BUNDESDRUCKEREI

Certification Practice Statement

D-TRUST Telematikinfrastruktur

Version 2.0

D-TRUST EINE MARKE DER BUNDESDRUCKEREI

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement der D-TRUST Telematikinfrastruktur

©2018 D-TRUST GmbH

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.

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

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

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	01.05.2015	Initialversion
2.0	30.11.2018	▪ Dieses CPS steht zukünftig vollständig unter der Certificate Policy der D-TRUST GmbH ▪ Integration des HBA in den bestehenden qualifizierten Vertrauensdienst der D-TRUST GmbH gemäß EN 319 411-2 ▪ Dieses CPS gilt für HBA und SMC-B

Inhaltsverzeichnis

1. Einleitung 6
1.1 Überblick 6
1.2 Name und Kennzeichnung des Dokuments 9
1.3 PKI-Teilnehmer 9
1.4 Verwendung von Zertifikaten 11
1.5 Administration der Policy 11
1.6 Begriffe und Abkürzungen 12
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 14
3. Identifizierung und Authentifizierung 15
3.1 Namensregeln 15
3.2 Initiale Überprüfung der Identität 20
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) 21
3.4 Identifizierung und Authentifizierung von Sperranträgen 22
4. Betriebsanforderungen 23
4.1 Zertifikatsantrag und Registrierung 23
4.2 Verarbeitung des Zertifikatsantrags 24
4.3 Ausstellung von Zertifikaten 25
4.4 Zertifikatsübergabe 25
4.5 Verwendung des Schlüsselpaars und des Zertifikats 26
4.6 Zertifikatserneuerung (certificate renewal) 27
4.7 Zertifikatserneuerung mit Schlüsselerneuerung 27
4.8 Zertifikatsänderung 29
4.9 Sperrung und Suspendierung von Zertifikaten 29
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 TSP 36
5.7 Kompromittierung und Geschäftsweiterführung beim TSP 36
5.8 Schließung des TSP 37
6. Technische Sicherheitsmaßnahmen 38
6.1 Erzeugung und Installation von Schlüsselpaaren 38
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module 39
6.3 Andere Aspekte des Managements von Schlüsselpaaren 40
6.4 Aktivierungsdaten 41
6.5 Sicherheitsmaßnahmen in den Rechneranlagen 41
6.6 Technische Maßnahmen während des Life Cycles 42
6.7 Sicherheitsmaßnahmen für Netze 43
6.8 Zeitstempel 43

7. Profile von Zertifikaten, Sperrlisten und OCSP 44
7.1 Zertifikatsprofile 44
7.2 Sperrlistenprofile 47
7.3 Profile des Statusabfragedienstes (OCSP) 47
8. Auditierungen und andere Prüfungen 49
9. Sonstige finanzielle und rechtliche Regelungen 50

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Certification Practice Statement (CPS) der von D-TRUST GmbH betriebenen TSP in der Telematikinfrastruktur des Gesundheitswesens für Zertifikate des HBA (TSP-X.509QES und TSP-X.509nonQES) und der SMC-B.

1.1.1 Vertrauensdiensteanbieter

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

1.1.2 Über dieses Dokument

Dieses CPS nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-TRUST GmbH mit der OID 1.3.6.1.4.1.4788.2.200.1 und die EN 319 411-2. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

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

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

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

Dieses CPS definiert Abläufe und Vorgehensweisen des von der D-TRUST GmbH betriebenen TSP im Umfeld der Telematikinfrastruktur während der gesamten Lebensdauer der Zertifikate von HBA und SMC-B. Es werden Mindestmaßnahmen konstatiert, die von allen Teilnehmern der Zertifizierungsinfrastruktur zu erfüllen sind.

In den ausgestellten Zertifikaten des TSP können zusätzlich zu der CP der D-TRUST GmbH noch weitere CPs referenziert werden, die detailliert Anforderungen und Beschränkungen definieren. Zu diesen CPs gehören:

- „Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL" (s. [gemRL_TSL_SP_CP] Version: 2.2.0),
- Gemeinsame Policy für die Ausgabe der Heilberufsausweise – Zertifikatsrichtlinie HBA (s. [CP-HBA Version: 2.0.0),
- ZOD 2.0 - Certificate Policy (s. [ZODPol]) und

Diese Policy beschreibt auch die Mindestanforderungen an das qualifizierte Zertifikat des HBA. Aufgrund der eIDAS-Verordnung sind durch den Vertrauensdiensteanbierter umfangreiche weitere Anforderungen hinsichtlich des Betriebs, der Identifizierung, der Validierung und Archivierung umzusetzen.

Weitere für die Zertifikatsnutzer relevanten Informationen werden auf den Webseiten der Herausgeber des HBA (Bundesärztekammer) bereitgestellt.

Werden Anforderungen an den TSP-X.509QES und TSP-X.509nonQES bzw. an TSP-X.509QES-Zertifikate und TSP-X.509nonQES-Zertifikate gleichermaßen gestellt, wird in diesem Dokument nur vom TSP bzw. von Zertifikaten gesprochen.

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

1.1.3 Eigenschaften der PKI

Die nachstehende Abbildung zeigt die Zertifizierungsinfrastruktur für den HBA für qualifizierte Vertrauensdienste in der Telematikinfrastruktur.

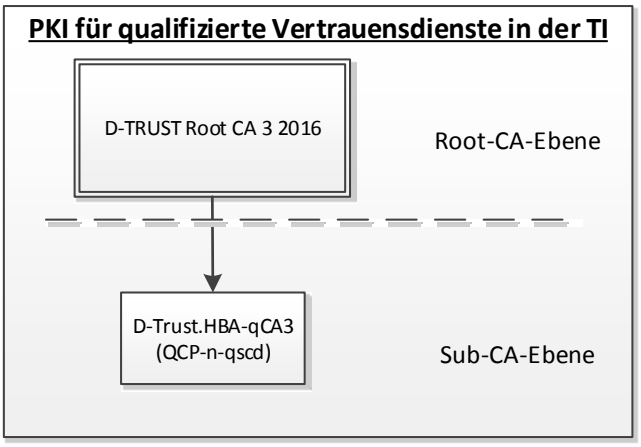

Abbildung 1: Einordnung der vom TSP-X.509QES betriebenen HBA-CA

Qualifizierte CA-Zertifikate

D-TRUST Root CA 3 2016 http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2016.crt Fingerprint: SHA1: 16 ab fe 95 5b ba 80 f0 d7 07 9d 24 01 88 c6 33 df 5d db 7f
D-Trust.HBA-qCA3[1] Zertifizierungsklasse: QCP-n-qscd OID: 1.3.6.1.4.1.4788.2.211.1

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

[1] Link wird bekannt gegeben, sobald der Service zur Verfügung gestellt wird.

Die nachstehende Abbildung zeigt die Zertifizierungsinfrastruktur für den HBA und SMCB für nicht-qualifizierte Vertrauensdienste in der Telematikinfrastruktur.

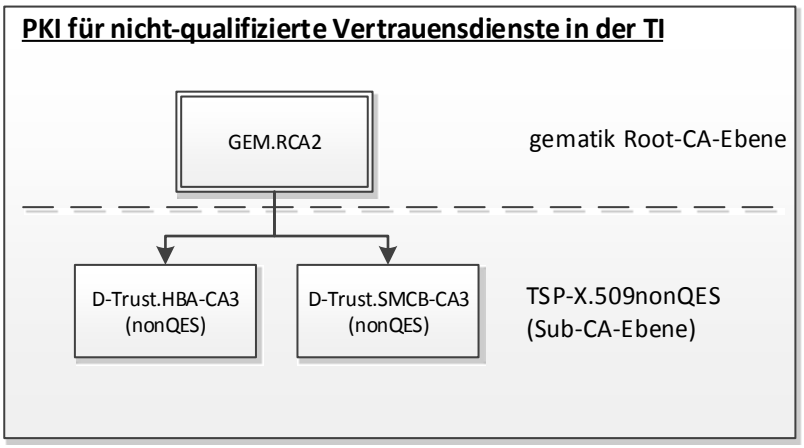

Abbildung 2:
Einordnung der vom TSP-X.509nonQES betriebenen HBA-CA und SMCB-CA

Nicht-qualifizierte CA-Zertifikate

Gematik Root-CA: GEM.RCA2 https://download.tsl.ti-dienste.de/GEM.RCA2.der Fingerprint: SHA1: 85 10 b8 59 b3 7d 50 56 69 a0 d2 2c 73 7b 17 3c e1 bb 9b 6e OID: 1.2.276.0.76.4.163
D-Trust.HBA-CA3 (nonQES) https://download.tsl.ti-dienste.de/D-Trust.HBA-CA3.der Fingerprint: SHA1: b8 c0 76 d8 d4 6b 0e 80 79 3f 95 c8 13 10 9d 9c 0f 72 59 8f OID: 1.2.276.0.76.4.145
D-Trust.SMCB-CA3 (nonQES) https://download.tsl.ti-dienste.de/D-Trust.SMCB-CA3.der Fingerprint: SHA1: 0a 88 20 d3 33 fd 25 9f c7 ab 9d 65 3d ff 33 69 73 d9 f3 0a OID: 1.2.276.0.76.4.163

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

1.2 Name und Kennzeichnung des Dokuments

Dokumentname: Certification Practice Statement D-TRUST Telematikinfrastruktur

Version 2.0

1.3 PKI-Teilnehmer

Die Definition und Abgrenzung der Teilnehmer in der Zertifizierungsinfrastruktur der Telematikinfrastruktur erfolgt im Rahmen von [gemKPT_PKI_TIP#2.7], [gemSpec_PKI#6.1]. Im vorliegenden Dokument erfolgt eine kurze Darstellung der in dieser Policy relevanten Teilnehmer.

1.3.1 Zertifizierungsstellen (CA) – TSP-X.509 QES bzw. TSP-X.509 nonQES

Zertifizierungsstellen (Certification Authority – CA) werden vom Vertrauensdiensteanbieter betrieben und stellen Zertifikate sowie Sperrlisten aus.

Der Trust Service Provider stellt Zertifikate für berechtigte Personen aus und ermöglicht die Abfrage des Sperrstatus von durch ihn ausgestellten Zertifikaten (s. [gemKPT_Arch_TIP]).

Die entsprechende Zertifizierungsstelle (HBA-CA bzw. SMCB-CA) ist in den ausgestellten Zertifikaten und CRLs namentlich im Feld issuer benannt.

Möglich sind folgende Arten von Zertifikaten:

Personenzertifikate für natürliche Personen (EE-Zertifikat),

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

1.3.2 Registrierungsstellen (RA)

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

Weiterhin nehmen die Registrierungsstellen auch Sperranträge entgegen, veranlassen die operative Sperrung von Zertifikaten und betreiben eine Hotline für die von ihnen bereitgestellten Dienste. Registrierungsstellen bilden die Kundenschnittstelle der Zertifizierungsinfrastruktur zu den Zertifikatsnehmern.

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

1.3.3 Zertifikatnehmer (ZNE) und Endanwender (EE)

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

Endanwender (*subject;* End-Entity (EE)) verwenden die privaten Endanwenderschlüssel (EE-Schlüssel). Die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft. Der Endanwender kann mit dem Zertifikatnehmer identisch sein.

Zulässige Endanwender sind:

- natürliche Personen,
- juristische Personen.

Die Verantwortung für Schlüssel und Zertifikat trägt der Zertifikatnehmer, sobald diese durch den Vertrauensdiensteanbieter an ihn übergeben wurden. Darüber hinaus ergeben sich nach [EN 319 411-1] bzw. [EN 319 411-2] weitere Pflichten. Spätestens zum Zeitpunkt der Antragstellung wird der Zertifikatnehmer über diese Pflichten durch die Bereitstellung dieses CPS und der allgemeinen Verpflichtungserklärung (subscriber agreement) informiert und muss sich zu deren Einhaltung verpflichten.

QCP-n-qscd

Für qualifizierte Signaturzertifikate müssen Zertifikatnehmer und Endanwender identisch sein.

Der Zertifikatsnehmer eines X.509-QES- und X.509-nonQES-Zertifikats eines HBA im Sinne dieser Policy ist die natürliche Person, auf die diese X.509-QES- und X.509-nonQES-Zertifikate des HBA gemäß dieser Policy ausgestellt wurde und die in der alleinigen Kontrolle über den diesem Zertifikat zugeordneten privaten Schlüssel ist.

Der Zertifikatnehmer der X.509-nonQES-Zertifikate einer SMC-B im Sinne dieser Policy ist die medizinische Institution, die über dieses X.509-nonQES-Zertifikat der SMC-B repräsentiert wird.

1.3.4 Zertifikatsnutzer (ZNU)

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

1.3.5 Antragsteller

Antragsteller des HBA und somit der enthaltenen X.509-QES- und X.509-nonQES-Zertifikate ist immer eine natürliche Person, die einen HBA bei einem für ihn zuständigen Kartenherausgeber beantragt (s. [CP-HBA#1.3]).

Antragsteller der SMC-B und somit der enthaltenen X.509-nonQES-Zertifikate ist immer eine natürliche Person, die für die medizinische Institution vertretungs- und zeichnungsberechtigt ist [s. [gemKPT_PKI_TIP#2.7.5).

1.3.6 Kartenherausgeber

Kartenherausgeber für den HBA und den SMC-B sind die jeweiligen Körperschaften des öffentlichen Rechts.

Der Kartenherausgeber ist die verantwortliche Stelle im Sinne des DSGVO und damit Ansprechpartner im datenschutzrechtlichen Bezug für alle Antragsteller bzw. Karteninhaber.

1.3.7 Karteninhaber (Inhaber)

Die Begriffe Karteninhaber und Zertifikatnehmer sind in diesem Dokument gleichgesetzt.

1.3.8 Sperrberechtigter

Ein Sperrberechtigter ist eine natürliche oder juristische Person, die zur Sperrung eines Zertifikats berechtigt ist.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

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

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

Ein vom TSP ausgestelltes Zertifikat eines HBA oder einer SMC-B darf ausschließlich für die Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten (keyUsage) stehen.

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

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

1.4.2 Verbotene Verwendungen von Zertifikaten

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

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

1.4.3 Verwendung von Dienstezertifikaten

Der TSP verwendet Dienstezertifikate zur Erbringung von Vertrauensdienste gemäß [eIDAS]. Dienstezertifikate werden durch den TSP selbst und zur eigenen Verwendung ausgestellt. Sie unterliegen den Anforderungen der jeweilig anwendbaren Zertifizierung.

Zu den Verwendungsarten zählen:

- CA-Zertifikate zur CA- und Zertifikatserstellung
- Signatur von Sperrauskünften[2]

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird durch die D-TRUST GmbH gepflegt. Der Beauftragte der Geschäftsführung übernimmt die Abnahme des Dokuments.

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

Siehe [CP der D-TRUST 1.5]

---

[2] OCSP-Auskünfte werden durch gesonderte OCSP-Dienstezertifikate signiert.

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

Zur Meldung von Sicherheitsvorfällen kontaktieren Sie bitte unseren Support:

support@bdr.de

1.5.3 Verträglichkeit von CPs fremder CAs mit dieser CPS

Sowohl in CA- als auch in EE-Zertifikaten können weitere CPs über Policy-OIDs referenziert werden, die dieser CPS nicht widersprechen. Die Referenz einer Policy-OID in den Zertifikatserweiterungen bestätigt die Kompatibilität der Zertifizierungspraktiken mit der referenzierten CP (z. B. NCP 0.4.0.2042.1.1 gemäß [EN 319 411-1]).

In dieser CP werden Mindestanforderungen beschrieben, die von allen Teilnehmern der Zertifizierungsinfrastruktur erfüllt werden müssen.

In den vom TSP ausgestellten Zertifikaten können weitere Policies über Policy-OIDs referenziert werden, die dieser CP nicht widersprechen. Die Referenz einer Policy-OID in den Zertifikatserweiterungen bestätigt seitens des TSP die Kompatibilität der Zertfizierungspraktiken mit der referenzierten Policy.

Die hierin getroffenen Regelungen bilden widerspruchsfrei zu den folgend aufgezählten, übergreifenden Regelungen als Präzisierung diejenigen Sachverhalte ab, die für den von der von D TRUST GMBH betriebenen TSP relevant sind.

- „Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL“ (s. [gemRL_TSL_SP_CP]),
- Gemeinsame Policy für die Ausgabe der Heilberufsausweise – Zertifikatsrichtlinie Heilberufsausweis (s. [CP-HBA]),
- ZOD 2.0 - Certificate Policy (s. [ZODPol]).

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Diese Regelungen sind in der CP der D-TRUST GmbH festgehalten.

Innerhalb der D-TRUST Telematikinfrastruktur werden zusätzlich die folgenden Begriffe verwendet:

Sperrantragsteller_AS	Zur Sperrung von Zertifikaten berechtigter Zertifikatnehmer, welcher über einen HBA oder einen SMC-B verfügt.
Sperrantragsteller_KHG	Zur Sperrung von Zertifikaten berechtigte Stellen, z.B. Vertreter des Kartenherausgebers

1.6.2 Abkürzungen

Diese Regelungen sind in der CP der D-TRUST GmbH festgehalten.

Innerhalb der D-TRUST Telematikinfrastruktur des Gesundheitswesens werden zusätzlich die folgenden Abkürzungen verwendet:

DKG	Deutsche Krankenhausgesellschaft
HBA	Heilberufsausweis

KBV	Kassenärztliche Bundesvereinigung
KZBV	Kassenzahnärztliche Bundesvereinigung
LEO	Leistungserbringer-Organisation
SMC-B	Sicherheitsmodul vom Typ B <medizinische Institution>
TSP	Trust Service Provider (TSP) bzw. Vertrauensdiensteanbieter (VDA) für TSP-X.509 QES und TSP-X.509 nonQES
TSP-X.509 nonQES	Trust Service Provider für nicht-qualifizierte X.509-Anwenderzertifikate
TSP-X.509 QES	Trust Service Provider für qualifizierte X.509-Anwender-zertifikate

1.6.3 Referenzen

Diese Regelungen sind in der CP der D-TRUST GmbH festgehalten.

Innerhalb der D-TRUST Telematikinfrastruktur des Gesundheitswesens werden zusätzlich die folgenden Abkürzungen verwendet:

[gemSpec_PKI][3]	Übergreifende Spezifikation - Spezifikation PKI, Version: 2.3.0
[gemRL_TSL_SP_CP][3]	„Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL, Version: 2.2.0
[CP-HBA]),	Gemeinsame Policy für die Ausgabe der Heilberufsausweise – Zertifikatsrichtlinie Heilberufsausweis, Version: 2.0.0
[ZODPol]	ZOD 2.0 - Certificate Policy

[3] Die Konzepte und Spezifikationen können vom gematik Fachportal runtergeladen werden: https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/konzepte-und-spezifikationen/ . Bei einer berechtigten Anfrage können die referenzierten Dokumente auch von der D-TRUST GmbH bereitgestellt werden.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Diese Regelungen sind in der CP der D-TRUST GmbH festgehalten.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- EE-Zertifikate , so dies vom Zertifikatnehmer gewünscht wurde,
- CA-Zertifikate,
- Sperrlisten (CRLs) und Statusinformationen,
- die CP der D-Trust GmbH,
- dieses CPS,
- die Verpflichtungserklärung für Zertifikate des TSP-X.509 QES unter dieser Policy

2.3 Häufigkeit von Veröffentlichungen

EE-Zertifikate können veröffentlicht, d.h. in das öffentliche Verzeichnis des TSP aufgenommen werden. Der Zertifikatnehmer kann der Veröffentlichung zustimmen oder diese ablehnen.

QCP-n-qscd,
Veröffentlichte EE-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für zehn Jahre und bis zum Jahresende abrufbar.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und mindestens 10 Jahre (QCP-n-qscd) und bis zum Jahresende nach Ablauf der Gültigkeit der CA vorgehalten.

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

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

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

2.4 Zugriffskontrollen auf Verzeichnisse

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

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

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

CA- und EE-Zertifikate enthalten grundsätzlich Angaben zu Aussteller (issuer) und Zertifikatnehmer bzw. Endanwender (subject). Diese Namen werden entsprechend dem Standard [X.509] als DistinguishedName vergeben.

Innerhalb der Telematikinfrastruktur des Gesundheitswesens gelten zusätzlich die folgenden Anforderungen an Namen:

Siehe [gemSpec_PKI#4], [gemRL_TSL_SP_CP#4.1.1]

3.1.2 Notwendigkeit für aussagefähige Namen

Der verwendete DistinguishedName ist eindeutig innerhalb dieser PKI.

Eine eindeutige Zuordnung des Zertifikats zum Zertifikatnehmer bzw. Endanwender ist gegeben.

Siehe [gemSpec_PKI#4], [gemRL_TSL_SP_CP#4.1.3]

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 Zertifikate im HBA für natürliche Personen benutzt.

Generell werden Pseudonyme vom TSP vergeben. Der Kartenherausgeber stellt die Eindeutigkeit der pseudonymen Zertifikate sicher (s. [gemRL_TSL_SP_CP#4.1.5]). Die Freiwählbarkeit von Pseudonymen kann vereinbart werden, siehe Abschnitt 3.1.6. Der TSP behält sich vor, die Vergabe eines Pseudonyms abzulehnen. Die Ablehnung bedarf keiner Begründung.

Nur falls der vollständige Name in ein Zertifikat im HBA nicht aufgenommen werden kann (z.B. weil er zu lang ist), muss der commonName als Pseudonym gekennzeichnet werden.

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

Generell werden Pseudonyme vom TSP vergeben. Der Kartenherausgeber stellt die Eindeutigkeit der pseudonymen Zertifikate sicher.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Abbildung einer realen Identität (Person, Dienst, Institution) (eines Zertifikatsnehmers) in ein Zertifikat erfolgt durch den Inhalt der Felder SubjectDN (subject distinguishedName). Dabei werden die übergreifenden Kodierungsvorschriften aus [gemSpec_PKI#4] umgesetzt. Insbesondere wird für die einzelnen Felder ein Zeichensatz gemäß [ETSI EN 319 412] und speziell eine UTF8-Kodierung eingesetzt. Somit können Sonderzeichen und Umlaute verwendet werden (s. [gemSpec_PKI#4.1.1]).

Die SubjectDN-Felder für HBA-Zertifikate (TSP-X.509 QES) werden entsprechend [gemSpec_PKI#Anhang C] befüllt.

Die Felder serialNumber, givenName, surName und commonName werden in einem SET als ein einziges multivaluedRDN kodiert. Die entsprechenden Kodierungsregeln von X.690 (Reihenfolge im SET) werden dabei berücksichtigt.

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

SubjectDN Felder für Zertifikate für den HBA (TSP-X.509 QES und nonQES)

DN-Bestandteil	Interpretation
G (given name)	*Vorname(n)* der natürlichen Person QCP-n-qscd Das Attribut givenName enthält alle Vornamen des Zertifikatnehmers.
SN (surname)	*Familienname* der natürlichen Person QCP-n-qscd Der surname enthält (zusätzlich zum commonName) den Nachnamen des Inhabers. Evtl. vorhandene Namensbestandteile wie „Graf von", „jr.", so genannte „generation qualifier" (üblich im amerikanischen Sprachraum, z.B. „III") usw. werden im surname aufgenommen, wenn sie im Reisepass oder Personalausweis als Teile des Nachnamens betrachtet werden. Ggf. im Personalausweis aufgenommene akademische Titel (Dr) werden nicht im surname aufgenommen.
CN (common name)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN) Nur falls der vollständige Name in ein Zertifikat im HBA nicht aufgenommen werden kann (z.B. weil er zu lang ist), muss der commonName als Pseudonym gekennzeichnet werden. Der commonName enthält den vollständigen Namen des Zertifikatnehmers, ohne akademische Titel (auch wenn sie im Personalausweis des Antragstellers eingetragen sind). Die Länge des Attributes ist auf 64 Zeichen beschränkt. Falls der vollständige Name nicht aufgenommen werden kann (z. B. weil er zu lang ist), dann muss, nur dann wenn dies aus gesetzlichen Bestimmungen hervorgeht, der commonName als Pseudonym gekennzeichnet werden. In diesem Fall wird der Zusatz „:PN" (ohne Anführungsstrichen) aufgenommen; die effektive Länge reduziert sich damit auf 61 Zeichen. Falls eine Kürzung vorgenommen werden soll, entsprechen die Kürzungsregeln den Regelungen in der eGK-Spezifikation: ▪ erster "Givenname" und „Surname" bleiben vollständig, sonstige Vornamen werden auf den ersten Buchstaben plus Punktzeichen gekürzt, ▪ falls immer noch >61 bzw. 64 Zeichen: sonstige Vornamen werden gestrichen, ▪ falls immer noch >61 bzw. 64 Zeichen: der Nachname wird gekürzt und mit Punktzeichen gekennzeichnet, so dass die Gesamtlänge (ggf. inkl. :PN) 64 Zeichen beträgt

DN-Bestandteil	Interpretation
serialNumber	Seriennummer: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Um eine Unterscheidung bei Namensgleichheit zu gewährleisten, wird das Feld serialNumber verwendet. Um unterschiedliche Namen im globalen LDAP-Tree über alle TSP zu erreichen, sind zweistellige Prefixe definiert und den TSP zugewiesen. Das serialNumber-Feld aller Zertifikate für HBAs, die durch den von der D-Trust GmbH betriebenen TSP ausgestellt werden, beginnt mit dem zugewiesenen Prefix „10" (ohne Anführungszeichen). Alle Zertifikate eines HBA erhalten die gleiche Nummer im serialNumber-Feld wie das Zertifikat für qualifizierte Signaturen dieses HBA.
C (country)	Das aufzuführende Land wird gemäß [ISO 3166] notiert. Beim HBA ist im DistinguishedName keine Organisation O aufgeführt, daher wird das Land aufgenommen, dass das Dokument ausgestellt hat, mit dem der Zertifikatnehmer identifiziert wurde. Das Attribut countryName enthält den ISO-3166 Code des Landes, also DE, kodiert als printableString.

QCP-n-qscd

Qualifizierte Zertifikate für natürliche Personen enthalten mindestens die subject-DN-Bestandteile „CommonName", „Country", „subjectSerialNumber" sowie entweder „GivenName" und „Surname" oder „Pseudonym".

SubjectDN Felder für X.509-nonQES–Zertifikate für die SMC-B

SubjectDN der X.509-nonQES –Zertifikate für die SMC-B werden entsprechend [gemSpec_PKI#Anhang A] befüllt.

Folgende Felder des SubjectDN werden für alle X.509-nonQES –Zertifikate Sektor übergreifend für die SMC-B verwendet:

- countryName
- serialnumber

Alle anderen Felder sind Sektor spezifisch (KZBV, KBV, DKG).

Der eindeutige Identitätsschlüssel der Organisation oder Einrichtung des Gesundheitswesens wird durch die Telematik-ID in der Zertifikatserweiterung „Admission" abgebildet.

DN-Bestandteil	Interpretation
G (given name)	▪ **KZBV** Kein Wert ▪ **KBV** Vorname des Verantwortlichen/ Inhabers ▪ **DKG** nicht belegt
SN (surname)	▪ **KZBV** Kein Wert ▪ **KBV** Nachname des Verantwortlichen/ Inhabers ▪ **DKG** nicht belegt
Title	▪ **KZBV** Kein Wert ▪ **KBV** Titel des Verantwortlichen/ Inhabers ▪ **DKG** nicht belegt
CN (common name)	▪ **KZBV** - Gemäß Freigabedaten der zuständigen KZV - Der commonName beinhaltet den „Kurzname" der Institution, so wie er sich selbst nach [DIN5008] auf dem Anschriftenfeld findet. (Zeilen 1-2, ggf +3-4). Überlange Attribute des SubjectDN werden zusätzlich in der Extension „SubjectAltNames" in voller Länge abgebildet. ▪ **KBV** Der commonName beinhaltet den „Kurzname" der Institution, so wie er sich selbst nach [DIN5008] auf dem Anschriftenfeld findet. (Zeilen 1-2, ggf +3-4). Überlange Attribute des SubjectDN werden zusätzlich in der Extension „Sub-jectAltNames" in voller Länge abgebildet. ▪ **DKG** Gemäß Freigabedaten der DKTIG

DN-Bestandteil	Interpretation
serialNumber	Seriennummer: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt. Die serialNumber wird als technisches Unterscheidungsmerkmal mit den 10 letzten Ziffern der ICC Serial Number (Chipkarten-Seriennummer) der SMC-B belegt.
C (country)	Das Attribut countryName enthält den ISO-3166 Code des Landes, also DE, kodiert als printableString.
O (organization Name)	▪ **KZBV** Gemäß Freigabedaten der zuständigen KZV (Telematik-ID). ▪ **KBV** - 9-stellige Betriebsstättennummer (z.B.„121234512") der Praxis als eindeutige Nummer. - Für privat abrechnende Ärzte wird hier eine 10-stellige Ersatznummer eingefügt. ▪ **DKG** Abgeleitet aus dem Institutionskennzeichen eines Krankenhauses.
Street	▪ **KZBV** Kein Wert ▪ **KBV** Strasse, Hausnummer der Anschrift. ▪ **DKG** Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)
PostalCode	▪ **KZBV** Kein Wert ▪ **KBV** Postleitzahl der Anschrift. ▪ **DKG** Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)
Locality	▪ **KZBV** Kein Wert ▪ **KBV** Stadt des Standortes ▪ **DKG** Stadt des Intitut-Standortes
State or ProvinceName	▪ **KZBV** Kein Wert ▪ **KBV** Bundesland des Standortes ▪ **DKG** Bundesland des Intitut-Standortes

Es müssen nicht alle genannten DN-Bestandteile verwendet werden. Weitere können ergänzt werden. Ergänzende DN-Bestandteile müssen [RFC 5280], [RFC 6818] und ETSI [ETSI EN 319 412] entsprechen.

3.1.5 Eindeutigkeit von Namen

Der TSP stellt sicher, dass ein in EE-Zertifikaten verwendeter Name (DistinguishedName) des Zertifikatnehmers bzw. des Endanwenders (Feld subject) innerhalb dieser PKI stets dem gleichen Zertifikatnehmer bzw. Endanwender zugeordnet ist.

Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer und Herausgeber (issuer) erzielt.

Der TSP stellt die Eindeutigkeit von distinguished names 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 Zertifikatsrichtlinie der D-TRUST GmbH, Abschnitt 9.5).

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Siehe [Abschnitt 4.4.1], [gemRL_TSL_SP_CP#4.2.1], [CP-HBA# 3.3.4f].

Der Zertifikatsnehmer (Karteninhaber) muss den Erhalt von HBA bzw. SMC-B dem TSP revisionssicher bestätigen.

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

3.2.2 Identifizierung und Authentifizierung von Organisationen

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

Wird der Antrag im Auftrag einer juristischen Person gestellt, muss der Vertreter seine diesbezügliche Berechtigung nachweisen und sich authentifizieren.

SMC-B
Für die Prüfung der Identität eines SMC-B Antragstellers werden keine Identitätsverfahren durch eine externe Stelle durchgeführt. Im Rahmen der Freigabe wird die Praxiszugehörigkeit und somit die Berechtigung zur Antragstellung eines SMC-B geprüft.

Die vorgestellten Prüfverfahren werden 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.

Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [EN 319 411-1] je nach Anwendbarkeit oder [EN 319 411-2]. Die Prüfung erfasst alle DN-Bestandteile.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

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

HBA

Die Prüfung der Identität des Antragstellers erfolgt mit den Verfahren Pers-Ident bzw. KammerIdent mit Hilfe der jeweiligen Kammer.

Die vorgestellten Prüfverfahren werden 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.

	HBA (QCP-n-qscd)
G	Pers-Ident/ KammerIdent
SN	
CN	

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatnehmer

Die Angaben des Zertifikatnehmers werden entsprechend den Abschnitten 3.2.2, 3.2.3 und 4.2.1 geprüft bzw. nicht geprüft. Andere Angaben zum Zertifikat wie Adressen von Internetseiten und LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Im Rahmen der Antragstellung wird die Prüfung der Berechtigung des Antragstellers auf einen HBA durchgeführt. Dabei werden Identitätsnachweis und Kammerzugehörigkeit mittels der Verfahren gemäß Abschnitt 3.2.3 ermittelt und geprüft bzw. bestätigt s. [CP-HBA# 3.3.2.1].

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 und Schlüsseln sowie einer entsprechenden Karte (HBA oder SMC-B) für denselben Karteninhaber.

Bei Anträgen zur Schlüsselerneuerung eines HBA kann auf eine erneute Identifizierung des Antragstellers verzichtet werden, sofern die vorherige Identifizierung noch gemäß [eIDAS] verwendbar ist. Die Attributsbestätigungen sind jedoch zu erneuern.

Eine Prüfung der Berechtigung zur Antragsstellung auf Schlüsselerneuerung eines HBA oder einer SMC-B wird jedoch vorgenommen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der TSP prüft vor der Sperrung eines Zertifikats die Berechtigung des Sperrantragstellers.

Die Sperrberechtigung wird wie folgt geprüft:

- Bei einer Sperrung durch den Kartenherausgeber über das Freigabeportal muss der Antrag ggf. qualifiziert signiert sein. Die Gültigkeit der Signatur wird zusätzlich zur Authentifizierung genutzt.
- Der Karteninhaber kann über das Antragsportal die Sperrung beantragen. Die Sperrberechtigung wird mittels SMS-TAN oder Servicepasswort geprüft.

Sperrverfahren werden in Abschnitt 4.9 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

Anträge auf Ausstellung eines Zertifikats (für einen HBA oder eine SMC-B) bzw. auf Herausgabe eines HBA oder einer SMC-B dürfen von natürlichen Personen und juristischen Personen (deren autorisierten Vertretern) gestellt werden.

Antragsberechtigt für X.509-nonQES-Zertifikate der SMC-B sind Institutionen (juristische Personen) des Gesundheitswesens, vertreten durch nachgewiesen vertretungs- / zeichnungsberechtigte natürliche Personen.

Siehe [gemRL_TSL_SP_CP#5.1.1 (GS-A_4199)], [CP-HBA# 3.3.2.1e].

Der Kartenherausgeber hat die Pflicht, seinerseits verwalteten Antragstellern die Beantragung eines Heilberufsausweises bei jedem Anbieter, der für seinen Sektor zugelassen ist, zu ermöglichen.

Siehe [gemRL_TSL_SP_CP#5.12.2 (GS-A_4246)], [CP-HPC#2.1].

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

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Einhaltung des Registrierungsprozesses gewährleistet der TSP. Teilaufgaben können von vertraglich gebundenen Partnern oder externen Anbietern übernommen werden, die die Maßgaben der CP der D-TRUST GmbH und dieses CPS erfüllen.

Dem Zertifikatsnehmer stehen bereits zu Beginn des Registrierungsprozesses CP, CPS und Verpflichtungserklärung sowie weitere Dokumente zur Verfügung, um ihm zu ermöglichen, sich über die Bedingungen für die Verwendung des gewählten Zertifikats zu informieren. Dies erfolgt im Rahmen des Antragprozesses auf Herausgabe eines HBA oder einer SMC-B.

Siehe [gemRL_TSL_SP_CP#5.1.2], [CP-HPC# 3.3.2.1].

QCP-n-qscd

Dem Zertifikatnehmer liegen vor Abschluss des Registrierungsprozesses CP, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Zertifikatnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [EN 319 411-1] und [EN 319 411-2]. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Zertifikatnehmers zur Veröffentlichung oder Nicht-Veröffentlichung der Zertifikate. Nachweise werden elektronisch oder papierbasiert hinterlegt. Die Verpflichtungserklärung entspricht dem „Subscriber Agreement" gemäß den Vorgaben aus [GL-BRO].

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

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

Siehe [gemRL_TSL_SP_CP#5.2.1], [CP-HPC# 3.3.2.1].

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

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

Der TSP definiert die folgenden Prüfverfahren für die Beantragung qualifizierter Zertifikate für den HBA:

Pers-Ident

Die natürliche Person muss sich gegenüber einer RA oder einem zugelassenem Partner (im Fall von Postident Mitarbeiter der Filiale der DPAG) oder einem externen Anbieter, der die Maßgaben des CPS erfüllt, anhand eines gültigen amtlichen Ausweises persönlich authentifizieren. Zulässige Dokumente sind Personalausweis oder Reisepass bei Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes, oder Dokumenten mit gleichwertiger Sicherheit. Nachweise werden hinterlegt. Die Bestätigung der Berufsgruppe erfolgt über das Freigabeportal.

KammerIdent

Mit einem ausgedruckten Antrag begibt sich der Antragssteller zu der ihm zugeordneten Kammer (Kartenherausgeber). Dort führt der dortige Identifikationsmitarbeiter eine Identifizierung anhand des Personalausweises durch. Bei einer erfolgreichen Identifikation bestätigt der Identifikationsmitarbeiter die korrekten Antragsdaten.

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

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die Annahme eines Antrags auf Ausstellung eines Zertifikats (für einen HBA oder eine SMC-B) bzw. auf Herausgabe eines HBA oder einer SMC-B erfolgt nur für identifizierte Antragsteller mit berechtigtem Antrag (s. [gemRL_TSL_SP_CP#5.2.2]. In allen anderen Fällen wird der Antrag abgelehnt.

Ein SMC-B Antrag ist genehmigt, wenn der Kartenherausgeber über das Freigabeportal seine Genehmigung erteilt.

Im Falle eines HBA Antrags prüft eine vom TSP beauftragte "unabhängige zweite" Person die Antragsunterlagen nach folgenden Kriterien:

- wurde die Authentifizierung des Zertifikatnehmers korrekt durchlaufen und dokumentiert,
- wurden alle notwendigen Nachweise erbracht,

- liegen Gründe vor, die eine Ablehnung des Antrags nahe legen.

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

Weitere Gründe für die Antragsablehnung können sein:

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

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

Erst nachdem der TSP den Zertifikatsantrag positiv überprüft hat, der Kartenherausgeber über das Freigabeportal den Datensatzes freigegeben 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 TSP bei der Ausstellung von Zertifikaten

Im Hochsicherheitsbereich des Trustcenters werden die entsprechenden Zertifikate ausgefertigt.

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

Die vollständige Antragsdokumentation wird entweder vom TSP gemäß Abschnitt 5.5 revisionssicher archiviert oder der TSP schließt vertragliche Vereinbarungen mit Partnern, dass die Antragsunterlagen und/oder Requests sicher und vollständig bis zum Ablauf der Frist nach Abschnitt 5.5.2 zu verwahren sind.

4.3.2 Benachrichtigung des Zertifikatnehmers über die Ausstellung des Zertifikats

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

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Karten (HBA oder SMC-B) werden an die angegebene Adresse per Briefdienstleister oder Kurier versendet. Der Antragsteller hat den Erhalt der Karte (HBA oder SMC-B) gegenüber dem TSP zu bestätigten.

Siehe [gemRL_TSL_SP_CP#5.3.4], [CP-HBA#3.3.4f].

Entdeckt der Zertifikatnehmer Fehler in seinen Zertifikaten oder bei der Funktion der Schlüssel und Karte (HBA oder SMC-B), so hat er dies dem TSP mitzuteilen. Alle zur Karte gehörenden

Zertifikate werden gesperrt. Nach erfolgter Sperrung kann der TSP verlangen, dass die Karte vom Zertifikatnehmer an den TSP zurückgesendet wird.

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

QCP-n-qscd

Der TSP verwendet ausschließlich qualifizierte Signaturerstellungseinheiten und überwacht während der Gültigkeit der ausgegebenen qualifizierten Zertifikate den Status dieser qualifizierten Signaturerstellungseinheiten im Sinne EN 319 411-2. Die PIN wird separat an den Endanwender übergeben.

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

4.4.2 Veröffentlichung des Zertifikats durch den TSP

Hat der Zertifikatnehmer im Zertifikatsantrag der Veröffentlichung der Zertifikate zugestimmt, werden die Zertifikate (HBA oder SMC-B) nach der Produktion in den öffentlichen Verzeichnisdienst eingestellt. Hat der Zertifikatnehmer die Veröffentlichung abgelehnt, wird das Zertifikat nicht veröffentlicht.

Der Status des Zertifikats ist nach Ausgabe des Zertifikats in Abhängigkeit vom Herausgeber der Karte über CRLs oder OCSP abrufbar (siehe Abschnitt 2.1) und

(s. [gemRL_TSL_SP_CP#5.4.2], [CP-HPC# 3.3.5]).

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Der TSP informiert den Kartenherausgeber einer über den Zertifikatsstatus:

- Freischaltung der Zertifikate
- Sperrung der Zertifikate

Siehe [CP-HPC# 3.3.4e], [gemRL_TSL_SP_CP#5.3.5].

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.

Nach Ablauf des Gültigkeitszeitraums oder nach Sperrung der Karte (HBA oder SMC-B) dürfen die zugehörigen privaten Schlüssel nicht mehr genutzt werden. Der Karteninhaber muss auch nach Ablauf des Gültigkeitszeitraums dafür sorgen, dass die privaten Schlüssel nicht missbräuchlich verwendet werden können.

Bei Entsorgung muss die Karte sicher vernichtet bzw. unbrauchbar gemacht werden (beispielsweise durch physische Zerstörung der Karte).

Für Zertifikatnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatnutzer

Die Zertifikate aus dieser PKI können von allen Zertifikatnutzern verwendet werden. Es kann jedoch nur dann darauf vertraut werden, wenn

- die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Extentions) benutzt werden,
- die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt werden kann[4],
- der Status der Zertifikate über den Statusabfragedienst (OCSP) positiv geprüft wurde und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifische Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

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. Eine Zertifikatserneuerung ist nicht möglich.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Bei CA-Schlüsseln wird keine Zertifikatserneuerung durchgeführt.

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. Dies erfordert die Herausgabe einer neuen Karte (HBA oder SMC-B) bzw. einer Ersatzkarte und wird vom TSP wie die Erstbeantragung eines Zertifikats behandelt. Die weiteren Zertifikate, die zur Karte gehören (auch qualifizierte Zertifikate), werden dann ebenfalls mit Schlüsselerneuerung erneuert werden.

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 die aktuelle CP der D-Trust GmbH und dieses CPS.

4.7.1 Bedingungen für eine Zertifikatserneuerung

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

---

[4] 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 ETSI [ETSI EN 319 412], Part 5.

Voraussetzung ist, dass das Zertifikat für denselben Endanwender ausgestellt wird. Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Zertifikatserneuerung noch gültig sein oder geprüfte Daten und Nachweise sind für die Erneuerung vorhanden und verwendbar. Zertifikatnehmer 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 Zertifikatnehmer 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 dem Verfahren in Abschnitt 3.2.2. Wurde die Organisationszugehörigkeit widerrufen, muss sie ggf. erneut nachgewiesen werden, andernfalls wird die Organisation nicht wieder ins Zertifikat auf genommen.

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

4.7.2 Berechtigung zur Zertifikatserneuerung

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

4.7.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Es gelten die in Abschnitt 4.3 festgelegten Regelungen.

Zertifikatnehmer, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, nutzen das Antragsportal des TSP zur Antragstellung.

https://ehealth.d-trust.net/antragsportal/

4.7.4 Benachrichtigung des Zertifikatnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die in Abschnitt 4.3.2 festgelegten Regelungen.

4.7.5 Verhalten bei der Ausgabe einer Zertifikatserneuerung

Es gelten die in Abschnitt 4.4.1 festgelegten Regelungen.

4.7.6 Veröffentlichung der Zertifikatserneuerung durch den TSP

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen, je nach Angaben im Erstantrag.

Der Zertifikatnehmer kann seine Entscheidung zur Veröffentlichung ändern.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Die Verfahren des TSP erfüllen die Bedingungen aus [EN 319 411-1].

QCP-n-qscd
Die Verfahren des TSP erfüllen die Bedingungen aus [EN 319 411-2].

Zertifikatnehmer oder betroffenen Dritte sind aufgefordert, die Sperrung unverzüglich zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden oder Inhaltsdaten des Zertifikats nicht mehr korrekt sind.

Die Sperrung eines Zertifikats führt unmittelbar zur Sperrung der entsprechenden Karte (HBA oder SMC-B) und aller zur Karte gehörenden weiteren Zertifikate (auch der qualifizierten).

Die Sperrung eines Zertifikats wird bei folgenden Ereignissen durchgeführt:

- auf Verlangen des Zertifikatnehmers bzw. der zuständigen Kammer/ des Kartenherausgebers,
- Ungültigkeit von Angaben im Zertifikat,
- wenn der TSP seine Tätigkeit beendet und diese nicht von einem anderen TSP fortgeführt wird.

Unabhängig davon kann der TSP Sperrungen veranlassen, wenn:

- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- das Schlüsselpaar sich auf einem HBA befindet, auf der gleichzeitig andere Schlüssel liegen, welche gesperrt werden,
- 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 oder anderweitig missbraucht wurde,
- der Kunde nach zweimaliger Mahnung mit dem Entgelt in Verzug ist bzw. gegen die anwendbare AGB verstoßen hat,
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde.

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

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zur Sperrung

Der TSP ist sperrberechtigt.

Er führt Sperrungen im Rahmen eines definierten Incident-Prozesses mit den zuständigen und betroffenen Parteien aus.

Der Zertifikatnehmer hat stets ohne Angabe von Gründen die Berechtigung zur Sperrung seiner Zertifikate. Ein solcher, welcher über eine Karte (HBA oder SMC-B) verfügt und hierfür einen Sperrantrag stellt, wird im folgenden Sperrantragsteller_AS genannt.

Die weiteren zur Sperrung von Zertifikaten (HBA oder SMC-B) berechtigten Stellen (z.B. Vertreter des Kartenherausgebers und der Attribute bestätigenden Stellen) werden im folgenden Sperrantragsteller_KHG genannt. Sperrantragsteller_KHG können somit sein:

- Benutzer des Freigabeportals mit entsprechender Berechtigung,
- Leiter oder als sperrberechtigt gemeldete Mitarbeiter einer Identifizierungsstelle des KHG,
- Leiter oder als sperrberechtigt gemeldete Mitarbeiter einer attributbestätigenden Stelle des KHG.

Siehe [gemRL_TSL_SP_CP#5.8.9], [CP-HBA#3.3.7].

4.9.3 Verfahren für einen Sperrantrag

Ein Sperrantrag für die Sperrung einer Karte (HBA oder SMC-B) führt zur Sperrung aller sperrfähigen Zertifikate der betroffenen Karte. Ein Sperrantrag für ein Zertifikat ist umgekehrt automatisch ein Sperrantrag für die entsprechende Karte. Der TSP sperrt auch in diesem Fall alle anderen, sperrfähigen Zertifikate.

Für die Sperrung eines HBAs werden den Sperrantragstellern verschiedene Wege der Kartensperrung bereitgestellt. In der folgenden Tabelle sind den Sperrantragstellern die durch sie verwendbaren Sperrwege zugeordnet.

Sperrung durch	Sperrwege für HBA und SMC-B
Sperrantragsteller_AS	▪ Antragsportal https://ehealth.d-trust.net/antragsportal/
Sperrantragsteller_KHG	▪ Freigabeportal https://ehealth.d-trust.net/freigabeportal/ ▪ SOAP-Schnittstelle (technische Schnittstelle)

Tabelle 1: Übersicht Sperrwege der Sperrantragsteller

Technische Angaben zu Freigabeportal und SOAP-Schnittstelle werden dem Sperrantragsteller_KHG bei seiner Erfassung mitgeteilt.

Sperrungen finden im Verantwortungsbereich des TSP statt. Ungeachtet dessen kann der TSP Teilaufgaben an vertraglich gebundene Dritte weiter geben. Die Sperrdienstleistung kann von Dritten übernommen werden, die nach den Maßgaben des TSP handeln.

Die vom Sperrantragsteller angegebenen Sperrgründe werden dokumentiert. Nach erfolgter Sperrung wird der Zertifikatnehmer, der Kartenherausgeber sowie ggf. die Attribut bestätigende Stelle über die Sperrung informiert (s. [CP-HBA#3.3.7]).

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

4.9.4 Fristen für einen Sperrantrag

Der Zertifikatnehmer oder ein sperrberechtigter Dritter muss in eigener Verantwortung dafür sorgen, dass er oder eine für ihn sperrberechtigte Person unverzüglich die Sperrung beantragt, sobald Gründe zur Sperrung bekannt werden.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Anträge per Antragsportal, Freigabeportal, SOAP-Schnittstelle werden spätestens am folgenden Arbeitstag bearbeitet.

QCP-n-qscd

Die Sperrung erfolgt umgehend nach erfolgreicher Autorisierung des Sperrantragstellers per SMS-TAN oder Servicepasswort.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

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

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

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

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Siehe Abschnitt 2.3.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden unmittelbar nach ihrer Erzeugung veröffentlicht.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

Zur Onlineprüfung steht ein 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. Die Formate und Protokolle der Dienste sind in den Abschnitten 7.2 und 7.3 beschrieben.

Die Systemzeit des OCSP-Responder wird über DCF77 täglich gegen die offizielle Zeit synchronisiert.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst ist 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. Der Sperrauftrag zu einem Zertifikat durch Zertifikatnehmer oder Sperrberechtigte Dritte löst die Sperrung durch den TSP aus. Die vertraglichen Hauptleistungspflichten des TSP sind damit vollständig erfüllt.

4.12 Schlüsselhinterlegung und –wiederherstellung

Nicht relevant

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Nicht relevant

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Nicht relevant

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die HBA-CA[5] und SMCB-CA[5], die bei der D-TRUST GmbH gemäß [EN 319 411-1] und [EN 319 411-2] betrieben werden.

5.1 Bauliche Sicherheitsmaßnahmen

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine anerkannte Prüf- und Bestätigungsstelle geprüft. Die Prüfung und Bestätigung wird gemäß [EN 319 411-1] und [EN 319 411-2] regelmäßig wiederholt.

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

Die CAs der hier behandelten PKI werden vom TSP unter den gleichen Bedingungen betrieben wie die CAs der D-TRUST GmbH zur Ausstellung qualifizierter Zertifikate.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

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

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

5.2.2 Mehraugenprinzip

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

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

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

[5] Siehe PKI Struktur in Kapitel 1.1.3 Abbildung 1 und Abbildung 2.

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

5.2.4 Rollenausschlüsse

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Verhalten vorzubeugen.

5.3 Eingesetztes Personal

Der TSP erfüllt die Anforderungen an das Personal aus [EN 319 411-1] und [EN 319 411-2].

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

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

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft. Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit. Schulungen und Leistungsnachweise werden dokumentiert.

5.3.2 Sicherheitsprüfungen

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

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

5.3.3 Schulungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind.

5.3.4 Häufigkeit von Schulungen und Belehrungen

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

5.3.5 Häufigkeit und Folge von Job-Rotation

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult.

5.3.6 Maßnahmen bei unerlaubten Handlungen

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

5.3.7 Anforderungen an freie Mitarbeiter

Entfällt; freie Mitarbeiter werden nicht eingesetzt.

5.3.8 Ausgehändigte Dokumentation

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

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts

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

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

5.4.2 Überwachung von organisatorischen Maßnahmen

Ein weiterer Bestandteil ist die Überwachung von organisatorischen Maßnahmen.

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

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

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden.

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

5.5.2 Aufbewahrungsfristen für archivierte Daten

Dokumente zur Antragstellung und Prüfung sowie die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden mindestens zehn Jahre und bis zum Jahresende aufbewahrt[6]. Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

---

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

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

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

5.5.3 Sicherung des Archivs

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

5.5.4 Datensicherung des Archivs

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

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Der TSP betreibt keinen Zeitstempeldienst in der Telematikinfrastruktur des Gesundheitswesens.

5.5.6 Archivierung (intern / extern)

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

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

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

5.6 Schlüsselwechsel beim TSP

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

5.7 Kompromittierung und Geschäftsweiterführung beim TSP

5.7.1 Behandlung von Vorfällen und Kompromittierungen

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

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren.

5.7.3 Kompromittierung des privaten CA-Schlüssels

Im Fall einer Kompromittierung oder der Bekanntgabe von Unsicherheit von Algorithmen oder assoziierten Parametern durch die Herausgeber der maßgeblichen Kataloge nach Abschnitt 0, veranlasst der TSP folgendes:

- betroffenen CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden gesperrt,

- involvierte Zertifikatnehmer werden über den Vorfall und dessen Auswirkungen informiert,
- die zuständige Aufsichtsstelle wird informiert und der Vorfall wird auf den Webseiten des TSP veröffentlicht mit dem Hinweis, dass Zertifikate, die von dieser CA ausgestellt wurden, ihre Gültigkeit verlieren.

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

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach Kompromittierung und Desaster

In einem Notfall entscheidet der TSP je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 6.2.4 beschriebene Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 0 verfahren wird.

5.8 Schließung des TSP

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

Der Verzeichnisdienst und Dokumente zur Antragstellung von X.509-QES-Zertifikaten werden an die Bundesdruckerei GmbH übergeben und unter äquivalenten Bedingungen weitergeführt. Die Aufrechterhaltung des Verzeichnisdienstes wird bis Ablauf der Gültigkeit des X.509-QES-Zertifikats zugesichert und entweder einem anderen TSP oder der Bundesdruckerei GmbH übergeben.

Der TSP verfügt über eine entsprechende Zusicherung der Bundesdruckerei für die Erfüllung dieser Mindestanforderungen.

Der Verzeichnisdienst und Dokumente zur Antragstellung von X.509-nonQES-Zertifikaten werden an die gematik mbH übergeben und unter äquivalenten Bedingungen weitergeführt.

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

D-TRUST verfügt über einen fortlaufend aktualisierten Beendigungsplan.

6. Technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die PKI-Dienste, die in diesem CPS behandelt werden und bei der D-TRUST GmbH betrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel werden in einem „FIPS 140-2 Level 3" konformen Hardware Security Module (HSM) erzeugt. Das HSM befindet sich im Hochsicherheitsbereich des Trustcenters. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip erzwungen. Bei der Erzeugung von CA-Schlüsseln ist stets ein unabhängiger Auditor anwesend oder der Auditor kann sich nach der Schlüsselerzeugung durch eine Videoaufzeichnung vom ordnungsgemäßen Ablauf der Schlüsselerzeugung überzeugen. Weiterhin wird die Erstellung von CA-Schlüsseln gemäß [EN 319 411-1] bzw. [EN 319 411-2] dokumentiert.

QCP-n-qscd

Werden EE-Schlüssel vom TSP erzeugt, werden diese mit Hilfe eines HSMs oder auf einer qualifizierten Signaturerstellungseinheit in der sicheren Umgebung des Trustcenters erzeugt und entsprechen den Vorgaben aus [EN 319 411-2].

Werden EE-Schlüssel und EE-Zertifikate auf Chipkarten oder anderen hardwarebasierten Token erzeugt oder aufgebracht, verfährt der TSP bei der Beschaffung, Lagerung, Personalisierung und beim PIN-Handling gemäß den entsprechend anwendbaren Vorgaben des Herstellers oder des Zertifizierers der Chipkarte bzw. des Tokens.

6.1.2 Lieferung privater Schlüssel an Zertifikatnehmer

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

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

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

Nicht relevant.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Der öffentliche Schlüssel der ausstellenden CA ist im Zertifikat enthalten. Dieses Zertifikat befindet sich i. d. R. auf der Karte (HBA oder SMC-B), die dem Zertifikatnehmer übergeben wird. Darüber hinaus können die CA-Zertifikate aus dem öffentlichen Verzeichnis bezogen werden, in dem sie nach ihrer Erstellung veröffentlicht werden.

6.1.5 Schlüssellängen

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

Für EE-Zertifikate auf HBA und SMC-B werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit verwendet.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

CA- und EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die den Vorgaben der Gematik in der aktuell gültigen Fassung entsprechen, soweit Kompatibilität im Verwendungsumfeld gewährleistet ist.

QCP-n-qscd

EE-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die zusätzlich zu [ETSI-ALG] auch [EN 319 411-2] in der aktuell gültigen Fassung entsprechen.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 7.1.3 genannt.

6.1.7 Schlüsselverwendungen

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

Die EE-Schlüssel dürfen nur für die im Zertifikat benannten Nutzungsarten verwendet werden. Die Nutzungsarten werden in den Feldern *KeyUsage* und *ExtKeyUsage* im Zertifikat definiert und ggf. durch weitere Extentions eingeschränkt (siehe Abschnitt 7.1.2).

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

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

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

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

6.2.3 Das 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. Hinterlegung privater Schlüssel (key escrow)

Private CA- und EE-Schlüssel, die die Anforderungen nach [EN 319 411-1] oder [EN 319 411-2] erfüllen, werden nicht hinterlegt.

6.2.4 Backup privater Schlüssel

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

6.2.5 Archivierung privater Schlüssel

Private CA- und EE-Schlüssel werden nicht archiviert.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

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

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten CA-Schlüssel liegen verschlüsselt im HSM vor.

6.2.8 Aktivierung privater Schlüssel

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

Private EE-Schlüssel werden durch Eingabe der PIN aktiviert.

6.2.9 Deaktivieren privater Schlüssel

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

Die jeweilige Anwendung deaktiviert den privaten EE-Schlüssel, spätestens aber das Ziehen der Karte aus dem Kartenleser.

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

6.2.10 Zerstörung privater Schlüssel

Nach Ablauf der Gültigkeit der privaten CA-Schlüssel werden diese gelöscht. Dies erfolgt durch Löschen auf dem HSM und gleichzeitigem Löschen der auf Datenträgern angelegten Backups. Bei Stilllegung des HSMs werden die privaten Schlüssel auf dem Gerät gelöscht.

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

6.2.11 Beurteilung kryptographischer Module

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

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

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

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer der CA-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt 8 Jahre.

Die Gültigkeitsdauer der EE-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt 5 Jahre.

QCP-n-qscd

EE-Zertifikate werden mit einer maximalen Gültigkeit von 63 Monaten ausgestellt. Eine längere Gültigkeit kann vertraglich vereinbart werden.

Wird ein Zertifikat für einen längeren Zeitraum als 24 Monate ausgestellt, trägt der Kunde danach das Risiko eines aus sicherheitstechnischen Gründen erforderlichen Austausches.

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.

Erzeugt der TSP die Schlüssel, wird entweder ein Transport-PIN-Verfahren genutzt oder die PINs werden in einen PIN-Brief gedruckt und an den Zertifikatnehmer versandt.

6.4.2 Schutz von Aktivierungsdaten

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

Zertifikatnehmer: Beim Transport-PIN-Verfahren ist die Unversehrtheit der Karte über die Transport-PIN erkennbar. In anderen Verfahren werden die PINs einmalig in einen besonders gesicherten PIN-Brief gedruckt und an den Zertifikatnehmer versandt.

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.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom TSP eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die nicht im Widerspruch zu der CP der D-TRUST GmbH und [EN 319 411-1] bzw. [EN 319 411-2] und den Vorgaben der Telematikinfrastruktur der Gematik stehen.

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

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

Zertifikatnehmer und Zertifikatsnutzer müssen vertrauenswürdige Computer und Software verwenden.

6.5.2 Beurteilung von Computersicherheit

Die für die CA-Schlüssel eingesetzten Computer, Netze und andere Komponenten wurden durch anerkannte Prüf- und Bestätigungsstellen geprüft und unterliegen gemäß [EN 319 401] einem entsprechenden Monitoring.

6.5.3 Monitoring

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

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

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

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

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich entsprechend dem Rollenkonzept autorisiertes Personal darf Computer, Netze und andere Komponenten administrieren. Es findet eine regelmäßige Auswertung von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle statt. Überwachungsmaßnahmen beginnen mit Inbetriebnahme eines Gerätes und enden mit dessen Entsorgung.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

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

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

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

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

6.7 Sicherheitsmaßnahmen für Netze

Im Betrieb der CAs wird ein Netzkonzept realisiert, welches sicherstellt, dass die relevanten CA-Systeme in besonders gesicherten Netzwerkzonen betrieben werden. Die Netzwerkarchitektur des TSP beinhaltet ein mehrstufiges Konzept der Netzwerksicherheitszonen. Die Root CAs werden in der Netzwerksicherheitszone mit dem höchsten Schutzbedarf betrieben. Für das Netzkonzept liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

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

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

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

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

6.8 Zeitstempel

Der TSP betreibt einen Zeitstempeldienst. 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 und gemäß EN 319 412-2 ausgegeben.

In dieser CPS wird das X.509-QES-Zertifikat des HBAs (C.HP.QES) gemäß [gemSpec_PKI#Anhang C] für den HBA beschrieben.

Zudem werden nicht-qualifizierte Zertifikate für den HBA für Ver- und Entschlüsselung sowie Authentisierung nach Benennungsschema [gemSpec_PKI#2] X.509-nonQES-Zertifikate erstellt:

- C.HP.ENC und
- C.HP.AUT.

Diese Zertifikate werden für die verschiedenen Berufsgruppen (Ärzte - BÄK, Zahnärzte - BZÄK, Psychotherapeuten - BPtK) erstellt.

Die Vorgaben für die X.509-QES- und X.509-nonQES–Zertifikate für den HBA sind in den folgenden Dokumenten beschrieben:

- Zertifikatsprofile für X.509 Basiszertifikate der Ärzte [baekCerts]
- Zertifikatsprofil des elektronischen Zahnarztausweises [bzaekCert]
- Gemeinsame Policy für die Herausgabe der HBA [CP-HBA]
- Die Vorgaben für den Inhalt der Felder SubjectDN der X.509-nonQES –Zertifikate für die SMC-B werden in [gemSpec_PKI#5.3] definiert.

Ferner werden X.509-nonQES-Zertifikate für die SMB-C jeweils für die drei Anwendungsfelder Ver- und Entschlüsselung, Authentisierung und Non-Repudiation erstellt, d.h. nach Benennenungsschema [gemSpec_PKI#2] X.509-nonQES-Zertifikate:

- C.HCI.ENC,
- C.HCI.AUT,
- C.HCI.OSIG.

Diese Zertifikate werden für die verschiedenen Sektoren KZBV, KBV und DKG erstellt.

Die Vorgaben für die X.509-nonQES –Zertifikate für die SMC-B werden in [gemSpec_PKI#5.3] definiert.

7.1.2 Zertifikatserweiterungen

Die Wahl der Erweiterung ist weitestgehend produktabhängig.

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

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

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

Erweiterung	OID	Parameter
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
CRLDistributionPoints	2.5.29.31	Adresse(n) der CRL-Ausgabestell(n)e
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}* *accessMethod=caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs
SubjectAltName	2.5.29.17	Alternativer Inhabername

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

EE-Zertifikate enthalten folgende *kritische* Erweiterungen:

Erweiterung	OID	Parameter
KeyUsage	2.5.29.15	Möglich sind: *digitalSignature, keyEncipherment, dataEncipherment, keyAgreement,*

EE-Zertifikate können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
ExtKeyUsage	2.5.29.37	Entsprechend [RFC 5280], [RFC 6818]
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
CRLDistributionPoints	2.5.29.31	CRL-Ausgabestelle als ldap-Adresse

Erweiterung	OID	Parameter
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}* *accessMethod= caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs *cpsURI*
SubjectAltName	2.5.29.17	Alternativer Inhabername
QCStatements (nur QCP-n-qscd und QCP-l-qscd) (nur relevant bei HBA nicht bei SMC-B)	*1.3.6.1.5.5.7.1.3*	esi4-qcStatement-1 {0 4 0 1862 1 1}; esi4-qcStatement-2 {0 4 0 1862 1 2}; esi4-qcStatement-4 {0 4 0 1862 1 4}; esi4-qcStatement-6: id-etsi-qct-esign {0 4 0 1862 1 6 1};

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.3 Algorithmen-OIDs

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

- RSA-PSS mit OID 1.2.840.113549.1.1.10.

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

- SHA512 RSA mit OID 1.2.840.113549.1.1.13,
- 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 5280], [RFC 6818] (kodiert als IA5String) stehen.

7.1.5 Name Constraints

„NameConstraints" wird nicht benutzt.

7.1.6 Certificate Policy Object Identifier

„CertificatePolicies" kann den OID unterstützter CPs enthalten.

Weitere Regelungen sind in der CP enthalten.

7.1.7 Nutzung der Erweiterung „PolicyConstraints"

„PolicyConstraints" wird nicht benutzt.

7.1.8 Syntax und Semantik von „PolicyQualifiers"

„PolicyQualifier" können benutzt werden.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung CertificatePolicies

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

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

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

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Sperrlisten können folgende unkritische Erweiterungen enthalten:

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

7.3 Profile des Statusabfragedienstes (OCSP)

Der OCSP-Responder unterstützt zusätzlich zu RFC 6960 auch Positivauskünfte.

7.3.1 Versionsnummer(n)

Es wird OCSP v1 gemäß [RFC 6960] eingesetzt.

7.3.2 OCSP-Erweiterungen

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

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

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

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

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

8. Auditierungen und andere Prüfungen

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

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

CP und CPS erfüllen für Zertifikate die Anforderungen gemäß [EN 319 411-1] bzw. [EN 319 411-2] Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten („competent independent party" gemäß [EN 319 411-1] bzw. [EN 319 411-2] belegt die Kompatibilität.

Der TSP gibt Zertifikate mit einer Policy-OID-Referenz auf [EN 319 411-1] und [EN 319 411-2] erst nach der initialen und erfolgreich abgeschlossenen Prüfung nach [EN 319 411-1] oder [EN 319 411-2] durch einen unabhängigen externen Zertifizierer aus. Es finden regelmäßige Wiederholungsprüfungen statt. Sollten sich die Verfahren als nicht mehr konform zu den aktuellen Richtlinien von [EN 319 411-1] oder [EN 319 411-2] erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde. Diese Auditierung findet jährlich statt.

Darüber hinaus finden regelmäßig interne Audits statt.

9. Sonstige finanzielle und rechtliche Regelungen

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