Certification Practice Statement
des Vertrauensdiensteanbieters DGN
Version 2.3

DGN Deutsches Gesundheitsnetz Service GmbH

Änderungshistorie

Version	Datum	Kommentar/Änderungen	Autor	Kapitel
0.9	13.06.2006	Initialversion	BN et al.	Entwurf
1.0	03.07.2006	Vervollständigung	Knut Goldberg, Robert Kurz	Freigegeben
1.1	21.05.2007	Einarbeitung Kommentare BNetzA	Robert Kurz	Entwurf
1.1	23.05.2007	Freigabe	Knut Goldberg	Freigegeben
1.2	01.08.2007	Einarbeitung Kommentare BNetzA	Knut Goldberg	Entwurf
1.2	01.08.2007	Freigabe	Robert Kurz	Freigegeben
2.0	24.06.2016	Anpassungen an eIDAS, Ergänzung Zeitstempeldienst	Knut Goldberg, Robert Kurz	Entwurf
2.0	24.06.2016	Freigabe	Knut Goldberg	Freigegeben
2.1	19.05.2017	Weitere Anpassungen an eIDAS, Ergänzung OID	Knut Goldberg, Robert Kurz	Freigegeben
2.2	13.12.2018	Entfernen SigG/SigV	Rainer Raunitschke	Entwurf
2.3	04.08.2023	Aktualisierung für neue Kartengeneration mit ECC	Knut Goldberg	Entwurf
2.3	28.08.2023	Freigabe	Ottke	Freigegeben

Inhaltsverzeichnis

1 Einleitung

Die DGN Deutsches Gesundheitsnetz Service GmbH (im Folgenden DGN) ist einer der marktführenden Telematik-Dienstleister für das deutsche Gesundheitswesen. Unsere Spezialgebiete sind die sichere elektronische Vernetzung sowie anwenderfreundliche IT- und Kommunikationslösungen, die Arbeitsabläufe im ambulanten und stationären Sektor effizienter machen.

DGN setzt beim Thema Sicherheit auf Public Key Infrastrukturen (PKI). Sie betreibt als (qualifizierter) Vertrauensdiensteanbieter verschiedene qualifizierte und nicht qualifizierte Vertrauensdienste und bietet dazu unterschiedliche Klassen von Zertifizierungsdienstleistungen an. Hierzu zählen insbesondere Zertifikate für die Anwendungen: Signatur, Authentisierung, Entschlüsselung und Siegel. Die hierbei verwendeten Klassen adressieren nicht nur unterschiedliche Zielgruppen und Mandanten, sondern beinhalten auch abgestufte Sicherheitsanforderungen bzw. Sicherheitsniveaus. Sofern im Folgenden nicht differenziert wird, steht der Begriff Zertifikat synonym für Zertifikate aller vorgenannten Anwendungen.

1.1 Überblick

Dieses Certification Practice Statement (CPS) enthält die Richtlinien für den Betrieb des Trustcenters der DGN als (qualifizierter) Vertrauensdiensteanbieter und der erbrachten (qualifizierten) Vertrauensdienste. Ferner werden in diesem Dokument Informationen über die Anwendung der angebotenen Zertifikate und Zeitstempel bereitgestellt.

Zertifikate werden entsprechend den vorgegebenen (Sicherheits-)Anforderungen in Zertifikatsklassen unterteilt. Dabei werden u.a. das Niveau der Identifikationsprüfung sowie die Sicherheit des Schlüsselmediums berücksichtigt. Sofern erforderlich, sind spezifische Informationen oder abweichende Festlegungen zu den einzelnen Zertifikatsklassen in speziellen Certificate Policies (CPs) aufgeführt.

Die hier beschriebenen Richtlinien gelten zusammen mit etwaigen Certificate Policies als Maßstab für das Niveau der Sicherheit des Trustcenters und der ausgestellten Zertifikate und Zeitstempel und bilden die Vertrauensgrundlage der Endteilnehmer und der Öffentlichkeit gegenüber den bereitgestellten Vertrauensdiensten.

Dieses Certification Practice Statement beschreibt die Umsetzung der gesetzlichen Anforderungen sowie der jeweiligen Certification Policy. Sie bezieht sich auf technische und organisatorische Sachverhalte, die sich nicht auf eine spezielle Zertifikatsklasse beschränken und gilt daher – sofern in ihr selbst keine Differenzierung vorgenommen wird - übergreifend für alle Certificate Policies.

Die Gliederung sowie die Empfehlungen des RFC 3647 (Version von November 2003) der IETF kommen zur Anwendung.

1.2 Identifikation des Dokumentes

Name: Certificate Practice Statement des Vertrauensdiensteanbieters DGN
Version: 2.3
Datum: 04.08.2023
Status: Freigegeben
OID: 1.3.6.1.4.1.15787.2.1.7.1
1.3.6.1.4.1.15787.2.1.7.1.1
1.3.6.1.4.1.15787.2.1.7.2.1
1.3.6.1.4.1.15787.2.1.7.2.2

1.3 Teilnehmer der Zertifizierungsinfrastruktur

Der Vertrauensdiensteanbieter ist die Firma DGN Deutsches Gesundheitsnetz Service GmbH, Düsseldorf. Es werden Vertrauensdienste sowohl speziell für Mitglieder des deutschen Gesundheitswesens aber auch allgemein für die Öffentlichkeit erbracht und entsprechende Zertifikate und Zeitstempel ausgestellt.

1.3.1 CAs

Mit den Vertrauensdiensten der DGN werden sowohl qualifizierte Zeitstempel als auch nicht qualifizierte Zertifikate und qualifizierte Zertifikate erzeugt. Entsprechend existieren unterschiedliche oberste Zertifizierungsstellen. Root-CAs des DGN Trustcenters für nicht qualifizierte Zertifikate und Zeitstempel sowie qualifizierte Zertifikate und Zeitstempel nach eIDAS sind jeweils eigene Wurzelinstanzen, d.h. diese Root-CA Schlüssel sind selbstsigniert.
CA-Zertifikate werden von der jeweiligen Root-CA (s.o.) zertifiziert. Von diesen CA´s abgeleitete Sub-CA´s werden nur dann ausgestellt, wenn dies in der jeweiligen CP explizit geregelt wird.
Die CAs der DGN zertifizieren die öffentlichen Schlüssel der Endteilnehmer.

1.3.2 RA

DGN als Vertrauensdiensteanbieter verfügt über eine Registrierungsstelle, die Endteilnehmer der Vertrauensdienste sowie Mitarbeiter des Trustcenters identifiziert. Darüber hinaus arbeitet DGN mit weiteren externen Identifizierungsstellen zusammen. Die externen Identifizierungsstellen sind an die Sicherheitsrichtlinien des Vertrauensdiensteanbieters DGN gebunden, so dass ein hohes Sicherheitsniveau garantiert wird.

1.3.3 Endteilnehmer

Die Vergabe von Zertifikaten richtet sich primär, aber nicht exklusiv, an Teilnehmer im Gesundheitswesen. Als Endteilnehmer gelten in diesem Zusammenhang natürliche Personen und Organisationen, die für sich selbst, aber auch für Systeme der Datenverarbeitung Zertifikate beantragen.

1.3.4 Relying Party

Zertifikatsnutzer sind alle natürlichen Personen oder Organisationen, die die Zertifikate oder Zeitstempel der DGN Vertrauensdienste nutzen.

1.4 Anwendungsbereich

Die Verwendung der vom Trustcenter der DGN erzeugten Zertifikate ergibt sich aus dem im Zertifikat selbst angegebenen Verwendungszweck (key usage).

1.5 Verwaltung der Richtlinie

Das vorliegende Dokument wurde erstellt, registriert und wird fortgeschrieben von DGN.

Postadresse:

DGN Deutsches Gesundheitsnetz Service GmbH

Niederkasseler Lohweg 185

40547 Düsseldorf

Email: trustcenter@dgnservice.de

Telefonisch ist die DGN zu erreichen unter 0211 77008-0.

Weitere Informationen über das Trustcenter und das angebotene Service-Portfolio sind unter http://www.dgn.de verfügbar. Unter derselben Adresse kann auch der „Fingerabdruck" der CA-Zertifikate abgerufen werden.

1.6 Definitionen und Abkürzungen

BNetzA	Bundesnetzagentur
CA	Certification Authority, Zertifizierungsstelle
CN	Common Name, Name
CP	Certificate Policy, Richtlinie für die Vergabe von Zertifikaten
CPS	Certificate Practice Statement, Regeln für den Betrieb (Umsetzung der CPs) einer Zertifizierungsstelle
CRL	Certificate Revocation List, Sperrliste für Zertifikate , enthält die revozierten Zertifikate
DN	Distinguished Name, systemweit eindeutiger Name, wird durch Verkettung aller Namensbestandteile von der Wurzel bis zum entsprechenden Eintrag erzeugt.
eIDAS	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PN	Pseudonym, Kennzeichnung im DN bei pseudonymen Namen
QSEE	Qualifizierte Signaturerstellungseinheit (Smartcard)
RA	Registration Authority, hier: Stelle zur Identifizierung und Überprüfung von Zertifikatsantragstellern und Zertifikatsanträgen
Revokation	Sperrung eines Zertifikats
SSEE	Sichere Signaturerstellungseinheit (Smartcard)

Trustcenter	von einem Vetrauensdiensteanbieter betriebene Infrastrukturen zur Erbringung der Vertauensdienste
Vertrauensdienst	hier: elektronischer Dienst zur Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln
Vetrauensdiensteanbieter	natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt
Zertifikat	Zuordnung eines kryptographischen Schlüssels zu einer Identität
Zeitstempel	Bestätigung über das Vorhandensein eines Dokumentes zu einem angegebenen Zeitpunkt

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienst

Ein zentraler Verzeichnisdienst für die ausgestellten Zertifikate der DGN steht unter LDAP://ldap.dgnservice.de zur Verfügung.

Darüber hinaus können anwendungs-, dienste- oder klassenspezifische Verzeichnisdienste angeboten werden.

2.2 Veröffentlichung von Informationen

Das Trustcenter publiziert folgende Informationen:

a.) über die Webseite http://www.dgnservice.de/trustcenter/public/dgnservice/index.html:
- dieses Certificate Practice Statement (CPS)
- ggf. Certificate Policy (CP)
- Teilnehmerunterrichtung

b.) über die Webseite unter http://www.dgn.de:
- Root- und CA-Zertifikate sowie deren „Fingerabdruck"
- Teilnehmerunterrichtung
- Allgemeine und ggf. besondere Geschäftsbedingungen

c.) über den LDAP-Verzeichnisdienst:
- ausgestellte Endteilnehmer-Zertifikate, sofern für den Zertifikatstyp vorgesehen und vom Zertifikatsinhaber zugestimmt
- Sperrlisten, sofern für eine Zertifikatsklasse Sperrlisten ausgestellt werden

d.) über den OCSP-Dienst unter der im jeweiligen Zertifikat angegebenen Adresse:
- Statusauskünfte für Zertifikate
- ausgestellte Endteilnehmer-Zertifikate, sofern für den Zertifikatstyp vorgesehen und vom Zertifikatsinhaber zugestimmt

e.) über die Deutsche Vertrauensliste (TSL), verwaltet von der Bundesnetzagentur (abrufbar unter https://tl.bundesnetzagentur.de/TL-DE.XML):
- die für den qualifizierten Betrieb gemäß der eIDAS-Verordnung erforderlichen Dienst-Zertifikate (CA-, OCSP-Signer und TSS-Signer-Zertifikate)

Informationen werden auch über andere Wege veröffentlicht. So kann beispielsweise der „Fingerabdruck" der CA-Zertifikate auch über die Hotline der DGN erfragt werden. Die aktuelle Rufnummer der Hotline wird dem Teilnehmer mit seinen Unterlagen mitgeteilt und ist auf obiger Website veröffentlicht.

2.3 Aktualisierung

Sofern aktualisierte Informationen vorliegen, z.B. im Falle einer Zertifikatssperrung, werden sie unverzüglich publiziert. Insofern CRLs mit begrenzter Gültigkeit Verwendung finden, werden rechtzeitig vor Ablauf neue CRLs erstellt.

2.4 Zugang zu den Diensten

Alle veröffentlichten Informationen werden zum Abruf bereitgestellt. Eine aktive Verteilung oder Benachrichtigung bei Aktualisierungen ist nicht vorgesehen.

Den Endteilnehmern und der Öffentlichkeit wird ohne Zugangskontrolle lesender Zugriff auf diese Informationen gewährt. Schreibenden Zugriff haben nur autorisierte Mitarbeiter der DGN. Die Systeme sind gegen unautorisierte Schreibzugriffe besonders geschützt.

3 Identifizierung und Authentifizierung

3.1 Namensgebung

3.1.1 Namenstypen

Es werden Namenshierarchien genutzt, die X.501-Distinguished-Names benutzen. Für Personen wird entweder der reale Name oder ein Pseudonym verwendet, das als solches gekennzeichnet wird (Zusatz „:PN“ am Common Name).
Es wird sichergestellt, dass nur Namen aus dem zugeordneten Namensraum vergeben werden.

3.1.2 Aussagekraft von Namen

Die Eindeutigkeit der Identifikation des Endteilnehmers durch seinen Namen (DN) im Zertifikat wird innerhalb der PKI der DGN Vertrauensdienste garantiert. Der verwendete Name (DN) wird auf den realen Namen des Teilnehmers beschränkt oder ist pseudonym.

3.1.3 Anonyme / Pseudonyme

Anonyme Zertifikate werden nicht erzeugt, pseudonyme werden unterstützt. Der Zertifizierungsdienst kann ein Pseudonym für ein Zertifikat festlegen oder die Verwendung eines vom Endteilnehmer gewünschten Pseudonyms ablehnen.

3.1.4 Interpretationsregeln für Namensformen

Der Zusatz „:PN“ bedeutet, dass es sich beim vorliegenden Namen um ein Pseudonym handelt.

3.1.5 Eindeutigkeit von Namen

Zur Gewährleistung der Eindeutigkeit innerhalb der PKI der DGN Vertrauensdienste wird eine Seriennummer in den DN aufgenommen. Der Endteilnehmer kann seine ihm zugewiesene Seriennummer nicht beeinflussen und darf sie nicht ablehnen.

3.1.6 Maßnahmen zur Auflösung von Streitigkeiten über einen Namen

Eine Überprüfung auf Verletzung von Markenrechten, Warenzeichen oder anderer Rechte findet durch den Zertifizierungsdienst nicht statt. Vielmehr ist der Antragsteller dafür verantwortlich, dass durch seinen Antrag keine Markenrechte, Warenzeichen oder andere Rechte Dritter verletzt werden. DGN übernimmt für solche Streitigkeiten keine Verantwortung oder Haftung. Pseudonyme oder Server-Namen, die geltendes Recht verletzen, sind nicht zulässig. Ein auf einen unzulässigen Namen ausgestelltes Zertifikat wird sofort nach bekannt werden der Rechtsverletzung gesperrt.

3.1.7 Anerkennung von Warenzeichen

Falls ein Pseudonym (erkennbar am Zusatz „:PN“ hinter dem Namen im Distinguished Name) an Stelle des Namens verwendet wird, darf dieses keine Warenzeichen, Markenrechte usw. verletzen. Der Zertifizierungsdienst überprüft solche Rechte nicht. Allein der Antragsteller ist für solche Überprüfungen

verantwortlich. Falls der Zertifizierungsdienst über eine Verletzung solcher Rechte informiert wird, wird nach den gesetzlichen Bestimmungen das Zertifikat gesperrt.

3.2 Erstregistrierung

3.2.1 Maßnahmen zur Überprüfung des Besitzes der sicheren Signaturerstellungseinheit, der zum zertifizierten öffentlichen Schlüssel gehört.

Fremderzeugte Schlüssel oder Schlüsselpaare anderer Trustcenter werden für qualifizierte Zertifikate nicht zertifiziert. Eine Überprüfung des Besitzes derartiger privater Schlüssel wird daher nicht durchgeführt.

Prüfungen des Besitzes fremderzeugter privater Schlüssel nicht qualifizierter Zertifikate werden in der jeweiligen CP festgelegt.

3.2.2 Authentisierung von Organisationen

Nur natürliche Personen dürfen qualifizierte Zertifikate beantragen und erhalten.

Die Authentisierung von Organisationen für nicht qualifizierte Zertifikate sowie von qualifizierten Siegeln werden in der jeweiligen CP geregelt.

3.2.3 Authentisierung von Personen

Personen, die ein qualifiziertes Zertifikat beantragen, werden bei der Antragstellung durch eine der folgenden Möglichkeiten authentisiert bzw. identifiziert:

- Durch persönliche Identifikation bei einem autorisierten Mitarbeiter. Der autorisierte Mitarbeiter, der auch einem von DGN beauftragten Dritten angehören darf, identifiziert den Antragsteller und prüft die Angaben durch Prüfung von zugelassenen gültigen Ausweispapieren mit Lichtbild.
- Durch geeignete technische Verfahren mit gleichwertiger Sicherheit zu einer persönlichen Identifizierung anhand von zugelassenen gültigen Ausweispapieren, z.B. mittels der eID-Funktion des Personalausweises.
- Durch Prüfung der Antragsdaten gegen bereits bei DGN registrierte Daten des Antragstellers, die auf Basis der zuvor genannten Verfahren erhoben wurden und Prüfung der Daten durch die RA des Trustcenters.
- Durch einen elektronisch signierten Antrag, falls der Antragsteller ein Zertifikat der erforderlichen Zertifikatsklasse besitzt, welches noch gültig ist.

Weitere oder ggfs. abweichende Authentisierungsverfahren werden in der CP der jeweiligen Zertifikatsklasse festgelegt.

3.2.4 Nicht überprüfte Attribute

Es werden keine nicht überprüften Attribute in qualifizierte Zertifikate übernommen.

3.2.5 Überprüfung fremder CAs, RAs

Eine Crosszertifizierung anderer CAs oder Einbeziehung fremder RAs ist derzeit nicht geplant. Sollte für bestimmte Zertifikatstypen oder –klassen eine Crosszertifizierung vorgesehen sein, wird dies in der jeweiligen CP geregelt.

3.2.6 Interoperabilität

Die Verwendbarkeit eines von DGN erzeugten Zertifikats außerhalb der von DGN betriebenen Public-Key-Infrastruktur wird nicht zugesichert.

3.3 Routinemäßige Erneuerung / Rezertifizierung

Eine routinemäßige Rezertifizierung findet nicht statt, nach Ablauf des Gültigkeitszeitraums des Zertifikats muss ein neues Zertifikat erzeugt werden.

Für eine Erneuerung nach Ablauf sowie nach Sperrung/Revokation muss in der Regel ein neuer Antrag gestellt werden. Mit dem Zertifikatsinhaber oder in der jeweiligen CP können hiervon abweichende Verfahren vereinbart werden.

3.4 Revokationsantrag

Die Revokation eines Zertifikates kann schriftlich per Brief oder qualifiziert signiertem Dokument, mündlich per Telefon oder persönlich beantragt werden. Zur Identifikation werden Ausweisdaten, Unterschriften, qualifizierte Signaturen sowie bei Antragstellung vergebene Revokationspasswörter herangezogen.

Falls eine Person mehrere Signaturzertifikate (Signaturkarten) besitzt und nur eines davon revoziert werden soll, werden spezifische Merkmale der zu sperrenden Signaturkarte/-zertifikate abgefragt. Wenn die zu sperrende Signaturkarte oder das zu sperrende Zertifikat nicht sicher identifiziert werden kann, werden nach entsprechendem Hinweis an den Antragsteller und dessen Zustimmung alle Signaturkarten bzw. Zertifikate des Antragstellers revoziert.

4 Betriebliche Abläufe

4.1 Antrag auf Ausstellung von Zertifikaten

Ein Antrag auf Ausstellung von qualifizierten Zertifikaten kann nur persönlich und von einer natürlichen Person gestellt werden. Die Identifikation des Antragstellers erfolgt nach den Regelungen des Kapitels 3.2.3 bzw. der jeweiligen CP.

4.2 Bearbeitung von Zertifikatsanträgen

Die Antragsprüfung erfolgt durch die RA der DGN. Anträge auf qualifizierte Zertifikate werden im Trustcenter von zwei Registraren bearbeitet, die die elektronisch vorliegenden Antragsdaten im RA-System überprüfen.

Der Antrag wird bearbeitet, sofern alle Antragsdaten und Dokumente vollständig vorliegen und keine anderen Gründe entgegenstehen.

4.3 Zertifikatsausstellung

Stehen keine Gründe gegen eine Produktion, werden die beantragten Zertifikate produziert und bei qualifizierten Zertifikaten auf eine qualifizierte elektronische Signaturerstellungseinheit (QSEE) aufgebracht.

4.4 Entgegennahme von Zertifikaten / Signaturkarte

Personalisierte Smartcards oder Zertifikate und private Schlüssel werden über ein mit dem Antragsteller vereinbarten Verfahren zugestellt oder persönlich übergeben.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Die Verwendung der Schlüssel und Zertifikate ist auf den jeweiligen Anwendungskontext, der sich in Übereinstimmung mit dem jeweils im Zertifikat enthaltenen Verwendungszweck befinden muss, beschränkt.

4.6 Zertifikatserneuerung / Wiederzertifizierung

Eine Zertifikatserneuerung / Wiederzertifizierung bestehender Schlüsselpaare wird nicht unterstützt.

4.7 Zertifikatserneuerung / Re-Key

Eine Zertifikatserneuerung / Re-Key wird nicht direkt unterstützt, es können neue Zertifikate/Karten beantragt werden.

4.8 Zertifikatsmodifizierung

Eine Änderung von Inhalten der Zertifikate (z.B. nach Namensänderung) ist nur über einen Neuantrag möglich. Haben sich die Identifikationsdaten eines Zertifikatsinhabers geändert (Name, Vorname, Staatsangehörigkeit, Geburtsort, Geburtstag), muss eine erneute Identifikationsprüfung durchgeführt werden.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Revokationsgründe

Ein Zertifikat kann aus folgenden Gründen revoziert (gesperrt) werden:

- bei Kompromittierung des privaten Schlüssels des Endteilnehmers oder der CA,
- bei Verlust oder Diebstahl des privaten Schlüssels des Endteilnehmers,
- bei Beendigung des Vertrags zwischen dem Endteilnehmer und dem Zertifizierungsdienst,
- bei Ausstellung des Zertifikats auf Grundlage falscher Daten,
- bei Änderung der Daten des Endteilnehmers, die Grundlage der Zertifikatserstellung waren (z.B. Namensänderung),
- bei Wegfall der Berechtigung zum Führen eines Attributes, z.B. der Berufsgruppen- oder Unternehmenszugehörigkeit,
- auf Wunsch des Endteilnehmers oder
- bei Sicherheitsmängeln in der eingesetzten Hard- und Software sowie in den verwendeten Kryptoalgorithmen.

4.9.2 Berechtigte Personen, die eine Revokation veranlassen können

Zur Sperrung eines Zertifikats sind der Zertifikatseigentümer oder von ihm benannte Vertreter, attributvergebende Stellen sowie die Bundesnetzagentur (für qualifizierte Zertifikate) und dafür benannte Mitarbeiter der DGN berechtigt.

4.9.3 Prozedur für einen Antrag auf Revokation

Der Antrag auf Revokation kann sowohl schriftlich (Papier/Brief oder elektronisch) als auch mündlich (auch telefonisch) erfolgen.

Zur Bearbeitung sind folgende Informationen nötig:

Schriftlich oder elektronisch: Vorname und Name des Zertifikatsinhabers, der Name des Sperrantragstellers und Informationen zur Identifikation der zu sperrenden Zertifikate bzw. Signaturkarte. Dabei werden zur Prüfung der Berechtigung zur Sperrung die Signatur und/oder das angegebene Revokationspasswort sowie weitere Authentisierungsdaten geprüft.

Telefonisch: Vorname und Name des Zertifikatsinhabers, der Name des Sperrantragstellers, Informationen zur Identifikation der zu sperrenden Zertifikate bzw. der Signaturkarte sowie das Revokations- bzw. Autorisierungspasswort. Die Daten werden erfragt, wobei ggf. noch weitere Einzelheiten über die zu revozierende Signaturkarte mitgeteilt werden müssen.

Nach erfolgreicher Prüfung des Sperrantrags wird ein interner Antrag auf Revokation in das Sperr-System eingegeben und verarbeitet.

Es werden stets alle Zertifikate einer Signaturkarte (QSEE) revoziert.

4.9.4 Revokationsfrist für den Zertifikatsinhaber

Falls der begründete Verdacht einer Kompromittierung des privaten Schlüssels eines Endteilnehmers besteht, ist der Endteilnehmer verpflichtet, seine Zertifikate unverzüglich sperren zu lassen.

Auch eine Revokation aus anderem Grund durch den Zertifikatsinhaber muss umgehend erfolgen, sobald der dafür zutreffende Grund vorliegt.

4.9.5 Revokationsbearbeitungsfrist für das Trustcenter

Eine Revokation auf Basis eines telefonischen Sperrantrags wird unverzüglich durchgeführt. Schriftliche Sperranträge werden an Arbeitstagen in NRW (außer an Rosenmontag) bearbeitet.

4.9.6 Mechanismen für Relying Parties

Sperrinformationen können jederzeit über den OCSP- und Verzeichnisdienst abgerufen werden. Die Authentizität der Informationen kann durch Prüfung der Signatur der OCSP-Antwort bzw. der Sperrliste (sofern für diese Zertifikatsklasse Sperrlisten ausgestellt werden) verifiziert werden.

4.9.7 Aktualisierungsfrequenz einer CRL (Liste revozierter Zertifikate)

Sobald ein Zertifikat revoziert wird, wird eine neue CRL erzeugt und veröffentlicht, sofern für Zertifikate dieser Klasse Sperrlisten ausgestellt werden.

4.9.8 Maximale Wartedauer auf neue CRL (Liste revozierter Zertifikate).

Aktualisierungszeiten werden entsprechend der jeweiligen CP umgesetzt.

4.9.9 Online Statusprüfung

Für den OCSP- und Verzeichnisdienst und die CRL sind Zugangsmöglichkeiten via ldap und http verfügbar.

4.9.10 Anforderungen an Endteilnehmer zur Nutzung der Online Statusprüfung

Der Endteilnehmer kann gemäß der jeweiligen CP verpflichtet werden, vor der Nutzung eines Zertifikats (insbesondere, wenn eine Signatur überprüft wird), eine Online-Statusüberprüfung durchzuführen. Dies kann entweder durch Herunterladen und Prüfen der aktuellen CRL (soweit vorhanden) oder durch Nutzung des Online-Statusdienstes OCSP erfolgen.

4.9.11 Andere Formen der Bekanntgabe von Revokationen

Die Überprüfung der Revokation eines Zertifikates kann über eine Revokationsliste (sofern für diese Zertifikatsklasse Sperrlisten ausgestellt werden) oder OCSP Anfrage durchgeführt werden.

4.9.12 Spezielle Anforderungen bei Re-Keying Kompromittierung

Re-Keying wird nicht unterstützt.

4.9.13 Gründe für Suspendierung

Die Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.14 Berechtigte für die Suspendierung

Die Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.15 Verfahren bei der Suspendierung

Die Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.16 Zeitrestriktionen für die Suspendierung

Die Suspendierung von Zertifikaten wird nicht unterstützt.

4.10 Dienste zur Online-Überprüfung eines Zertifikates (Statusabfrage)

Zur Überprüfung des Status eines Zertifikates werden Revokationslisten (CRL) und/oder OCSP-Dienste bereitgestellt.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Die Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer ist in den Allgemeinen Geschäftsbedingungen der DGN geregelt, abweichende Regelungen können im Vertrag definiert werden.

4.12 Schlüsselhinterlegung und –wiederherstellung

Eine Hinterlegung oder Sicherungsarchivierung privater Schlüssel der qualifizierten Zertifikate findet nicht statt.

Ggfs. abweichende Regelungen müssen in einer jeweiligen CP festgelegt werden.

5 Infrastruktur und betriebliche Abläufe

Nicht alle Informationen dieses Themenbereichs sind öffentlich.

5.1 Physische Sicherheitsmaßnahmen

Die physischen Sicherheitsmaßnahmen entsprechen den Anforderungen, die im Rahmen der Konformitätsbestätigung nach eIDAS an den Zertifizierungsdienst gestellt und umgesetzt wurden. Die Maßnahmen sind in einem separaten Sicherheitskonzept beschrieben, dessen Umsetzung durch eine unabhängige Prüfinstanz bestätigt wurde und regelmäßig geprüft wird.

5.1.1 Lage und Konstruktion der Betriebsstätten des Trustcenters

Das Trustcenter wird in den Rechenzentren der Deutschen Apotheker- und Ärztebank bzw. in den Räumen der DGN betrieben. Die Sicherheit der Räume ist in einem eigenen Sicherheitskonzept beschrieben und wurde und wird im Rahmen der Konformitätsbestätigung nach eIDAS in regelmäßigen Abständen durch eine Prüf- und Bestätigungsstelle überprüft. Sie bieten einen Schutz, der dem erforderlichen Sicherheitsniveau entspricht.

5.1.2 Zutrittskontrollen

CA:

Die Betriebsräume sind durch elektronische und mechanische Schlösser und durch eine Alarmanlage geschützt. Nur vom Sicherheitsbeauftragten autorisierten Personen wird Zutritt zu den Räumen des Trustcenters gewährt.

RA:

Die Betriebsräume befinden sich innerhalb des Bürogebäudes der DGN. Sie sind in speziellen Räumen untergebracht, die zutritts- und alarmgeschützt sind. Zu diesen Räumen wird nur vom Sicherheitsbeauftragten autorisierten Personen Zutritt gewährt.

Der Zutritt durch nicht mit entsprechenden Rollen des Trustcenters betraute Personen regelt eine gesonderte Besucherregelung.

5.1.3 Stromversorgung und Klimatisierung

Das Trustcenter verfügt über unabhängige redundante Stromkreise, die durch entsprechende Systeme gegen Unterbrechung gesichert sind.

Die Klimatisierung der Technikbereiche ist redundant ausgelegt. Die Leistungsfähigkeit gewährleistet eine ausreichende Entwärmung der Technikbereiche.

5.1.4 Abwehr von Wasserschäden

Ein angemessener Schutz vor Wasserschäden ist gewährleistet.

5.1.5 Abwehr von Feuerschäden

Eine Feuermeldeanlagen und Feuerlöscher sind nach den gültigen Brandschutzbestimmungen überall vorhanden. Einzelne Systeme sind mit Brandmelde- und Löschanlagen gesichert.

5.1.6 Aufbewahrung von Medien

Alle Backup-Medien sowie Papier-Archive werden in verschlossenen Schränken getrennt von den IT-Systemen in separaten Brandabschnitten gesichert aufbewahrt.

5.1.7 Abfallentsorgung

Datenträger mit sensiblen Daten werden ausschließlich durch einen zertifizierten Dienstleister entsorgt.

5.1.8 Externes Backup

Backups werden intern in separaten Brandabschnitten gesichert, externe Backups werden nicht vorgenommen.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollen

Als Bestandteil des Sicherheitskonzeptes des Vertrauensdiensteanbieters existiert ein umfangreiches Rollen- und Rechtekonzept, welches die Rollen, deren Aufgaben und Rechte beschreibt.

5.2.2 Involvierte Personen pro Arbeitsschritt

Die Festlegung der in die jeweiligen Arbeitsschritte involvierten Personen erfolgt über die Zuweisung zu den Rollen. Dabei wird die Unverträglichkeit von Rollen entsprechend des Sicherheitskonzeptes berücksichtigt.

5.2.3 Identifikation und Authentifizierung der Rollen

Die Identifikation und Authentifizierung von Rollen erfolgt auf Grundlage des als Bestandteil des Sicherheitskonzeptes umgesetzten Rollen- und Rechtemodells.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Sicherheitsüberprüfung der Personen, die sicherheitskritische Rollen im Trustcenter einnehmen

Ein polizeiliches Führungszeugnis wird von allen Personen, die dem Betrieb der Vertrauensdienste angegliedert sind, vorgelegt.

5.3.2 Sicherheitsüberprüfung für weiteres Hilfspersonal

Personen, die nicht am Betrieb der Vertrauensdienste teilnehmen aber für die die Notwendigkeit zum Betreten der Trustcenter-Bereiche gegeben ist, werden durch autorisiertes Personal begleitet,

5.3.3 Anforderungen an Kenntnisse und Weiterbildung

Für den Betrieb der Vertrauensdienste wird nur qualifiziertes Personal eingesetzt. Jeder Mitarbeiter des Trustcenters wird speziell geschult.

5.3.4 Frequenz und Anforderungen an eine regelmäßige Weiterbildung

Es werden regelmäßig Weiterbildungsveranstaltungen besucht sowie relevante Publikationen und Literatur speziell zum Thema Sicherheit angeboten.

5.3.5 Job Rotation

Eine Job Rotation findet nicht statt. Es existieren Vertretungsregeln für den kurzfristigen Ersatz bei Personalausfall.

5.3.6 Sanktionen für die unautorisierte Benutzung von Systemen

Bei unautorisierten Aktionen, die die Sicherheit des Systems gefährden, können arbeitsrechtliche Maßnahmen ergriffen werden. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

5.3.7 Anforderungen an die Arbeitsverträge freier Mitarbeiter

Spezielle Prüfungen für Verträge mit freien Mitarbeitern und Beratern sichern deren fachliche Kompetenz. Für alle Arbeitsverträge gilt das Recht der Bundesrepublik Deutschland.

5.3.8 Dokumentation, die dem Personal zur Verfügung steht

Folgende Dokumentation wird dem Personal zur Verfügung gestellt:
Sicherheitskonzept, CPS, CP, Rollendefinition und -vergabe, Organisationsstruktur des Vetrauensdiensteanbieters, Unverträglichkeiten von Rollen (Rollenmatrix), Prozessbeschreibungen und Verfahrensanweisungen für den regulären Betrieb, Backup-Prozesse, Abkürzungsverzeichnis und Glossar, Formulare für den regulären Betrieb, Notfallprozeduren, Notfallhandbuch inklusive Eskalationsverfahren.

5.4 Audit und Logging Prozeduren

Es wird umfangreiches Logging eingesetzt. Alle Arten von Events bei Alarmanlage, Zutrittskontrolle und die relevanten Schritte im Produktionsprozess werden protokolliert. Zusätzlich werden betriebliche Maßnahmen wie Datensicherungen protokolliert.
Die Protokolle werden auf Unregelmäßigkeiten geprüft.

5.5 Datensicherung

Von den Systemen werden regelmäßige Datensicherungen gemäß Datensicherungskonzept durchgeführt und ebenso wie papiergebundene Daten den gesetzlichen Vorgaben entsprechend sicher archiviert.

5.6 CA-Schlüsselwechsel

Wird der CA-Schlüssel gewechselt, werden neue CA-Schlüssel generiert und neue CA-Zertifikate in der eigenen Root-PKI erzeugt. Neue CA-Zertifikate werden rechtzeitig veröffentlicht. (Siehe Kapitel 2.2)

5.7 Notfall und Recovery

Die Behandlung von Notfällen ist in einem Notfall-Konzept und einem entsprechenden Notfall-Handbuch beschrieben. Das Notfall-Handbuch enthält alle im Notfall relevanten Informationen. Es sind Prozeduren beschrieben, wie im Notfall vorzugehen ist, Kontaktdaten hinterlegt und Arbeitsschritte beschrieben, wie die Betriebsfähigkeit wiederherzustellen ist.

5.8 Einstellung des Betriebes

Soll der Betrieb des Vertrauensdiensteanbieters eingestellt werden, muss ein nachfolgender Dienstleister gefunden werden, der die Bereitstellung der Statusinformationen zu den ausgestellten Zertifikaten übernimmt oder die Bundesnetzagentur übernimmt alle Zertifikate einschließlich der Widerrufsinformationen in die Vertrauensinfrastruktur nach Absatz 5 der eIDAS-Verordnung. Wird kein Nachfolger in diesem Sinne gefunden, werden die Zertifikate gesperrt.

6 Technische Sicherheitsmaßnahmen

Nachfolgend werden Einzelheiten zu technischen Sicherheitsmaßnahmen aufgeführt. Nicht alle Informationen dieses Themenbereichs sind jedoch öffentlich.

6.1 Schlüsselpaarerzeugung und Installation

6.1.1 Schlüsselpaarerzeugung

Für den Einsatz mit qualifizierten Zertifikaten handelt es sich dabei um geprüfte und bestätigte qualifizierte elektronische Signaturerstellungseinheiten oder um geprüfte und bestätigte Schlüsselgeneratoren.

6.1.2 Auslieferung des privaten Schlüssels

Private Schlüssel für qualifizierte Zertifikate werden über ein mit dem Antragsteller vereinbartem Verfahren oder persönlich ausgeliefert.
Weitere Auslieferungsformen können in der jeweiligen CP festgelegt werden.

6.1.3 Auslieferung des öffentlichen Schlüssels an den Zertifikatsinhaber

Der öffentliche Schlüssel des Endteilnehmers wird bei qualifizierten Zertifikaten zusammen mit dem privaten Schlüssel und dem Zertifikat auf einer QSEE ausgeliefert. Zusätzlich wird der öffentliche Schlüssel bei Zustimmung des Endteilnehmers als Bestandteil des Teilnehmerzertifikats im Zertifikatsverzeichnis oder über den OCSP-Dienst veröffentlicht.
Abweichende oder ergänzende Auslieferungsformen können in der jeweiligen CP festgelegt werden.

6.1.4 Auslieferung der öffentlichen Root- und CA-Schlüssel

Die öffentlichen Schlüssel der CAs der DGN werden über die in Kapitel 2.2 angegebene Publikationsadresse im Internet zum Abruf bereitgestellt. Der Endteilnehmer muss dabei den publizierten Fingerprint mit dem Fingerprint des öffentlichen Schlüssels vergleichen.
Die Veröffentlichung öffentlicher Schlüssel, die für den qualifizierten Betrieb erforderlich sind, erfolgt zusätzlich über die Deutsche Vertrauensliste (Siehe Kapitel 2.2).

6.1.5 Verwendete Schlüssellängen

Für qualifizierte Zertifikate werden die jeweils von der Bundesnetzagentur, BSI oder entsprechenden Stellen gemäß eIDAS empfohlenen Schlüssellängen verwendet. Diese sind für die CA-Schlüssel und für die Schlüssel der Endteilnehmer aktuell 2048 Bit bei RSA- und 256 Bit bei ECC-Verfahren. Eine Vergrößerung der Schlüssellänge kann in der Zukunft erfolgen, ohne dass diese im CPS vermerkt wird.

6.1.6 Parameter der öffentlichen Schlüssel

Die Parameter der öffentlichen Schlüssel werden bei qualifizierten Zertifikaten gemäß den gesetzlichen Regelungen bzw. gemäß der jeweiligen CP von der CA des Trustcenters erzeugt.

6.1.7 Verwendungszweck der Schlüssel

Beschränkungen aller Teilnehmerzertifikate: CA: false (critical)

Die Schlüssel der Endteilnehmer der qualifizierten Zertifikate haben in der Regel folgenden Verwendungszweck, wie im entsprechenden Feld des X.509v3 Zertifikates aufgeführt:

Signaturschlüssel: Non Repudiation

Der eingetragene Verwendungszweck weiterer auf den entsprechenden Signaturkarten enthaltener Zertifikate entspricht dem jeweiligen Einsatzgebiet:

Verschlüsselungsschlüssel: Data Encipherment, Key Encipherment (critical)

Authentisierungsschlüssel: Digital Signature (critical), Key Encipherment (critical)

Die Parameter werden bei deren Festlegung sorgfältig ausgewählt und überprüft.

6.2 Schutz des privaten Schlüssels

6.2.1 Standards des Schlüssel erzeugenden kryptographischen Moduls

Für den Einsatz mit qualifizierten Zertifikaten werden geprüfte und bestätigte qualifizierte elektronische Signaturerstellungseinheiten bzw. geprüfte und bestätigte Schlüsselgeneratoren eingesetzt.

6.2.2 Schlüsselteilung (key-sharing Algorithmus)

Die Schlüssel der Endteilnehmer werden nicht geteilt.

6.2.3 Schlüsselhinterlegung

Eine Hinterlegung der Teilnehmerschlüssel findet nicht statt.

6.2.4 Backup von privaten Schlüsseln

Ein Backup von privaten Schlüsseln wird für Dienstzertifikate durch Transfer zwischen geeigneten Kryptomodulen durchgeführt (siehe Kapitel 6.2.6). Ein Backup von privaten Schlüsseln der Endteilnehmer erfolgt nicht.

6.2.5 Archivierung privater Schlüssel

Es existiert keine Archivierung von Schlüsseln qualifizierter Zertifikate.

6.2.6 Transfer privater Schlüssel in ein Kryptomodul

Es erfolgt keine Speicherung privater Schlüssel der Endteilnehmer in ein Kryptomodul. Soweit private Schlüssel der Dienstzertifikate (Root, CA, OCSP-Signer, Zeitstempel-Signer) in einem geeigneten Kryptomodul gespeichert werden, erfolgt lediglich der Transfer zwischen Kryptomodulen zum Zwecke der Redundanz und zur Erfüllung von Lastanforderungen. Der Transfer erfolgt stets unter Einhaltung der organisatorischen und kryptografischen Sicherheitsvorgaben, die gemäß der Zertifizierung des Kryptomoduls vorgeschrieben sind.

Näheres kann durch eine CP geregelt werden.

6.2.7 Speicherung privater Schlüssel in ein Kryptomodul

Qualifizierte Zertifikate: Die privaten Schlüssel eines Endteilnehmers werden entsprechend den geltenden gesetzlichen Vorgaben (z.B. eIDAS-Verordnung) erzeugt und gespeichert.
Sonstige Zertifikate: Die Anforderungen der jeweiligen CP werden eingehalten.

6.2.8 Aktivierung privater Schlüssel

Ein privater Schlüssel einer QSEE (Signaturkarte) wird nur nach Eingabe einer PIN aktiviert. Die Aktivierung privater Schlüssel eines Kryptomoduls erfolgt gemäß den Vorgaben aus dessen Zertifizierung.

6.2.9 Deaktivierung privater Schlüssel

Für qualifizierte Zertifikate gilt, dass die privaten Schlüssel der Signaturkarte nach dreimaliger Eingabe einer falschen PIN blockiert werden, wenn nicht vor der dritten Fehleingabe die PIN korrekt eingegeben wurde. Mit einer PUK können die Schlüssel bis zu 10-mal freigeschaltet werden.
Abweichende Verfahren und Regelungen für sonstige, nicht qualifizierte Zertifikate können in einer CP geregelt sein.

6.2.10 Vernichtung privater Schlüssel

Die privaten Schlüssel auf einer Signaturkarte können vernichtet werden, indem der Chip auf der Karte physisch vernichtet (z.B. durchschnitten) wird. Die Vernichtung privater Schlüssel eines Kryptomoduls erfolgt durch administrativen Vorgang. Dabei ist der Schlüssel stets aus allen Kryptomodulen zu löschen, wenn dieser auf andere Module transferiert wurde (siehe 6.2.6).

6.2.11 Kryptomodul Rating

Keine Angaben.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden sowohl im Verzeichnisdienst als auch auf Backup-Medien archiviert.

6.3.2 Gültigkeit der Schlüsselpaare

Die Gültigkeit der Schlüsselpaare entspricht der Gültigkeitsdauer des Zertifikats, das auf Basis des öffentlichen Schlüssels erstellt wird. Die Standardgültigkeit von smartcard-basierten Zertifikaten beträgt 5 Jahre. In einer produktspezifischen CP können abweichende Regelungen zur Laufzeit geregelt sein.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs)

Die Aktivierungsdaten der CA-Schlüssel werden durch die Sicherungsmechanismen des jeweiligen Kryptomoduls festgelegt.
Für die PINs der Endteilnehmer-Schlüssel qualifizierter Zertifikate sowie weiterer auf den entsprechenden Signaturkarten enthaltener Zertifikate werden Zufallszahlen als sogenannte Transport-PINs erzeugt und in

der jeweiligen QSEE im Rahmen der Personalisierung im DGN Trustcenter gespeichert. Vor Anwendung eines Schlüssels müssen die PINs vom Endanwender geändert werden.

6.4.2 Schutz der Aktivierungsdaten

Die PINs der CA-Schlüssel werden verschlüsselt im hoch sicheren Kernsystem oder entsprechend gesicherten und geeigneten HSMs abgelegt.
Für die PINs der Endteilnehmer-Schlüssel qualifizierter Zertifikate sowie weiterer auf den entsprechenden Signaturkarten enthaltener Zertifikate werden vom Endteilnehmer selbst vergeben und in der QSEE gespeichert.

6.4.3 Weitere Aspekte

Die PINs der CA-Schlüssel werden unter Wahrung des 4-Augen-Prinzips verwendet. Dazu werden geeignete technische und organisatorische Verfahren eingesetzt.

6.5 Sicherheitsmaßnahmen für Computersysteme

6.5.1 Spezifische Sicherheitsmaßnahmen für die Computersysteme

Der Betrieb der Vertrauensdienste basiert auf einem durch eine unabhängige Prüfinstanz bestätigten Sicherheitskonzept.

6.5.2 Sicherheitseinstufung

Die Sicherheit der Computersysteme wird durch eine unabhängige Prüf- und Bestätigungsstelle bzw. Konformitätsbewertungsstelle regelmäßig überprüft.

6.6 Life-Cycle der Sicherheitsmaßnahmen

6.6.1 Sicherheitsmaßnahmen für die Entwicklung

Bei der Entwicklung der sicherheitsrelevanten Software für den Betrieb des Zertifizierungsdienstes werden geeignete Sicherheitsmaßnahmen ergriffen oder entsprechend geprüfte und geeignete Dienstleister gewählt. Neue Software-Versionen werden in einer baugleichen Testumgebung getestet und abgenommen, bevor sie im Produktivbetrieb eingesetzt werden.

6.6.2 Sicherheitsmanagement

Das Sicherheitsmanagement ist im Sicherheitskonzept beschrieben und umfasst u.a. ein Rollen- und Rechtekonzept, notwendige interne und externe Prüfungen und Revisionen sowie geeignete organisatorische und technische Überwachungsmaßnahmen. Der Sicherheitsbeauftragte überwacht die Einhaltung der Sicherheitsziele und Sicherheitsmaßnahmen des Vertrauensdiensteanbieters.

6.6.3 Sicherheitseinstufung

Eine Sicherheitseinstufung wird nicht durchgeführt.

6.7 Sicherheitsmaßnahmen für Netzwerke

Die Systeme der Produktionsumgebung sind in einem dedizierten LAN untereinander verbunden. Verbindungen zwischen den gesicherten Trustcenter-Bereichen sind kryptographisch gesichert. Für alle Netzsegmente sind Firewalls installiert, die den Netzwerkverkehr kontrollieren und nur für bestimmte Adressen, Ports und Dienste erlauben und die Anbindung weiterer Systeme unterbinden.

6.8 Zeitstempel

Die Bereitstellung von Zeitstempeldiensten erfolgt gemäß den Vorgaben der eIDAS-Verordnung. Für eine hinreichend genaue Systemzeit werden redundante Funkuhren (Stratum 0) betrieben, mit der die Systeme des Zeitstempeldienstes synchronisiert werden.

Die Nutzung des Zeitstempeldienstes ist nur über authentisierten Zugriff möglich. Authentisierungsdaten werden dem Nutzer nach Abschluss einer Nutzungsvereinbarung zur Verfügung gestellt.

Es werden nur Zeitstempel über einen vom Nutzer gelieferten Hashwert ausgestellt. Dabei werden nur Hashwerte akzeptiert, die auf geeigneten Algorithmen basieren und über die in der Nutzungsvereinbarung informiert wird. Die Erzeugung des Zeitstempel-Requests inklusive der Hashwert-Berechnung des zu signierenden bzw. mit einem Zeitstempel zu versehenden Dokuments, die Prüfung des ausgestellten Zeitstempels sowie dessen Zugehörigkeit zum Dokument liegen im Verantwortungsbereich des Nutzers.

In der eIDAS-Verordnung ist ferner auch die Rechtswirkung von elektronischen Zeitstempeln geregelt, wonach einem elektronischen Zeitstempel die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt. Jedoch gilt auch hier für qualifizierte elektronische Zeitstempel die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

7.1 Profile für Zertifikate

Die Profile der ausgestellten Zertifikate werden gemäß der jeweiligen externen Spezifikationsvorgaben oder einer dedizierten CP erstellt.

7.2 Profil der Revokationslisten

Die Profile der ausgestellten Revokationslisten werden, soweit für die jeweilige Zertifikatsklasse vorgesehen, gemäß der jeweiligen externen Spezifikationsvorgaben oder einer dedizierten CP erstellt.

7.3 OCSP Profil

7.3.1 OCSP Version

OCSP-Responder nehmen Anfragen gemäß RFC6960 entgegen, Antworten sind ebenfalls konform zu RFC6960. Mehrfachanfragen werden nicht unterstützt.

7.3.2 OCSP Extensions

Keine Angabe

8 Konformitätsprüfung

Die Zertifizierungsstelle der DGN verpflichtet sich, nach den hier und ggf. in CP´s beschriebenen Abläufen zu verfahren. Eine Überprüfung der Einhaltung dieser Verpflichtung findet im Rahmen regelmäßiger Audits statt.

8.1 Frequenz und Umstände der Überprüfung

Der Vertrauensdiensteanbieter unterliegt einer ständigen Kontrolle einer internen Revision und für den Betrieb qualifizierter Vertrauensdienste zusätzlich regelmäßigen Audits einer unabhängigen Konformitätsbewertungsstelle.

8.2 Identität des Überprüfers

Die Audits werden im Rahmen einer internen Revision durch den Revisor des Vertrauensdiensteanbieters durchgeführt.
Als externe unabhängige Konformitätsbewertungsstelle ist zurzeit die Firma T-Systems tätig.

8.3 Verhältnis von Prüfer zu Überprüftem

Der interne Auditor ist als Revisor des Vertrauensdiensteanbieters beauftragt. Er nimmt keine weiteren Aufgaben im operativen Betrieb des Trustcenters wahr und ist in seiner Revisionstätigkeit weisungsunabhängig.

8.4 Überprüfte Bereiche

Es werden alle Instanzen, Rollen, Prozesse, Personen, Protokolle und Log-Dateien des Trustcenters stichprobenartig überprüft.

8.5 Fehlerkorrektur

Werden Mängel festgestellt, werden geeignete Maßnahmen zu deren Beseitigung eingeleitet. Falls die Sicherheit des Betriebs der Vertrauensdienste gefährdet ist, wird gegebenenfalls der Betrieb bis zur Beseitigung der Mängel eingestellt.

8.6 Veröffentlichung der Ergebnisse

Die Ergebnisse des Audits bzw. der Mängelbeseitigung werden nicht veröffentlicht.

9 Sonstige Regelungen

9.1 Gebühren

Die Gebühren für Leistungen der Vertrauensdienste sind in den Unterlagen zum jeweiligen Produkt (unter http://www.dgn.de) bzw. in den Verträgen festgelegt.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Der Vertrauensdiensteanbieter verfügt über eine Deckungsvorsorge gemäß eIDAS Art. 24 Abs. 2c) bzw. VDG §10.

9.2.2 Vermögenswerte

Keine Angaben

9.2.3 Versicherungsschutz für Kunden (Zertifikatsinhaber)

Keine Angaben

9.3 Vertraulichkeit von Geschäftsinformationen

Die Klassifikation von Informationen und Dokumenten sowie deren Weitergabe erfolgt gemäß der Sicherheitseinstufung der DGN.

9.4 Schutz personenbezogener Daten (Datenschutz)

Im Rahmen des Betriebs der Vertrauensdienste werden persönliche Daten erhoben. Diese werden gemäß den geltenden gesetzlichen Vorgaben (u.a. Datenschutzgrundverordnung Art. 5, eIDAS, …) behandelt.

9.4.1 Vertraulich zu behandelnde Informationen

Alle persönlichen Daten (Ausnahme: Zertifikatssperrung, Zeitpunkt der Sperrung) gelten als vertrauliche Informationen, sofern der Eigentümer deren Veröffentlichung der Information nicht explizit zugestimmt hat. Hat der Zertifikatsinhaber der Veröffentlichung seines Zertifikates zugestimmt, gelten die im Zertifikat enthaltenen persönlichen Daten als nicht vertraulich.

9.4.2 Nicht vertraulich zu behandelnde Informationen

Alle Daten, deren Veröffentlichung der Eigentümer der Information explizit zugestimmt hat, gelten als nicht vertraulich.

Insbesondere sind Daten, die im durch den Inhaber zur Veröffentlichung freigegebenen Zertifikat oder in veröffentlichten Verzeichnissen für die Überprüfung eines Zertifikats (CRLs, OSCP) enthalten sind oder die aus diesen Daten ableitbar sind, öffentlich und damit nicht vertraulich.

9.4.3 Verantwortung für vertraulich zu behandelnde Informationen

Die DGN wird vertrauliche Daten mit derselben Sorgfalt sichern, mit der auch eigene vertrauliche Daten gesichert werden. Eine Weitergabe vertraulicher Daten an Dritte ist nicht geplant. Sofern sie dennoch

erfolgen muss, werden dazu vorher entsprechend geeignete Vertraulichkeitsvereinbarungen mit dem Empfänger abgeschlossen. Ausgenommen von dieser Regelung sind lediglich Auskünfte gemäß den gesetzlichen Verpflichtungen (z.B. §8 (2) VDG).

9.5 Urheberrechte

CA-Zertifikate der DGN sowie die zugehörigen privaten und öffentlichen Schlüssel sind Eigentum der DGN. Ihre Nutzung für Zwecke, die in dieser CPS oder ggf. der jeweiligen CP vorgesehen sind, ist jedem Teilnehmer der PKI erlaubt.

Die Zertifikate sowie die privaten und öffentlichen Schlüssel der Endteilnehmer sind Eigentum der jeweiligen Endteilnehmer.

Der Nutzung der Zertifikate für Zwecke, die in dieser CPS oder ggf. der jeweiligen CP vorgesehen sind, hat der Endteilnehmer durch den Zertifizierungsantrag zugestimmt.

9.6 Verpflichtungen

In diesem Abschnitt werden die Verpflichtungen sowohl des Vertrauensdiensteanbieters als auch der Endteilnehmer aufgeführt. Ziel ist die durchgehende Einhaltung eines hohen Sicherheitsniveaus.

9.6.1 Verpflichtungen des Vertrauensdiensteanbeiters, CA

Die CA als Instanz des Vertrauensdiensteanbieters verpflichtet sich, nach den Richtlinien dieses CPS sowie der jeweiligen CP (sofern vorhanden) zu arbeiten. Insbesondere wird dem Schutz des privaten Schlüssels der CA absolute Priorität eingeräumt. Die CA stellt Zertifikate für Endteilnehmer gemäß dieses CPS sowie ggf. der jeweiligen CP aus. Dafür vertraut sie der RA und lehnt unautorisierte Anträge ab. Die CA verpflichtet sich, Revokationsanträge gemäß dieses CPS sowie ggf. der jeweiligen CP zu bearbeiten und soweit vorgesehen eine entsprechende CRL auszustellen. Die CA verpflichtet sich, qualifiziertes Personal zu beschäftigen, dessen Zuverlässigkeit geprüft wurde. Die Sicherheitsvorkehrungen werden eingehalten.

9.6.2 Verpflichtungen des Vertrauensdiensteanbeiters, RA

Die RA des Vertrauensdiensteanbieters verpflichtet sich, nach den Richtlinien des vorliegenden CPS sowie der jeweiligen CP (sofern vorhanden) zu arbeiten und die Identität der Antragsteller entsprechend den gesetzlichen Anforderungen und denen der jeweiligen CP (sofern vorhanden) zuverlässig zu prüfen. DGN wird eine entsprechende Verpflichtungserklärung zur Identifizierung der Endteilnehmer von jedem beauftragten Dritten einholen. Die Sicherheitsvorkehrungen werden eingehalten.

9.6.3 Verpflichtungen des Endteilnehmers (Zertifikatsinhabers)

Die Verpflichtungen des Endteilnehmers ergeben sich aus den zugrundliegenden vertraglichen Vereinbarungen sowie ggf. der jeweiligen CP.

9.6.4 Verpflichtungen des Endteilnehmers (Überprüfer eines Zertifikates, Relying Party)

Die Verpflichtungen des Endteilnehmers, der ein Zertifikat überprüfen möchte, ergeben sich aus den zugrundliegenden vertraglichen Vereinbarungen sowie ggf. der jeweiligen CP.

9.7 Gewährleistung

Die DGN bietet alle Dienstleistungen mit der gesetzlichen Pflicht zur Mängelbeseitigung (Gewährleistung) an.

9.8 Haftungsbeschränkung

Die DGN haftet gemäß den gesetzlichen Bestimmungen sowie den entsprechenden Allgemeinen Geschäftsbedingungen (siehe http://www.dgn.de/agb).

9.9 Haftungsfreistellung

Die Verwendung der privaten Schlüssel obliegt, soweit in einer jeweiligen CP nicht anderweitig geregelt, ausschließlich dem Zertifikatsinhaber. Dieser haftet allein für alle aus der Verwendung resultierenden Schäden und stellt die DGN von eventuellen Ansprüchen frei, die Dritte gegen sie erheben könnten.

9.10 Inkrafttreten und Aufhebung

Dieses Certification Practice Statement (CPS) wird durch die DGN verwaltet und tritt mit seiner Freigabe in Kraft.

Es kann unter Wahrung bestehender Vertragsverhältnisse jederzeit aufgehoben werden.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Eine individuelle Benachrichtigung oder aktive Kommunikation mit den Teilnehmern ist nicht vorgesehen.

9.12 Änderungen und Ergänzungen der Richtlinien

Diese Richtlinie kann unter Wahrung bestehender Vertragsverhältnisse jederzeit ergänzt oder geändert werden. Eine neue Version wird unter http://www.dgn.de bekannt gegeben.

9.13 Konfliktbeilegung

Im Falle von Streitigkeiten steht der Rechtsweg offen.

9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland.

9.15 Konformität mit dem geltenden Recht

Keine Angaben.

9.16 Weitere Regelungen

Keine.

9.17 Andere Regelungen

Keine.