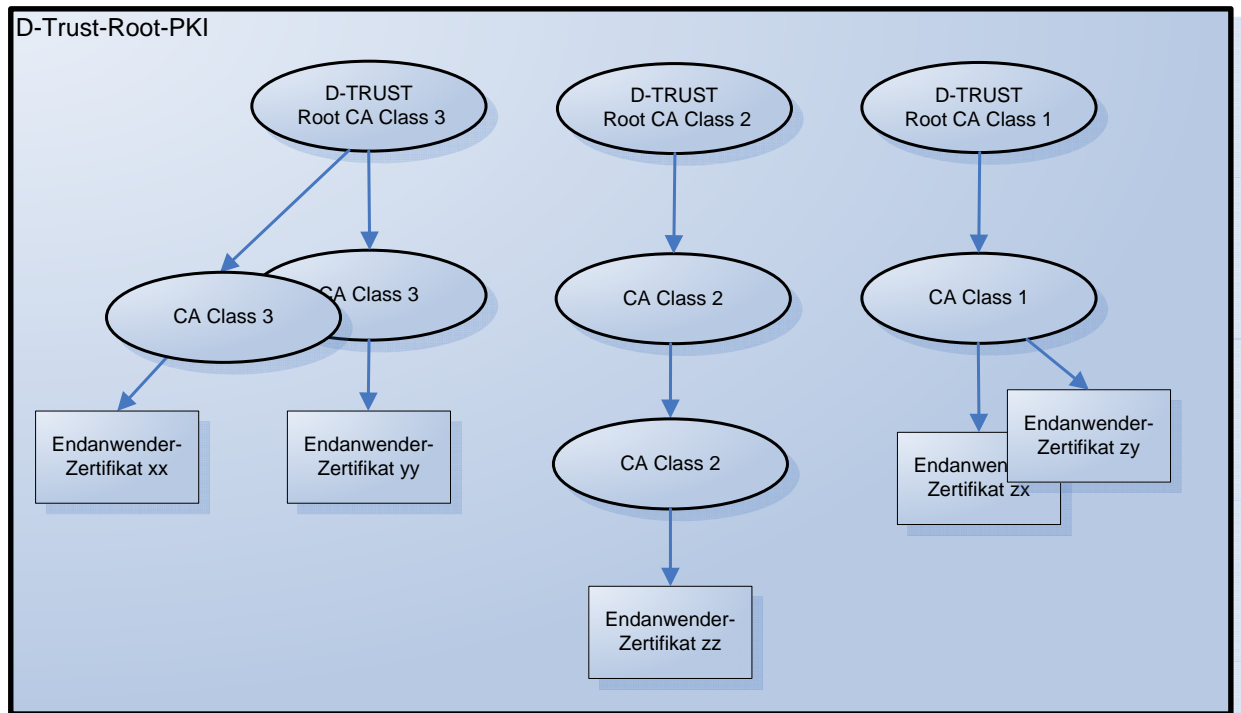


Abbildung 1 Beispielkonstellation der D-TRUST-Root-PKI

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 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 3 EV-Zertifikate

Ein Sonderfall unter den Class-3-Zertifikaten sind Class 3 SSL-EV-Zertifikate. Sie unterliegen den Vorgaben der [GL-BRO] bzw. [ETSI-F] „EVCP“. Dass es sich um EV-Zertifikate handelt, ist in den EA-Zertifikaten an der EV-Policy-OID (entsprechend Abschnitt 1.2) erkennbar.

Class 2

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

Class 1

Class-1-Zertifikate sind einfache Zertifikate, die nicht die Anforderungen von [ETSI-F] erfüllen.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname: Zertifikatsrichtlinie der D-TRUST-Root-PKI

Kennzeichnung (OID): Dieses Dokument erhält die Policy-OID:
1.3.6.1.4.1.4788.2.200.1

Für die EV-Policy-OID wird die Verwendung bei EV-Zertifikaten gemäß [GL-BRO] vergeben:
1.3.6.1.4.1.4788.2.202.1

Version 1.3

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.

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 und Einzelunternehmen),
- 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 ausschließlich für juristische Personen ausgestellt.

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 Classe 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

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

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

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

1.4.2 Verbotene Verwendungen von Zertifikaten

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

1.5 Pflege der CP/des CPS

1.5.1 Zuständigkeit für das Dokument

Diese CP 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

1.5.3 Verträglichkeit von CPs fremder CAs mit dieser CP

In dieser CP werden Mindestanforderungen beschrieben, die von allen PKI-Teilnehmern erfüllt werden müssen.

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

Für CAs, die eine in allen wesentlichen technischen und juristischen Aspekten der Dienstleistungen mindestens das gleiche Sicherheits- und Vertrauensniveau gewährende CP haben, kann der ZDA ein Cross-Zertifikat ausstellen, wodurch die Gleichwertigkeit des Standards der entsprechenden CP vom ZDA bestätigt wird. Die Crosszertifizierung wird ausschließlich durch CAs vorgenommen, die nicht ETSI-zertifiziert wurden bzw. für CAs die bereits ETSI-zertifiziert sind. Cross-Zertifikate müssen den Eintrag „path-length=1“ haben und werden im Verzeichnis des ZDA veröffentlicht (siehe Abschnitt 2.1).

Der ZDA steht für die Richtigkeit der Angaben in den Cross-Zertifikaten, die für die „fremde“ CA ausgestellt werden, sowie für die Verträglichkeit der Fremd-Policy mit die-

ser CP zum Zeitpunkt der Ausstellung des Cross-Zertifikats ein. Eine wesentliche Änderung der Fremd-Policy, welche die Verträglichkeit beeinträchtigt, zieht die Sperrung des Cross-Zertifikats durch den ZDA nach sich.

Ist eine Crosszertifizierung durch andere CAs vorgesehen, müssen diese CAs die D-TRUST GMBH unverzüglich informieren. Die D-TRUST GMBH behält sich vor, einer Aufnahme in eine Crosszertifizierung zu widersprechen.

Class 3 SSL-EV-Zertifikate, deren Sub- sowie Root-CAs kommen den Anforderungen des CA/Browser Forum Guidelines for Extended Validation Certificates [GL-BRO] nach. Im Falle von Inkonsistenzen zwischen diesem Dokument und den genannten Guidelines gelten die [GL-BRO] vorrangig, bezogen auf Class 3 SSL EV CAs sowie deren Sub- und Root CAs.

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: http://www.deutschepost.de/
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
FQDN	Fully qualified domain name

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
[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
[Co-PKI]	Common PKI Specification, Version 2.0 vom 20. Januar 2009
[ETSI-ALG]	ETSI, Algorithms and Parameters for Secure Electronic Signatures, TS 102 176-1, ETSI 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 17. Juli 2009 (BGBl. I S. 2091)
- [SigV] Verordnung zur elektronischen Signatur vom 16. November 2001 (BGBl. I., S. 3074), zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932)
- [SiKo-DTR] Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GMBH
- [WebTrustEV] WEBTRUST SM/TM for Certification Authorities – Extended Validation Audit Criteria, Canadian Institute of Chartered Accountants (1.1, 2008)
- [WebTrustCA] WebTrust CA - WebTrust Program for Certification Authorities (Version 1.0; August 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.

Zusätzlich werden CA-Zertifikate auf den Webseiten der D-TRUST GMBH veröffentlicht und können abgefragt werden unter dem URL:

<https://www.d-trust.net/internet/content/d-trust-roots.html>

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.

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

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,
- diese CP,
- das [CPS],
- Cross-Zertifikate.

2.3 Häufigkeit von Veröffentlichungen

EA-Zertifikate können veröffentlicht, d. h. in das öffentliche Verzeichnis des ZDA aufgenommen werden. Der Antragsteller kann der Veröffentlichung zustimmen oder diese ablehnen. Produktabhängig kann die Zustimmung zur Veröffentlichung Voraussetzung für die Beantragung sein. 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) und bis zum Jahresende bzw.
- mindestens 1 Jahr und bis zum Jahresende (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 sicher, dass mindestens alle 5 Tage Sperrlisten ausgestellt werden. Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vorgehalten.

Diese CP und das [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 Webseiten sind hoch verfügbar.

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

Der verwendete *DistinguishedName* des Zertifikatnehmers ist eindeutig innerhalb der D-TRUST-Root-PKI.

Class 3-2

Eine eindeutige Zuordnung des Zertifikats zum Zertifikatnehmer ist gegeben.

Bei alternativen Namen (*subjectAltName*) gibt es, mit Ausnahmen von SSL-Zertifikaten (einschließlich Class 3 EV-Zertifikate), keine Notwendigkeit für aussagefähige Namen.

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

3.1.3 Anonymität oder Pseudonyme von Zertifikatnehmern

Pseudonyme werden ausschließlich für natürliche Personen benutzt. Generell werden Pseudonyme vom ZDA vergeben. Die Freiwählbarkeit von Pseudonymen kann vereinbart werden, siehe Abschnitt 3.1.6. Der ZDA behält sich vor, die Vergabe eines Pseudonyms abzulehnen. Die Ablehnung bedarf keiner Begründung.

Class 3-2

Auch bei Zertifikaten, die mit Pseudonymen erstellt werden, wird durch den ZDA die reale Identität des Antragstellers in den Unterlagen festgehalten.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Das Verfahren für die Aufnahme bzw. Interpretation der Namen ist im [CPS] definiert.

Es müssen nicht alle dort genannten DN-Bestandteile verwendet werden. Weitere können ergänzt werden.

Class 3 EV-Zertifikate

EA-Zertifikate enthalten mindestens die *subject*-DN-Bestandteile „O“, „CN“ oder „subjectAlternativName mit der Domain“, „BusinessCategory“, „Jurisdiction of Incorporation or Registration“, „Seriennummer“, „L“, „State“ sowie „C“. Optional können die „Street“ sowie „Postal Code“ aufgenommen werden.

Class 3-2

Ergänzende DN-Bestandteile müssen [RFC 5280] und [Co-PKI] entsprechen.

3.1.5 Eindeutigkeit von Namen

Class 3-2

Der ZDA stellt sicher, dass ein in EA-Zertifikaten verwendeter Name (DistinguishedName) des Zertifikatnehmers bzw. des Endanwenders (Feld *subject*) innerhalb der D-TRUST-Root-PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatnehmer zugeordnet ist. Die Eindeutigkeit wird mittels der Seriennummer (i.d.R. Antragsnummer oder bei Class 3 EV Zertifikaten Handelsregisternummer entsprechend [GL-BRO] Abschnitt 6(a) (5)) erzielt. Dadurch ist die eindeutige Identifizierung² des Zertifikatnehmers anhand des im EA-Zertifikat verwendeten Namens (*subject*) gewährleistet.

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

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

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

Class 3 EV-Zertifikate

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

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Es werden zwei Fälle unterschieden:

1. Schlüsselpaare von Zertifikatnehmern werden im Verantwortungsbereich des ZDA produziert. Mit der Übergabe der Token und ggf. PIN-Briefe gemäß Abschnitt 4.4.1 an die Zertifikatnehmer durch den ZDA wird sichergestellt, dass die privaten Schlüssel in den Besitz der Zertifikatnehmer gelangen.
2. Schlüsselpaare werden im Verantwortungsbereich des Antragstellers produziert. Der Besitz des privaten Schlüssels muss entweder technisch nachgewiesen werden oder vom Antragsteller nachvollziehbar bestätigt werden.

² Unter Identifizierung sind hier die Benennung des Zertifikatnehmers und dessen zum Zeitpunkt der Erstantragstellung (nicht Folgeantrag) aktuellen Daten zu verstehen. Nicht gemeint ist das Eruiieren aktueller Daten oder das Auffinden des Zertifikatnehmers zu einem späteren Zeitpunkt.

3.2.2 Identifizierung und Authentifizierung von Organisationen

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

Class 3

Identifizierung und Prüfung auf hoher Stufe. Die persönliche Teilnehmeridentifizierung und die Prüfung der Antragsdaten muss, wenn anwendbar, gemäß Verfahren erfolgen, die bei der Ausstellung qualifizierter Zertifikate Anwendung finden. Für juristische Personen gelten die Vorgaben aus [ETSI-F] Die Prüfung erfasst alle DN-Bestandteile.

Class 3 EV-Zertifikate

Für Identifizierung und Authentifizierung sowie Verifizierung von Antrags- und Zertifikationsdaten gelten die Vorgaben aus [GL-BRO] (siehe [CPS]Annex A) sowie Abschnitt H 30 [GL-BRO].

Class 2

Identifizierung und Prüfung auf mittlerer Stufe. Die Teilnehmeridentifizierung und die Prüfung der Antragsdaten erfolgt mindestens auf Basis der Angaben vertrauenswürdiger Dritter (z. B. Abteilungsleiter oder Personalabteilung nach vertraglicher Vereinbarung). Die Prüfung erfasst alle DN-Bestandteile.

Class 1

Identifizierung und Prüfung auf niedriger Stufe. Nur E-Mail-Adresse und ggf. Domain-Namen und/oder Organisationsnamen werden überprüft.

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 authentisieren.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

Natürliche Personen, die Zertifikate für sich selbst oder Dritte beantragen, die im Zertifikat benannt werden, müssen sich eindeutig authentisieren und ihre Berechtigung zur Antragstellung durch die Organisation nachweisen.

Class 3

Identifizierung und Prüfung auf hoher Stufe. Die persönliche Teilnehmeridentifizierung und die Prüfung der Antragsdaten muss, wenn anwendbar, gemäß Verfahren erfolgen, die bei der Ausstellung qualifizierter Zertifikate Anwendung finden. Die Prüfung erfasst alle DN-Bestandteile. Für die Identifizierung und Authentifizierung sowie Verifizierung von Daten für SSL-Zertifikate gelten die Vorgaben aus [ETSI-F].

Class 3 EV-Zertifikate

Für Identifizierung und Authentifizierung sowie Verifizierung von Daten gelten die Vorgaben aus [GL-BRO] (siehe [CPS]Annex A) sowie Abschnitt H 30 [GL-BRO].

Class 2

Identifizierung und Prüfung auf mittlerer Stufe. Die Teilnehmeridentifizierung und die Prüfung der Antragsdaten erfolgt mindestens auf Basis der Angaben vertrauenswürdiger Dritter. Die Prüfung erfasst alle DN-Bestandteile.

Class 1

Identifizierung und Prüfung auf niedriger Stufe. Nur E-Mail-Adresse und ggf. Domain-Namen und/oder Organisationsnamen werden überprüft.

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 von Internetseiten und LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft (siehe hierzu auch Abschnitt 4.9.1).

3.2.5 Prüfung der Berechtigung zur Antragstellung

Anträge dürfen von natürlichen Personen und jurischen Personen gestellt werden. Die Verfahren sind im [CPS] definiert.

3.2.6 Kriterien für die Interoperabilität

Siehe Abschnitt 1.5.3.

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

Eine Schlüsselerneuerung ist gleichbedeutend mit der erneuten Produktion von Zertifikaten ggf. Token und Schlüsseln für denselben 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.

3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

Für die Zeit nach Ablauf der Gültigkeit von EA-Zertifikaten (Class 3-2) oder auf Wunsch des Antragstellers werden auf Anforderung neue Zertifikate und ggf. Schlüssel und Token ausgegeben. Bei rechtzeitigen Anträgen zur Schlüsselerneuerung ist keine erneute Identifizierung erforderlich. Der Auftrag zur Schlüsselerneuerung muss signiert werden:

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

Die Bedingungen des Abschnitts 4.7 müssen erfüllt werden.

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.

Hinweis: Signaturen, die mit dem Schlüssel eines gesperrten oder abgelaufenen EA-Zertifikats erstellt wurden, können nicht anerkannt werden.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der ZDA prüft vor der Sperrung eines EA-Zertifikates die Berechtigung des Sperrantragstellers zur Antragstellung. Die Verfahren sind im [CPS] definiert.

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

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

Mit Ausnahme von Anträgen auf Class-3-Zertifikate für natürliche Personen und Class-1-Zertifikate können sich Zertifikatnehmer von einem Bevollmächtigten (Antragsteller) vertreten lassen.

Gruppenzertifikate werden ausschließlich für juristische Personen und Einzelunternehmen ausgestellt.

Private EA-Schlüssel, die keine Signaturschlüssel³ oder kein Schlüssel zu Class 3 EV-Zertifikaten sind, können gemäß den Vorgaben von 6.2.3 des [CPS] für eine spätere Wiederverwendung (key escrow, Wiederverwendung in einem neuen Token) vom ZDA sicher hinterlegt werden. Der Antragsteller muss die Hinterlegung beantragen und angeben, dass der private EA-Schlüssel für denselben Zertifikatnehmer und/oder eine Personengruppe wiederverwendet werden soll. Für die Wiederverwendung der EA-Schlüssel nach 6.2.3 [CPS] muss der Antragsteller nachweisen, dass er berechtigt ist, diesen Schlüssel wieder zu verwenden.

Class 3 EV-Zertifikate

Zertifikatnehmer müssen den Anforderungen aus Abschnitt C 5 [GL-BRO] entsprechen.

CA-Zertifikate werden ausschließlich an juristische Personen ausgegeben.

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

4.1.2 Registrierungsprozess und Zuständigkeiten

Dem Antragsteller stehen bereits bei Beginn des Registrierungsprozesses CP, CPS und (bei Antragstellung auf Class 3-2-Zertifikate) eine Verpflichtungserklärung (Subscriber Agreement) sowie weitere Dokumente zur Verfügung, um ihm zu ermöglichen, sich über die Bedingungen für die Verwendung des gewählten Zertifikats zu informieren.

Die Einhaltung des Registrierungsprozesses gewährleistet der ZDA. Teilaufgabe können von Partnern oder externen Anbietern übernommen, werden, die die Maßgaben der CP erfüllen.

³ Ein Signaturschlüssel ist ein Schlüssel, zu dem ein Zertifikat erstellt wird, das den öffentlichen Schlüssel des Schlüsselpaars enthält und die Schlüsselverwendung entweder "digital signature" oder "contentCommitment" bzw. "nonRepudiation" beinhaltet.

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.

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

Class 3-2

Natürliche Personen müssen eindeutig identifiziert werden, zum vollständigen Namen müssen Attribute wie Geburtsort, Geburtsdatum, Ausweis-/Passnummer oder andere anwendbare individuelle Merkmale Verwechslungen verhindern.

Werden juristische Personen im Zertifikat benannt, oder sind sie Zertifikatnehmer müssen der vollständige Name und der rechtliche Status sowie ggf. relevante Registerinformationen geprüft werden.

Die Identifizierung findet gemäß Abschnitt 3.2.3 statt. Die anwendbaren Prüfverfahren sind in diesem Abschnitt des [CPS] definiert.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

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.

Weitere Gründe für die Antragsablehnung können sein:

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

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

Erst nachdem der ZDA den Zertifikatsantrag positiv überprüft hat und das beantragte Zertifikat und ggf. Schlüsselmaterial übergeben wurde (vgl. Abschnitt 4.4), gilt der Antrag als vorbehaltlos angenommen.

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 werden im Hochsicherheitsbereich des Trustcenters die entsprechenden Zertifikate ausgefertigt. Die vollständigen Antragsunterlagen werden archiviert.

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 oder 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 LDAP-Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

Entdeckt der Zertifikatnehmer Fehler in seinen Zertifikaten oder bei der Funktion der Schlüssel und Token, so hat er dies dem ZDA mitzuteilen. Die Zertifikate werden gesperrt. Nach erfolgter Sperrung kann der ZDA verlangen, dass Chipkarten vom Zertifikatnehmer an den ZDA zurückgesendet werden.

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

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

4.4.2 Veröffentlichung des Zertifikats durch den ZDA

Hat der Antragsteller im Zertifikatsantrag der Veröffentlichung der Zertifikate zugestimmt, werden die Zertifikate nach der Produktion⁴ online über das Protokoll LDAP zur Verfügung gestellt. Hat der Antragsteller die Veröffentlichung abgelehnt, wird das Zertifikat nicht veröffentlicht.

Der Status ist in beiden Fällen nach Produktion über CRLs und OCSP abrufbar. (siehe Abschnitt 2.1)⁵.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

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

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer

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

Class 3-2

Für Zertifikatnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

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

- die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Extentions) benutzt werden,
- die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt werden kann⁶,
- der Status der Zertifikate über den Statusabfragedienst (OCSP) positiv geprüft wurde und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche

⁴ 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.

⁵ Sind auf dem Token zusätzlich zu den fortgeschrittenen Zertifikaten der Root-PKI weitere Endnutzerzertifikate (qualifizierte oder qualifizierte mit Anbieterakkreditierung), ist der Status nach Eingang der Empfangsbestätigung beim ZDA über CRLs und OCSP abrufbar.

⁶ Die Verifikation der Zertifikatskette soll entsprechend dem PKIX-Modell (auch Schalenmodell genannt) gemäß [RFC 5280], Abschnitt 6, erfolgen. Eine formale Beschreibung des Algorithmus zur Verifikation der Zertifikatskette ist zu finden in [Co-PKI], Part 5.

anwendungsspezifische Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

Hinweis: Im Gegensatz zu qualifizierten Signaturen gilt für nicht qualifizierte Signaturen vor Gericht nicht die Beweislastumkehr, d. h. die Gültigkeit der Signatur muss mittels Gutachten bewiesen werden. Das hohe Maß an Sicherheit und Qualität der Zertifikate Class 3-2, begünstigt die Ausgangsbedingungen für die Gutachtenerstellung.

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 gültigen EA-Schlüsseln, die sich auf Chipkarten befinden durchgeführt. Für SSL- und EV-Zertifikate wird keine Zertifikatserneuerung angeboten.

Bei CA-Schlüsseln wird generell keine Zertifikatserneuerung durchgeführt.

4.6.1 Bedingungen für eine Zertifikatserneuerung

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

Class 3-2

Voraussetzung ist, dass der Beantragende mit dem Antragsteller aus dem Erstantrag identisch ist. Aus dem Unterschriften- bzw. Signaturvergleich muss die Berechtigung erkennbar sein.

Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Zertifikatserneuerung noch gültig sein. Bei schriftlicher Antragstellung kann der Antrag auch nach Ablauf der Gültigkeit des Zertifikats gestellt werden.

Class 2

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

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

Werden Zertifikatsinhalte verändert, müssen diese klassenspezifisch entsprechend den Abschnitten 3.2.2 und 3.2.3 nachgewiesen werden. Die Antragsteller müssen bestätigen, dass sich andere Zertifikatsinhalte, als die angegeben nicht verändert haben.

Wurde die Bestätigung der Organisationszugehörigkeit im Erstantrag bzw. einem vorangegangenen Folgeantrag nur einfach und nicht widerruflich bestätigt, muss die Organisationszugehörigkeit erneut nachgewiesen werden. Dies geschieht analog zu den Verfahren in Abschnitt 3.2.3. Wurde die Organisationszugehörigkeit widerrufen,

muss sie ggf. erneut nachgewiesen werden, andernfalls wird die Organisation nicht wieder ins Zertifikat aufgenommen.

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

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

4.6.2 Berechtigung zur Zertifikatserneuerung

Jeder Antragsteller, der (nach Abschnitt 4.1.1) berechtigt ist, einen erneuten Zertifikatsantrag zu stellen, kann eine Zertifikatserneuerung beantragen, wenn die Bedingungen nach Abschnitt 4.6.1 erfüllt sind.

4.6.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Antragsteller, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, begeben sich persönlich zur RA, reichen den Antrag schriftlich ein (handschriftliche Unterschrift) oder senden den Antrag elektronisch (digital mit dem ursprünglichen oder einem Klassenspezifisch gleichwertigen, gültigen Zertifikat signiert).

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.

PINs werden im Zuge der Zertifikatserneuerung nicht verändert.

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 Schlüssel-erneuerung 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. Für SSL-Zertifikate wird keine Zertifikatserneuerung mit Schlüsselerneuerung angeboten.

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 und F 25 [GL-BRO].

4.7.1 Bedingungen für Zertifikate mit Schlüsselerneuerung

Ein Antrag auf die Schlüsselerneuerung entspricht einem Antrag auf Folgezertifikate. Dabei kann für den Antragsteller – im Gegensatz zu einem neuen Antrag auf Zertifikate – der Vorgang der initialen Identifizierung entfallen. Voraussetzung ist, dass der Beantragende mit dem Antragsteller aus dem Erstantrag identisch ist. Aus dem Unterschriften- bzw. Signaturvergleich muss die Berechtigung erkennbar sein.

Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Schlüsselerneuerung noch gültig sein. Bei schriftlicher Antragstellung kann der Antrag auch nach Ablauf der Gültigkeit des Zertifikats gestellt werden.

Antragsteller müssen ggf. entsprechend der Vorgaben aus Abschnitt 3.2.1 nachweisen, dass sie im Besitz des privaten Schlüssels sind.

Werden Zertifikatsinhalte verändert, müssen diese klassenspezifisch entsprechend den Abschnitten 3.2.2 und 3.2.3 nachgewiesen werden. Die Antragsteller müssen bestätigen, dass sich andere Zertifikatsinhalte, als die angegeben nicht verändert haben. Wurde die Bestätigung der Organisationszugehörigkeit im Erstantrag bzw. einem vorangegangenen Folgeantrag nur einfach und nicht widerruflich bestätigt, muss die Organisationszugehörigkeit erneut nachgewiesen werden. Dies geschieht analog zu den Verfahren in Abschnitt 3.2.3. Wurde die Organisationszugehörigkeit widerrufen, muss sie ggf. erneut nachgewiesen werden, andernfalls wird die Organisation nicht wieder ins Zertifikat aufgenommen.

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

Sollen Zertifikate zu einem vorhandenen Schlüsselpaar ausgestellt werden, muss der Besitz des privaten Schlüssels entsprechend Abschnitt 3.2.1, nachgewiesen werden. Das Schlüsselmaterial und der kryptographische Algorithmus müssen den Mindestanforderungen der zum Zeitpunkt der Antragstellung gültigen CP entsprechen, siehe Abschnitte 3.2.1, 6.1.1 [CPS] und 6.1.5 [CPS] und dürfen nicht kompromittiert sein.

4.7.2 Berechtigung zur Schlüsselerneuerung

Jeder Antragsteller der (nach Abschnitt 4.1.1) berechtigt ist, einen erneuten Zertifikatsantrag zu stellen, kann eine Schlüsselerneuerung für seine beantragten Zertifikate beantragen, wenn für diese Zertifikate die Bedingungen nach Abschnitt 4.7.1 erfüllt sind.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Anträge können schriftlich (handschriftliche Unterschrift) oder elektronisch mit dem ursprünglichen, gültigen Zertifikat signiert eingereicht werden.

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 gehört zu den vom ZDA vertraglich und gesetzlich geschuldeten Obliegenheiten gegenüber dem Zertifikatnehmer bzw. betroffenen Dritten. Die Verfahren des ZDA erfüllen die Bedingungen aus [ETSI-F] und [GL-BRO].

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

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

Der ZDA ist sperrberechtigt. Der ZDA muss gemäß [GL-BRO] Abschnitt 27.b bzw. 28 (c) sperren.

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

Enthält ein Zertifikat Angaben über die Vertretungsmacht des Zertifikatnehmers für eine dritte Person, so kann auch die dritte Person oder die für sonstigen Angaben zur Person zuständige Stelle eine Sperrung des betreffenden Zertifikates verlangen, wenn die Voraussetzungen für die Angaben zur Person nach Aufnahme in das Zertifikat entfallen. Zusätzliche Sperrberechtigte Dritte können benannt werden und haben dann stets die Berechtigung zur Sperrung dieser Zertifikate.

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

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:	sperr@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 Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

4.9.4 Fristen für einen Sperrantrag

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

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

Integrität und Authentizität der Sperrinformationen wird durch eine Signatur 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

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

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine.

4.9.13 Bedingungen für eine Suspendierung

Suspendierungen von Zertifikaten werden nicht angeboten.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

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

4.10.2 Verfügbarkeit des Statusabfragedienstes

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

4.10.3 Optionale Leistungen

keine

4.11 Austritt aus dem Zertifizierungsdienst

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

4.12 Schlüsselhinterlegung und –wiederherstellung

Das Hinterlegen privater EA-Schlüssel kann bis auf die im Folgenden aufgeführten Ausnahmen beantragt werden.

Class 3-2

Signaturschlüssel 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

Der Antragsteller muss die Hinterlegung beantragen und angeben, dass der private EA-Schlüssel für die Erstellung von Zertifikaten für denselben Zertifikatnehmer und/oder eine bestimmte Personengruppe wiederverwendet werden soll.

Sollen EA-Schlüssel nach 6.2.3 [CPS] wieder verwendet werden, muss der Antragsteller nachweisen, dass er berechtigt ist, diesen Schlüssel wiederzuverwenden.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Sitzungsschlüssel werden nicht angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Der ZDA etabliert nicht-technische Sicherheitsmaßnahmen, die die Anforderungen aus [ETSI-F] und [GL-BRO] erfüllen.

Die Verfahren sind im [CPS] definiert.

6. Technische Sicherheitsmaßnahmen

Der ZDA etabliert technische Sicherheitsmaßnahmen, die die Anforderungen aus [ETSI-F] und [GL-BRO] erfüllen.

Zertifikatnehmer und Zertifikatsnutzer müssen vertrauenswürdige Computer und Software verwenden.

Die Verfahren sind im [CPS] definiert.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

Die von CAs der D-TRUST-Root-PKI ausgestellten Zertifikate erfüllen die Anforderungen der Standards ITU [X.509] und IETF [RFC 5280], sowie der Profilierung Common PKI 2.0 [Co-PKI]. Abweichungen müssen ggf. in einem referenzierten Dokument beschrieben sein.

Class 3 EV-Zertifikate

In der D-TRUST-Root-PKI ausgestellte EV-Zertifikate erfüllen die Anforderungen aus [GL-BRO].

Die Profile sind im [CPS] definiert.

7.2 Sperrlistenprofile

Die ausgestellten Sperrlisten erfüllen die Anforderungen der Standards ITU [X.509] und IETF [RFC 5280] sowie der Profilierung Common PKI 2.0 [Co-PKI].

Die Profile sind im [CPS] definiert.

7.3 Profile des Statusabfragedienstes (OCSP)

Der Statusabfragedienst ist konform zum Standard [RFC 2560] und erfüllt die Anforderungen der Profilierung Common PKI 2.0 [Co-PKI].

Die Profile sind im [CPS] definiert.

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 her nach 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 überprüft 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 her nach 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. Diese Auditierung findet jährlich statt.

Darüber hinaus finden regelmäßig interne Audits statt.

9. Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

9.1.1 Preise für Zertifikate

Die Entgeltung der Zertifizierung gegenüber der D-TRUST GMBH wird in der Preisliste festgelegt, die abgefragt werden kann unter:

<https://www.d-trust.net/internet/files/2.Preisinformationen.pdf>

9.1.2 Preise für den Zugriff auf Zertifikate

Die Abfrage von Zertifikaten im Verzeichnisdienst ist kostenlos.

9.1.3 Preise für Sperrungen oder Statusinformationen

Sperrungen und das Abrufen von Statusinformationen sind kostenlos.

9.1.4 Preise für andere Dienstleistungen

Soweit angeboten siehe Preisliste gemäß Preisliste Abschnitt 9.1.1.

9.1.5 Regeln für Kostenrückerstattungen

Es gelten die AGB.

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Der ZDA D-TRUST GMBH verfügt über eine Versicherungsdeckung gemäß § 12 SigG:

„Der Zertifizierungsdiensteanbieter ist verpflichtet, eine geeignete Deckungsvorsorge zu treffen, damit er seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachkommen kann, die dadurch entstehen, dass er die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 verletzt oder seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen. [...]“

Der ZDA erfüllt die Anforderungen von [GL-BRO] 4.c und 37.a.

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung

Keine Angaben.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine Angaben.

9.3 Vertraulichkeit von Geschäftsdaten

9.3.1 Definition von vertraulichen Geschäftsdaten

Die Vertraulichkeit von Informationen kann vereinbart werden, sofern sie nicht bereits durch geltendes Recht definiert ist.

9.3.2 Geschäftsdaten, die nicht vertraulich behandelt werden

Als öffentlich gelten alle Informationen in ausgestellten und veröffentlichten Zertifikaten sowie die unter Abschnitt 2.2 genannten Daten.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten

Der ZDA kann im Einzelfall verpflichtet werden, die ihm als vertrauliche Geschäftsdaten benannten Daten durch entsprechende technische und organisatorische Maßnahmen gegen Preisgabe und Ausspähung zu schützen, und zu unterlassen, diese Daten zweckentfremdet zu nutzen oder sie Drittpersonen offen zu legen, soweit eine solche Verpflichtung nicht gegen das Gesetz verstößt. Im Rahmen der organisatorischen Maßnahmen werden die vom ZDA eingesetzten Mitarbeiter in dem gesetzlich zulässigen Rahmen zur Geheimhaltung der vertraulichen Daten verpflichtet.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Der ZDA arbeitet auf Basis eines auditierbaren Sicherheitskonzeptes, das den Schutz der vertraulichen personenbezogenen Daten (kurz Personendaten) regelt. Der ZDA erfüllt die Anforderungen nach § 4a, b, § 9 und §§ 27 ff des Bundesdatenschutzgesetzes.

9.4.2 Definition von Personendaten

Unter personenbezogene Daten (kurz Personendaten) fallen alle Angaben, die durch die RA zum Zweck der Zertifikatserstellung erhoben werden und die sich auf eine natürliche Person beziehen.

9.4.3 Daten, die nicht vertraulich behandelt werden

Daten, die explizit in Zertifikaten, in Sperrlisten und in Statusinformationen enthalten sind, gehören nicht zu den als vertraulich behandelten Daten.

9.4.4 Zuständigkeiten für den Datenschutz

Der ZDA gewährleistet die Einhaltung des Datenschutzes. Alle Mitarbeiter des ZDA sind auf die Einhaltung des Datenschutzes verpflichtet worden. Die interne Kontrolle erfolgt durch den betrieblichen Datenschutzbeauftragten, die externe Kontrolle erfolgt durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Dem Antragsteller wird bei Antragstellung kenntlich gemacht, welche persönlichen Daten im Zertifikat enthalten sein werden. Zertifikate werden nur veröffentlicht, wenn der Antragsteller dem bei der Antragstellung zustimmt.

Der Antragsteller wird bei Antragstellung darüber informiert, dass die RA nur Daten erhebt, die für die Zertifikatsausstellung sowie für den Betrieb der D-TRUST-Root-PKI notwendig sind. Weiterhin wird er dahingehend informiert, dass die Daten vor dem Zugriff unbefugter geschützt sind und nur im Rahmen gesetzlicher Verpflichtungen weitergegeben werden.

Alle nicht mehr benötigten Personendaten werden umgehend gelöscht. Für Personendaten, die zum Zertifikatsnachweis benötigt werden, gelten die Fristen nach Abschnitt 5.5.2 des [CPS].

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Es gilt § 14 (2) SigG:

„Der Zertifizierungsdiensteanbieter hat die Daten über die Identität eines Signaturschlüssel-Inhabers (Zertifikatnehmer) auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber (Zertifikatnehmer) über die Übermittlung der Daten zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers (Zertifikatnehmer) an der Unterrichtung überwiegt.“

Zu diesem Zweck werden Antragsdaten archiviert und während der Gültigkeit des Zertifikats sowie fristgerecht nach Abschnitt 5.5.2 des [CPS] aufbewahrt. Auskünfte werden dokumentiert und mindestens ein Jahr aufbewahrt.

9.4.7 Andere Bedingungen für Auskünfte

Auskünfte anderer Art als unter Abschnitt 9.4.6 beschrieben werden nicht erteilt.

9.5 Gewerbliche Schutz- und Urheberrechte

9.5.1 ZDA

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.5.2 Antragsteller

Der Antragsteller verpflichtet sich zur Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten.

9.6 Zusicherungen und Garantien

9.6.1 Leistungsumfang des ZDA

Es gelten die AGB. Soweit nicht ausdrücklich erwähnt, räumt der ZDA keine Garantien oder Zusicherungen im Rechtssinne ein.

Class 3-2

Der ZDA sorgt für die eindeutige, persönliche Identifizierung der Antragsteller und die Zuordenbarkeit des öffentlichen Schlüssels zum Zertifikatnehmer.

Der ZDA stellt sicher, dass die in den Abschnitten 4, 3.2 und 3.3 [CPS] beschriebenen Verfahren eingehalten werden.

Der ZDA stellt sicher, dass ein in Zertifikaten verwendeter Name (*DistinguishedName* im Feld *subject*) innerhalb der D-TRUST-Root-PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatnehmer zugeordnet ist. Dadurch ist die eindeutige Identifizierung⁷ des Zertifikatnehmers anhand des im Zertifikat verwendeten Namens (*subject*) gewährleistet.

Der ZDA hält den Betrieb der CAs, eines Verzeichnisdienstes sowie das Bereitstellen von Sperrinformationen vor.

Class 3 EV-Zertifikate

Der ZDA übernimmt keine Garantien im gesetzlichen Sinne nach dem BGB, unterwirft sich aber den Bestimmungen gemäß Abschnitt 3 [GL-BRO] hinsichtlich “Legal Existence“, “Identity“, “Right to Use Domain Name“, “Authorization for EV Certificate“, “Accuracy of Information“, “Subscriber Agreement“, “Status“, “Revocation“ und gewährleistet deren Einhaltung. Zusätzlich hält der ZDA den Betrieb einer EV-Reportingstelle gemäß Abschnitt 28 [GL-BRO] vor. Die Reportingstelle bietet Zertifikatsnutzern die Möglichkeit Ihnen suspekten EV-Zertifikate des ZDA anzuzeigen. Der ZDA geht dann dem Verdacht des Zertifikatsnutzers (z. B. Betrug, Phishing etc.) nach.

Der ZDA kann Teilaufgaben an Partner oder an externe Anbieter auslagern. Der ZDA stellt sicher, dass in diesem Fall die Bestimmungen von CP und [CPS] eingehalten werden.

9.6.2 Leistungsumfang der RA

Der ZDA betreibt Registrierungsstellen (RA). Die RA erbringt Identifizierung und Registrierung. Es gelten die AGB sowie die Bestimmungen dieser CP.

9.6.3 Zusicherungen und Garantien des Zertifikatnehmers

Es gelten die AGB des ZDA und diese CP.

Class 3

Bei Antragstellung unterschreibt der Antragsteller (ggf. in Vertretung für den Zertifikatnehmer) eine Verpflichtungserklärung (Subscriber Agreement), die Zusicherungen und Garantien des Zertifikatnehmers beinhaltet. Das Subscriber Agreement entspricht den Anforderungen von [ETSI-F].

⁷ Siehe Fußnote 2 auf Seite 17.

Class 3 EV-Zertifikate

Das Subscriber Agreement entspricht den Anforderungen von Abschnitt E 12[GL-BRO].

9.6.4 Zusicherungen und Garantien des Zertifikatsnutzers

Zusicherungen und Garantien des Zertifikatsnutzers werden nach dieser CP nicht geregelt. Es entsteht zwischen dem ZDA und dem Zertifikatsnutzer kein Vertragsverhältnis. Im Übrigen gelten die AGB sowie gesetzliche Bestimmungen.

9.7 Haftungsausschlüsse

9.7.1 Haftungsausschlüsse des ZDA

Es gelten die AGB.

Class 3 EV-Zertifikate

Soweit Class 3 EV-Zertifikate ausgegeben werden, geltend ergänzend die nachfolgenden Bestimmungen gemäß Abschnitt K 37 [GL-BRO]:

Soweit der ZDA ohne Abweichungen nach den Bestimmungen dieser Zertifikatsrichtlinie das Class 3 EV-Zertifikat ausgegeben hat, ist seine Haftung für mit dem Zertifikat verursachte Schäden ausgeschlossen.

9.8 Haftungsbeschränkungen

Soweit bei der Ausstellung des Class 3 EV-Zertifikats von den Bestimmungen dieser Zertifikatsrichtlinie abgewichen wurde, gelten die nachfolgenden Haftungsbestimmungen ebenfalls in Übereinstimmung mit den Vorgaben nach Abschnitt K 37 [GL-BRO]:

Für die korrekte Antragsprüfung und den daraus resultierenden Inhalt der Class 3 EV-Zertifikate haftet der ZDA nur im Rahmen seiner Prüfungsmöglichkeiten. Die Erteilung von Class 3 EV-Zertifikaten bestätigt nur, daß D-TRUST zum Zeitpunkt der Antragstellung der erforderliche Identitäts- bzw. Legitimationsnachweis nach den Vorgaben dieser Zertifikatsrichtlinie erbracht wurde. Soweit eine ausgelagerte Registrierungsstelle aufgrund des konkreten Vertragsverhältnisses mit D-TRUST erforderliche Identitätsprüfungen bezogen auf den Zertifikatsnehmer vornimmt, hat diese Registrierungsstelle die Vorgaben der D-TRUST im Einklang mit den Bestimmungen dieser Zertifikatsrichtlinie bei der Identitätsprüfung einzuhalten, wozu sie sich in dem konkreten Vertragsverhältnis mit der D-TRUST verpflichtet. Verstößt die Registrierungsstelle gegen diese Vorgaben, so hat sie D-TRUST hinsichtlich der daraus resultierenden Ansprüche des Zertifikatsnehmers oder sonstiger Dritter freizustellen. Selbiges gilt für die Fälle, dass der Antragsteller als Registrierungsstelle selbst Identifizierung von Zertifikatsnehmern vornimmt, die zu seiner eigenen Organisation gehören.

Der Antragsteller haftet für Schäden, die D-TRUST durch von ihm verursachte fehlerhafte Angaben im Class 3 EV-Zertifikat, sowie durch von ihm verschuldeten, fehlerhaften Einsatz der Class 3 EV-Zertifikate entstehen.

Im Übrigen ist in den vorgenannten Fällen die Haftung des ZDA auf einen Betrag von maximal 2.000,00 US Dollars bzw. auf den entsprechenden EURO Betrag am Tag des Schadenseintritts pro Class 3 EV-Zertifikat begrenzt.

9.9 Schadensersatz

9.9.1 Ansprüche des ZDA gegenüber Antragstellern/Zertifikatnehmern

Werden vom Antragsteller arglistig betrügerische oder falsche Daten gegenüber der RA angegeben, so hat der ZDA Anspruch auf Schadensersatz nach den gesetzlichen Bestimmungen.

9.9.2 Ansprüche der Zertifikatnehmer gegenüber dem ZDA

Es gelten die AGB.

9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit

9.10.1 Gültigkeitsdauer der CP

Diese CP gilt ab dem Zeitpunkt der Veröffentlichung und bleibt gültig, solange noch Zertifikate, die auf Basis dieser CP ausgestellt wurden, gültig sind.

9.10.2 Beendigung der Gültigkeit

Siehe Abschnitt 9.10.1.

9.10.3 Auswirkung der Beendigung

Siehe Abschnitt 9.10.1.

9.11 Individuelle Mitteilungen und Absprachen mit PKI-Teilnehmern

Mitteilungen des ZDA an Zertifikatnehmer werden an die letzte in den Unterlagen von D-TRUST GMBH verzeichnete Anschrift oder der entsprechenden E-Mail-Adresse aus dem Antrag (elektronisch signiert) versendet.

9.12 Nachträge

9.12.1 Verfahren für Nachträge

Nachträge zu dieser CP werden in dieses Dokument eingearbeitet und unter demselben OID veröffentlicht. Editorische Änderungen werden markiert.

9.12.2 Benachrichtigungsmechanismen und –fristen

Keine Angaben.

9.12.3 Bedingungen für OID-Änderungen

Keine Angaben.

9.13 Bestimmungen zur Schlichtung von Streitfällen

Beschwerden bezüglich der Einhaltung oder Umsetzung dieser CP sind beim ZDA (D-TRUST GMBH, Kommandantenstr. 15, 10969 Berlin, Germany) schriftlich einzureichen. Soweit nicht innerhalb einer Frist von 4 Wochen nach Einreichung der Beschwerde abgeholfen wurde, gilt: Für sämtliche Streitigkeiten steht jedermann der Rechtsweg nach deutschem Gesetz offen.

Zusätzlich hält der ZDA den Betrieb einer EV-Reportingstelle gemäß Abschnitt 9.6.1 vor. Ein Missbrauchsverdacht von D-Trust-EV-Zertifikaten kann unter der E-Mail-Adresse: ev-support@d-trust.net gemeldet werden.

9.14 Gerichtsstand

Es gelten die AGB.

9.15 Einhaltung geltenden Rechts

Diese CP unterliegt dem Recht der Bundesrepublik Deutschland.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitserklärung

Folgende Dokumente sind Gegenstand der geltenden Vereinbarungen zwischen ZDA und PKI-Teilnehmern:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Anwendung der PKI gültigen AGB,
- die zum Zeitpunkt der Anwendung der PKI gültige CP.

Abweichend gelten für Class 3 SSL CAs, deren Sub- sowie Root-CAs:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Anwendung der PKI gültigen AGB,
- die zum Zeitpunkt der Anwendung der PKI gültige Version der [GL-BRO].
- die zum Zeitpunkt der Anwendung der PKI gültige CP.

9.16.2 Abgrenzungen

entfällt

9.16.3 Salvatorische Klausel

Wenn eine Bestimmung dieser CP oder deren Anwendung aus irgendeinem Grund und in welchem Umfang auch immer für ungültig oder nicht vollstreckbar befunden wird, ist der Rest dieser CP (sowie die Anwendung der ungültigen oder nicht vollstreckbaren Bestimmung auf andere Personen oder unter anderen Bedingungen) so zu interpretieren, dass die Absichten der Parteien so weit wie möglich berücksichtigt werden.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Es gelten die AGB.

9.16.5 Höhere Gewalt

Es gelten die AGB.

9.17 Andere Bestimmungen

9.17.1 Konflikt von Bestimmungen

Die unter 9.16.1 genannten Regelungen sind abschließend. Sie gelten untereinander in der in 9.16.1 aufgeführten Reihenfolge jeweils nachrangig.

9.17.2 Einhaltung von Ausführungsgesetzen und -vorschriften

Die Ausfuhr bestimmter Software, die in Verbindung mit den öffentlichen Zertifizierungsleistungen von D-TRUST GMBH eingesetzt wird, kann von der Zustimmung der zuständigen Behörden abhängig sein. Die Parteien werden die einschlägigen Ausführungsgesetze und -vorschriften beachten.

Die Verwendung der öffentlichen Zertifizierungsdienstleistungen der D-TRUST GMBH unterliegt diversen Gesetzen der Bundesrepublik Deutschland. D-TRUST GMBH behält sich in jedem Fall der Zuwiderhandlung gegen die öffentlichen Zertifizierungsdienstleistungen der D-TRUST GMBH das Recht auf strafrechtliche Verfolgung vor.