

Dokumentation Trustcenter

Certificate Policy TypeA-Zertifikate

Änderungshistorie:

Version	Stand	Änderungen	Autor	Status
0.1	13.06.2006	Initialversion	BN	Entwurf
0.9	03.07.2006	Vervollständigung	Knut Goldberg, Robert Kurz	Entwurf
1.0	27.07.2006	Freigabe	Knut Goldberg, Robert Kurz	Freigegeben
1.01	04.08.2006	Korrektur Kap. 7.1.3/7.1.4	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	03.08.2007	Einarbeitung Kommen- tare BNetzA	Knut Goldberg	Entwurf
1.2	09.08.2007	Freigabe	Robert Kurz	Freigegeben

Inhaltsverzeichnis

1	Einleitung.....	5
1.1	Überblick	5
1.2	Identifikation des Dokumentes	5
1.3	Teilnehmer der Zertifizierungsinfrastruktur	6
1.4	Anwendungsbereich.....	7
1.5	Verwaltung der Richtlinie.....	7
1.6	Definitionen und Abkürzungen	7
2	Veröffentlichungen und Verzeichnisdienst.....	9
2.1	Verzeichnisdienst	9
2.2	Veröffentlichung von Informationen.....	9
2.3	Aktualisierung.....	9
2.4	Zugang zu den Diensten	9
3	Identifizierung und Authentifizierung	10
3.1	Namensgebung	10
3.2	Erstregistrierung.....	11
3.3	Routinemäßige Erneuerung / Rezertifizierung	11
3.4	Revokationsantrag	11
4	Betriebliche Abläufe	12
4.1	Antrag auf Ausstellung von Zertifikaten.....	12
4.2	Bearbeitung von Zertifikatsanträgen.....	12
4.3	Zertifikatsausstellung.....	12
4.4	Entgegennahme von Zertifikaten / SSEE	12
4.5	Verwendung des Schlüsselpaares und des Zertifikats	12
4.6	Zertifikatserneuerung / Wiederezertifizierung	13
4.7	Zertifikatserneuerung / Re-Key	13
4.8	Zertifikatsmodifizierung	13
	Sperrung und Suspendierung von Zertifikaten.....	13
4.10	Online-Überprüfung eines Zertifikates (Statusabfrage)	15
4.11	Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer.....	15
4.12	Schlüsselhinterlegung und –wiederherstellung	15
5	Infrastruktur und betriebliche Abläufe	16

Certificate Policy TypeA-Zertifikate

5.1	Physische Sicherheitsmaßnahmen	16
5.2	Organisatorische Sicherheitsmaßnahmen	16
5.3	Personelle Sicherheitsmaßnahmen.....	16
5.4	Audit und Logging Prozeduren.....	16
5.5	Datensicherung	16
5.6	CA-Schlüsselwechsel.....	16
5.7	Notfall und Recovery	16
5.8	Einstellung des Betriebes.....	16
6	Technische Sicherheitsmaßnahmen	17
6.1	Schlüsselpaarerstellung und Installation.....	17
6.2	Schutz des privaten Schlüssels.....	18
6.3	Weitere Aspekte des Schlüsselmanagements	19
6.4	Aktivierungsdaten.....	19
6.5	Sicherheitsmaßnahmen für Computersysteme	20
6.6	Life-Cycle der Sicherheitsmaßnahmen	20
6.7	Sicherheitsmaßnahmen für Netzwerke	20
6.8	Zeitstempel.....	20
7	Profile für Zertifikate, Widerruflisten und Online-Statusabfragen	21
7.1	Profile für Zertifikate	21
7.2	Profil der Revokationslisten.....	22
7.3	OCSP Profil.....	22
8	Konformitätsprüfung	23
8.1	Frequenz und Umstände der Überprüfung.....	23
8.2	Identität des Überprüfers.....	23
8.3	Verhältnis von Prüfer zu Überprüftem	23
8.4	Überprüfte Bereiche	23
8.5	Fehlerkorrektur.....	23
8.6	Veröffentlichung der Ergebnisse	23
9	Sonstige Regelungen	24
9.1	Gebühren	24
9.2	Finanzielle Verantwortung.....	24
9.3	Vertraulichkeit von Geschäftsinformationen	24
9.4	Schutz personenbezogener Daten (Datenschutz).....	24

Certificate Policy TypeA-Zertifikate

9.5	Urheberrechte	25
9.6	Verpflichtungen	25
9.7	Gewährleistung	26
9.8	Haftungsbeschränkung	26
9.9	Haftungsfreistellung.....	26
9.10	Inkrafttreten und Aufhebung.....	26
9.11	Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern.....	27
9.12	Änderungen und Ergänzungen der Richtlinien.....	27
9.13	Konfliktbeilegung.....	27
9.14	Geltendes Recht.....	27
9.15	Konformität mit dem geltenden Recht	27
9.16	Weitere Regelungen.....	27
9.17	Andere Regelungen	27

1 Einleitung

Die Zukunft des Gesundheitswesens ist digital. Webgestützte Kommunikation und Transaktion spielen im Arbeitsalltag von Heilberufsangehörigen eine immer größere Rolle. Als modernes Dienstleistungsunternehmen verfolgt die DGN Service GmbH ein klares Ziel: Mit innovativen Online-Services und besonders sicheren, maßgeschneiderten IT-Lösungen für Health Professionals wollen wir die Zukunft des Gesundheitswesens mitgestalten.

Die DGN Service GmbH setzt beim Thema Sicherheit auf Public Key Infrastrukturen (PKI) und bietet dazu unterschiedliche Klassen von Zertifizierungsdienstleistungen an, wobei die unterschiedlichen Klassen nicht nur unterschiedliche Zielgruppen und Mandanten adressieren, sondern auch abgestufte Sicherheitsanforderungen beinhalten.

1.1 Überblick

Die vorliegende Certificate Policy (CP) enthält die Richtlinien für die Vergabe von qualifizierten Zertifikaten durch den von der DGN Service GmbH betriebenen Zertifizierungsdienst mit freiwilliger Anbieterakkreditierung. In dieser Policy werden die Informationen zur Verwendung der angebotenen Zertifikate des Typs A bereitgestellt. Informationen zur Umsetzung der Richtlinien für den qualifizierten Betrieb des Trustcenters der DGN Service GmbH werden im „Certification Practice Statement Richtlinien für qualifizierte Zertifikate“ (qCPS) des Trustcenters aufgeführt.

Die CP liefert den Maßstab für das Niveau der Sicherheit der Zertifikate und bildet die Vertrauensgrundlage der Endteilnehmer und der Öffentlichkeit gegenüber diesen Zertifikaten.

Die Certificate Policy ist Bestandteil der Allgemeinen Geschäftsbedingungen für Trustcenterdienstleistungen und –produkte der DGN Service GmbH, die der Teilnehmer mit der Beantragung der Zertifikate bzw. der dgnserviceCard anerkennt.

Dieses Dokument bezieht sich auf technische und organisatorische Sachverhalte, die sich auf die spezielle, hier aufgeführte Zertifikate beschränken. Für vorhandene andere Zertifikatsklassen gelten eigene 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 Policy Type A Zertifikate

Version: 1.2

Datum: 09.08.2007

Status: Freigegeben

OID: 1.3.6.1.4.1.15787.2.1.4.2.1

1.3 Teilnehmer der Zertifizierungsinfrastruktur

Das Trustcenter wird von der Firma DGN Service GmbH, Düsseldorf betrieben. Es werden Zertifikate für Mitglieder des deutschen Gesundheitswesens aber auch für die Öffentlichkeit ausgestellt.

1.3.1 CAs

Die Root-CA des DGN Service Trustcenters für qualifizierte Zertifikate des Typs A ist die CA der Bundesnetzagentur (CA BNetzA).

Untergeordnete CA-Zertifikate (Sub-CAs) werden von der jeweiligen Root-CA zertifiziert.

Das CA-Zertifikat für qualifizierte Signaturzertifikate wird mit „Type A“ im CN gekennzeichnet.

Die untergeordneten Sub-CAs der DGN Service GmbH zertifizieren die öffentlichen Schlüssel der Endteilnehmer.

1.3.2 RA

Gemäß den gesetzlichen Vorgaben wird die Identifizierung der Antragsteller durch zuvor bestellte Personen der DGN Service GmbH oder beauftragte Dritte durchgeführt. Diese erfolgt entweder persönlich oder durch Prüfung der Antragsdaten gegen bereits registrierte Daten des Antragstellers, die auf Basis einer früheren persönlichen Vorstellung erhoben wurden.

Beauftragte Dritte werden durch die DGN Service GmbH benannt und zur Einhaltung der vorliegenden Richtlinie verpflichtet.

Die RA führt eine Antragsprüfung und eine Identifizierung auf Basis von Ausweisdaten durch. Näheres regelt Abschnitt 3.2.3.

1.3.3 Endteilnehmer

Die Vergabe von Zertifikaten richtet sich primär, aber nicht exklusiv, an Vertreter und Mitarbeiter des deutschen Gesundheitswesens.

Die Vergabe erfolgt nur an natürliche Personen, für juristische Personen und für Maschinen werden keine Zertifikate unter dieser CP ausgestellt.

1.3.4 Relying Party

Keine Angaben.

1.3.5 Sonstige

Keine.

1.4 Anwendungsbereich

Die Zertifikate der hier beschriebenen Zertifikatsklasse können für

- Signatur (Signaturzertifikat)
- Bestätigungen (Attributzertifikat)

verwendet werden. Die mit dem Signaturzertifikat erzeugten Signaturen sind qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung im Sinne des deutschen Signaturgesetzes.

Die Zertifizierung weiterer untergeordneter Zertifikate ist nicht gestattet.

1.5 Verwaltung der Richtlinie

Die vorliegende Richtlinie wurde erstellt, registriert und wird fortgeschrieben von der DGN Service GmbH.

Postadresse:

DGN Service GmbH
Postfach 102 144
40012 Düsseldorf

Email: trustcenter@dgnservice.de

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

Weitere Informationen über das Trustcenter und das angebotene Service-Portfolio sind unter <http://www.dgnservice.de/trustcenter> 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	Certification 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.
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol

Certificate Policy TypeA-Zertifikate

PN	Pseudonym, Kennzeichnung im DN bei pseudonymen Namen
RA	Registration Authority, hier: Stelle zur Identifizierung und Überprüfung von Zertifikatsantragstellern
Revokation	Sperrung / Widerruf eines Zertifikats
Zertifikat	Zuordnung eines kryptographischen Schlüssels zu einer Identität

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienst

Es ist ein Verzeichnisdienst zu betreiben, über den die öffentlichen Zertifikate abgerufen werden können.

2.2 Veröffentlichung von Informationen

Das Trustcenter muss folgende Informationen öffentlich verfügbar machen:

- Diese Certificate Policy (CP),
- die aktuell gültigen CRLs,
- die CA-Zertifikate jeweils mit „Fingerabdruck“.

2.3 Aktualisierung

Aktualisierte Informationen, z.B. im Falle einer Zertifikatssperrung, werden unverzüglich publiziert. Neue CRLs sollten mindestens alle 33 Tage bereitgestellt werden.

2.4 Zugang zu den Diensten

Der lesende Zugriff auf die unter 2.1 und 2.2 veröffentlichten Informationen sollte keiner Zugangskontrolle unterliegen, schreibenden Zugriff dürfen nur autorisierte Mitarbeiter erlangen. Die Systeme sind gegen unautorisierte Schreibzugriffe besonders zu schützen.

3 Identifizierung und Authentifizierung

3.1 Namensgebung

3.1.1 Namenstypen

Es sind Namenshierarchien der Normenserie X.500 zu nutzen, Für Personen kann entweder der reale Name oder ein Pseudonym verwendet werden, das als solches gekennzeichnet sein muss (Zusatz „:PN“ am Common Name).

Das Trustcenter darf nur Namen aus dem ihm zugeordneten Namensraum vergeben.

3.1.2 Aussagekraft von Namen

Die Eindeutigkeit der Identifikation des Endteilnehmers durch seinen Namen (DN) im Zertifikat muss gegeben sein. Der verwendete Name (DN) muss sich daher entweder auf den realen Namen des Teilnehmers beschränken oder pseudonym sein. In letzterem Fall muss das Pseudonym nicht aussagekräftig sein, mögliche Verwechslungen mit natürlichen Personen oder Syntaxelementen (z.B. DNS-Namen, IP-Adressen, Mail-Adressen) sind aber zu vermeiden.

3.1.3 Anonyme / Pseudonyme

Es müssen keine Zertifikate für anonyme Teilnehmer, wohl aber pseudonyme Namen unterstützt werden.

3.1.4 Interpretationsregeln für Namensformen

Der Zusatz „:PN“ darf nur im Zusammenhang mit der Verwendung von Pseudonymen vorkommen.

3.1.5 Eindeutigkeit von Namen

Der Distinguished Name des Endteilnehmer muss eindeutig sein.

3.1.6 Maßnahmen zur Auflösung von Streitigkeiten über einen Namen

Ein auf einen unzulässigen Namen ausgestelltes Zertifikat muss sofort nach bekannt werden der Rechtsverletzung gesperrt werden.

3.1.7 Anerkennung von Warenzeichen

Nur natürliche Personen dürfen ein Zertifikat dieser Zertifikatsklasse beantragen und erhalten. Da der Name auf dem Zertifikat sich explizit auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen somit nicht relevant.

Sollten bei Verwendung von Pseudonymen Markenrechte, Warenzeichen oder andere Rechte verletzt werden, muss das Trustcenter umgehend nach bekannt werden der Verletzung das betroffene Zertifikat sperren.

3.2 Erstregistrierung

3.2.1 Maßnahmen zur Überprüfung des Besitzes des privaten Schlüssels auf der SSEE, der zum zertifizierten öffentlichen Schlüssel gehört.

Der ZDA muss sich vom Besitz des privaten Schlüssels, der sich auf der SSEE befindet, gemäß den gesetzlichen Vorgaben überzeugen.

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

3.2.2 Authentisierung von Organisationen

Nur natürliche Personen dürfen ein Zertifikat dieser Zertifikatsklasse beantragen und erhalten.

3.2.3 Authentisierung von Personen

Personen, die ein Zertifikat dieser Zertifikatsklasse beantragen, müssen bei der Antragstellung sicher identifiziert werden.

3.2.4 Nicht überprüfte Attribute

Im Zertifikat aufgenommene Attribute Email-Adresse und freiwillige Beschränkungen müssen nicht explizit überprüft werden.

3.2.5 Überprüfung fremder CAs, RAs

Eine Crosszertifizierung anderer CAs oder Einbeziehung fremder RAs ist für diese Zertifikatsklasse derzeit nicht geplant.

3.2.6 Interoperabilität

Interoperabilität mit anderen PKI wird nicht gefordert.

3.3 Routinemäßige Erneuerung / Rezertifizierung

Eine routinemäßige Rezertifizierung wird nicht gefordert.

3.4 Revokationsantrag

Die Revokation eines Zertifikates erfordert eine effektive Prüfung der Autorisierung der Sperrantragstellenden Person. Es sind mindestens ein schriftliches Verfahren und ein telekommunikatives Verfahren für die Antragstellung gemäß den Vorgaben aus SigG/SigV einzurichten.

4 Betriebliche Abläufe

4.1 Antrag auf Ausstellung von Zertifikaten

Ein Antrag auf Ausstellung von Zertifikaten dieser Zertifikatsklasse darf nur persönlich und von einer natürlichen Person gestellt werden. Die Identifikation des Antragstellers muss nach den gesetzlichen Vorgaben sowie den Regelungen des Kapitels 3.2.3 dieser Certificate Policy erfolgen.

4.2 Bearbeitung von Zertifikatsanträgen

Die Antragsprüfung muss im 4-Augen-Prinzip erfolgen,

4.3 Zertifikatsausstellung

Nach Eingang und erfolgreicher Prüfung eines Zertifikatsantrags können die beantragten Zertifikate produziert werden, sofern keine weiteren Gründe gegen eine Produktion stehen.

4.4 Entgegennahme von Zertifikaten / SSEE

Die vom Trustcenter personalisierte SSEE muss entweder per Post im PostIdent-Verfahren der Deutschen Post AG zugestellt oder persönlich übergeben werden. Es können weitere Verfahren mit dem Antragsteller vereinbart werden.

Erst nach Vorliegen der Empfangsbestätigung im Trustcenter dürfen die zugehörigen Zertifikate aktiviert bzw. veröffentlicht werden.

Mit Annahme des Zertifikats versichert der Zertifikatsinhaber allen Teilnehmern der DGN Service PKI, dass sämtliche Daten und Erklärungen in Bezug auf die im Zertifikat enthaltenen Angaben wahr sind und ihre Verwendung im Einklang mit der vorliegenden Policy stehen.

Ferner sichert der Zertifikatsinhaber zu, dass er keiner unbefugten Person Zugang und Zugriff auf den privaten Schlüssel (die SSEE) verschaffen wird und den privaten Schlüssel (die SSEE) geschützt aufbewahren wird.

Für den Fall des Kartenverlusts, der möglichen Kompromittierung des privaten Schlüssels oder sofern Angaben des Zertifikats nicht mehr korrekt sind, wird der Karteninhaber die unverzügliche Sperrung der Zertifikate (Revokation) beantragen.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Die Verwendung der auf der Signaturkarte aufgebrauchten Schlüssel und Zertifikate muss auf den jeweiligen Anwendungskontext

-
- Signatur (Signaturzertifikat)

Certificate Policy TypeA-Zertifikate

- Attributprüfung (Attributzertifikat)

beschränkt sein. Eine bestimmungswidrige Nutzung ist nicht erlaubt.

4.6 Zertifikatserneuerung / Wiederzertifizierung

Ein Verfahren zur Zertifikatserneuerung / Wiederzertifizierung ist nicht gefordert.

4.7 Zertifikatserneuerung / Re-Key

Ein Verfahren zur Zertifikatserneuerung / Re-Keying ist nicht gefordert.

4.8 Zertifikatsmodifizierung

Eine Änderung von Inhalten der Zertifikate (z.B. nach Namensänderung) muss durchgeführt werden können.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Revokationsgründe

Ein Zertifikat muss revoziert (gesperrt) werden können bei:

- Kompromittierung des privaten Schlüssels des Endteilnehmers oder der CA
- Verlust oder Diebstahl des privaten Schlüssels des Endteilnehmers
- Vertragsbruch seitens des Endteilnehmers oder des Trustcenters
- Ausstellung des Zertifikats auf Grundlage falscher Daten
- Änderung der Daten des Endteilnehmers, die Grundlage der Zertifikatserstellung waren (z.B. Namensänderung)
- Wegfall der Berechtigung zum Führen eines berufsgruppenspezifischen Attributes (z.B. Arzt, Zahnarzt, Apotheker)
- Auf Wunsch des Endteilnehmers

4.9.2 Berechtigte Personen, die eine Revokation veranlassen können

Zur Sperrung eines Zertifikats müssen der Zertifikatseigentümer oder ein von ihm benannter Vertreter, Attributvergebende Stellen sowie die Bundesnetzagentur und Mitarbeiter des Trustcenters berechtigt sein.

4.9.3 Prozedur für einen Antrag auf Revokation

Der Antrag auf Revokation muss sowohl schriftlich (Papier/Brief) als auch mündlich (auch telefonisch) erfolgen können.

Zur Bearbeitung sind folgende Informationen nötig:

Certificate Policy TypeA-Zertifikate

Schriftlich oder elektronisch: Vorname und Name bzw. Pseudonym des Zertifikatsinhabers und Informationen zur Identifikation der zu sperrenden Zertifikate. Dabei werden die Signatur und/oder das angegebene Revokationspasswort geprüft.

Telefonisch: Vorname und Name bzw. Pseudonym des Zertifikatsinhabers, Informationen zur Identifikation der zu sperrenden Zertifikate sowie das Revokations- bzw. Autorisierungspasswort oder eine alternativ zum Revokationspasswort angegebene Antwort zu einer Sperrfrage. Die Daten werden erfragt, wobei ggf. noch weitere Einzelheiten über die zu revozierende Signaturkarte mitgeteilt werden müssen.

Nach erfolgreicher Prüfung des Antrages wird ein interner Antrag auf Revokation in das Sperr-System eingegeben und die Sperr-CA weitergegeben. Der Zeitpunkt der Eingabe des Antrages in das Sperr-System gilt als Sperrzeitpunkt. Anschließend stellt die Sperr-CA eine neue CRL (Revokationsliste) aus.

Es werden stets alle Zertifikate einer SSEE revoziert. Die neue CRL wird vom Verzeichnisdienst der Öffentlichkeit zur Verfügung gestellt.

4.9.4 Revokationsfrist für den Zertifikatsinhaber

Bei begründetem Verdacht einer Kompromittierung des privaten Schlüssels eines Endteilnehmers 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 muss unverzüglich durchgeführt werden.

4.9.6 Mechanismen für Relying Parties

Derartige Mechanismen werden nicht unterstützt.

4.9.7 Aktualisierungsfrequenz einer CRL (Liste revozierter Zertifikate)

Die CRL muss aktualisiert werden, sobald ein Zertifikat widerrufen wird.

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

Neue CRLs müssen spätestens alle 35 Tage veröffentlicht werden.

4.9.9 Online Zugriffsmöglichkeiten auf CRL

Die CRL muss online über mindestens zwei Arten abrufbar sein.

4.9.10 CRL: Anforderungen an Endteilnehmer

Ein Endteilnehmer, der ein Zertifikat benutzen möchte (insbesondere, wenn eine Signatur überprüft wird), ist verpflichtet zu überprüfen, ob das entsprechende Zertifikat gültig ist oder widerrufen wurde.

Die Benutzung eines Zertifikates ohne vorherige Überprüfung ist nicht gestattet.

4.9.11 Andere Formen der Bekanntgabe von Revokationen

Die Überprüfung der Revokation eines Zertifikates muss über eine Revokationsliste oder OCSP Anfrage durchgeführt werden können. Andere Formen müssen nicht vorgesehen werden.

4.9.12 Spezielle Anforderungen bei Re-Keying Kompromittierung

Re-Keying muss nicht unterstützt werden.

4.9.13 Gründe für Suspendierung

Die Suspendierung von Zertifikaten muss nicht unterstützt werden.

4.9.14 Berechtigte für die Suspendierung

Die Suspendierung von Zertifikaten muss nicht unterstützt werden.

4.9.15 Verfahren bei der Suspendierung

Die Suspendierung von Zertifikaten muss nicht unterstützt werden.

4.9.16 Zeitrestriktionen für die Suspendierung

Die Suspendierung von Zertifikaten muss nicht unterstützt werden.

4.10 Online-Überprüfung eines Zertifikates (Statusabfrage)

Die Überprüfung eines Zertifikates ist über Revokationslisten (CRL) oder OCSP Anfragen möglich.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Die Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer wird in den allgemeinen Geschäftsbedingungen des Anbieters geregelt, zusätzliche Vereinbarungen können in den Vertragsunterlagen enthalten sein.

4.12 Schlüsselhinterlegung und –wiederherstellung

Eine Hinterlegung oder Sicherungsarchivierung privater Schlüssel der Zertifikate darf nicht erfolgen.

5 Infrastruktur und betriebliche Abläufe

Nicht alle Informationen dieses Themenbereichs sind öffentlich.

5.1 Physische Sicherheitsmaßnahmen

Die physischen Sicherheitsmaßnahmen müssen den Anforderungen des Signaturgesetzes genügen.

5.2 Organisatorische Sicherheitsmaßnahmen

Die organisatorischen Sicherheitsmaßnahmen müssen den Anforderungen des Signaturgesetzes genügen.

5.3 Personelle Sicherheitsmaßnahmen

Die personellen Sicherheitsmaßnahmen müssen den Anforderungen des Signaturgesetzes genügen.

5.4 Audit und Logging Prozeduren

Audit und Logging müssen gemäß den Anforderungen des Signaturgesetzes durchgeführt werden.

5.5 Datensicherung

Datensicherung muss gemäß den Anforderungen des Signaturgesetzes durchgeführt werden.

5.6 CA-Schlüsselwechsel

Bei einem Schlüsselwechsel der CA muss ein neues CA-Zertifikat bei der Bundesnetzagentur beantragt werden.

5.7 Notfall und Recovery

Für den Notfall muss ein Notfallhandbuch existieren, dessen Informationen eine schnellstmögliche Wiederherstellung der Daten und Systeme und damit die Wiederherstellung der Betriebsfähigkeit ermöglichen.

5.8 Einstellung des Betriebes

Bei Einstellung des Betriebes muss ein nachfolgender Dienstleister die Bereitstellung der Zertifikate fortführen. 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

Private Schlüssel müssen nicht auslesbar auf SSEE gespeichert werden.

Die Schlüssel der CA müssen signaturgesetzkonform erzeugt werden.

Die qualifizierten Signaturschlüssel der Endteilnehmer müssen signaturgesetzkonform erzeugt werden.

6.1.2 Auslieferung des privaten Schlüssels

Die Auslieferung des privaten Schlüssels kann mit dem Antragsteller vor Auslieferung vereinbart werden. Vorzusehen sind mindestens die Verfahren PostIdent der Deutschen Post AG und eine persönliche Übergabe.

6.1.3 Auslieferung des öffentlichen Schlüssels an den Zertifikatsinhaber

Der öffentliche Schlüssel des Endteilnehmers muss zusammen mit dem privaten Schlüssel bzw. dem Teilnehmerzertifikat ausgeliefert werden.

6.1.4 Auslieferung der öffentlichen Root- und CA-Schlüssel

Die öffentlichen Schlüssel der CAs des Trustcenters müssen zusammen mit ihren Fingerprints im Internet zum Abruf bereitgestellt werden.

Die Veröffentlichung des öffentlichen Schlüssels der Root obliegt der Bundesnetzagentur.

6.1.5 Verwendete Schlüssellängen

Es dürfen nur die jeweils von der Bundesnetzagentur oder BSI empfohlenen Schlüssellängen verwendet werden. Diese sind aktuell 2048 Bit für den CA-Schlüssel und 2048 Bit für die Schlüssel der Endteilnehmer. Eine Vergrößerung der Schlüssellänge kann in der Zukunft erfolgen, ohne dass diese im CP vermerkt werden muss.

6.1.6 Parameter der öffentlichen Schlüssel

Die Parameter der öffentlichen Schlüssel müssen von der CA des Trustcenters erzeugt werden.

6.1.7 Verwendungszweck der Schlüssel

Beschränkungen aller Nicht-CA-Zertifikate: CA: false (critical)

Certificate Policy TypeA-Zertifikate

Die Schlüssel der Endteilnehmer erhalten folgenden Verwendungszweck, wie im entsprechenden Feld des X.509v3 Zertifikates aufgeführt:

Signaturschlüssel:

Non Repudiation (critical)

Die Parameter müssen bei deren Festlegung sorgfältig ausgewählt und überprüft werden.

6.2 Schutz des privaten Schlüssels

6.2.1 Standards des Schlüssel erzeugenden kryptographischen Moduls

Die Teilnehmerschlüssel der qualifizierten Signaturzertifikate müssen signaturgesetzkonform auf entsprechenden geprüften und bestätigten Modulen erzeugt werden.

6.2.2 Schlüsselteilung (key-sharing Algorithmus)

Die Schlüssel der Endteilnehmer werden nicht geteilt.

6.2.3 Schlüssel hinterlegung

Eine Hinterlegung der Teilnehmerschlüssel wird nicht gefordert.

6.2.4 Backup von privaten Schlüsseln

Ein Backup von privaten Schlüsseln darf nicht möglich sein.

6.2.5 Archivierung privater Schlüssel

Es wird keine Archivierungsmöglichkeit von Schlüsseln (Smartcards) von Endteilnehmern gefordert.

6.2.6 Transfer privater Schlüssel in ein Kryptomodul

Der Transfer fremderzeugter Schlüssel muss nicht unterstützt werden.

6.2.7 Speicherung privater Schlüssel in ein Kryptomodul

Die privaten Schlüssel der qualifizierten Signaturzertifikate eines Endteilnehmers müssen konform zu SigG/SigV erzeugt und auf geprüften und bestätigten SSEE nicht auslesbar gespeichert werden.

6.2.8 Aktivierung privater Schlüssel

Ein privater Schlüssel einer Signaturkarte darf nur nach Eingabe einer PIN aktiviert werden.

6.2.9 Deaktivierung privater Schlüssel

Die Signaturschlüssel einer Signaturkarte müssen nach aufeinanderfolgender, dreimaliger Eingabe einer falschen PIN unwiderruflich blockiert werden. Andere Schlüssel dürfen mit einer PUK wieder freigeschaltet werden können.

6.2.10 Vernichtung privater Schlüssel

Die Schlüssel einer SSEE müssen endgültig vernichtet werden können.

6.2.11 Kryptomodul Rating

Es müssen die Vorgaben des Signaturgesetzes und der Signaturverordnung eingehalten werden.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel müssen archiviert werden.

6.3.2 Gültigkeit der Schlüsselpaare

Die Gültigkeit von qualifizierten Zertifikaten richtet sich nach den gesetzlichen Bestimmungen und beträgt maximal 5 Jahre. Nach Ablauf der Gültigkeit muss ein neues qualifiziertes Zertifikat (mit neuem Schlüssel) beantragt werden.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs)

Die PINs der CA-Schlüssel werden bei der Erzeugung festgelegt.

Die PINs der Endteilnehmer-Schlüssel sollen als Transport-PINs realisiert werden. Der Endteilnehmer muss verpflichtet werden, die PINs unverzüglich bei der ersten Inbetriebnahme seiner Signaturkarte zu ändern.

6.4.2 Schutz der Aktivierungsdaten

Die PINs der Endteilnehmer-Schlüssel sollen als Transport-PINs realisiert werden und stellen daher keine besonderen Anforderungen an Schutzmassnahmen für den Transport.

Auf der Signaturkarte werden die PINs elektronisch durch die Signaturkarte selbst geschützt. Sie können nicht ausgelesen werden. Der Endteilnehmer verpflichtet sich, die PINs unverzüglich (bei der ersten Inbetriebnahme seiner Signaturkarte) durch „Brechen“ der Transport-PINs zu ändern. Eine Weitergabe der PINs an weitere Personen ist nicht gestattet. Wenn der Verdacht besteht, dass eine andere Person die PINs kennt, ist der Zertifikatsinhaber verpflichtet, sie unverzüglich zu ändern. Eine

regelmäßige Änderung der PINs (z.B. monatlich) wird aus Sicherheitsgründen generell empfohlen.

6.4.3 Weitere Aspekte

Keine Angaben.

6.5 Sicherheitsmaßnahmen für Computersysteme

6.5.1 Spezifische Sicherheitsmaßnahmen für die Computersysteme

Der Betrieb der Trustcentersysteme muss auf einem durch eine unabhängige Prüfinstanz bestätigten Sicherheitskonzept nach SigG basieren.

6.5.2 Sicherheitseinstufung

Eine Sicherheitseinstufung der Computersysteme muss nicht durchgeführt werden.

6.6 Life-Cycle der Sicherheitsmaßnahmen

6.6.1 Sicherheitsmaßnahmen für die Entwicklung

Es muss sichergestellt werden, dass erforderliche Updates den Betrieb nicht gefährden.

6.6.2 Sicherheitsmanagement

Es ist ein Sicherheitsmanagement zu betreiben, das die Wirksamkeit der Sicherheitsmaßnahmen des Trustcenters überwacht.

6.6.3 Sicherheitseinstufung

Eine Sicherheitseinstufung muss nicht durchgeführt werden.

6.7 Sicherheitsmaßnahmen für Netzwerke

Die Kommunikation zwischen den Systemen in den gesicherten Bereich des Trustcenters darf nur über ausreichend gesicherte Verbindungen erfolgen, der Netzwerkverkehr muss überwacht und kontrolliert werden.

6.8 Zeitstempel

Ein Zeitstempeldienst muss nicht bereitgestellt werden. Es sind geeignete Maßnahmen zu treffen, die hinreichend genaue Systemzeiten ermöglichen.

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

7.1 Profile für Zertifikate

7.1.1 Version

Die vom Trustcenter der DGN Service GmbH ausgestellten Zertifikate sind X.509v3 Zertifikate.

7.1.2 Zertifikatserweiterungen

Die Teilnehmerzertifikate haben folgende Erweiterungen:

- Basic Constraint
- Key Usage
- Certificate Policy
- CRL Distribution Point
- Subject Alternative Name
- Authority Key Identifier
- Subject Key Identifier
- Admission

7.1.3 Object-Identifiers der kryptographischen Algorithmen

RSA: 1.2.840.113549.1.1.1

SHA-1 mit RSA-Verschlüsselung: 1.2.840.113549.1.1.5

7.1.4 Namensformen

Die Distinguished Names der Zertifikate haben folgende Form:

CN=Vorname(n) Nachname

SERIALNUMBER=AntragsID

OU=Organisationseinheit

O=Organisation

C=Landeskennung

Bei nicht gesetzten Parametern für O und/oder OU werden diese im Subject nicht gesetzt.

7.1.5 Beschränkungen für Namen

Keine Bestimmungen.

7.1.6 Object Identifiers für die Certificate Policies

Für jede Certificate Policy gibt es einen object identifier, der in der jeweiligen CP aufgeführt wird.

Der OID für diese Certificate Policy ist 1.3.6.1.4.1.15787.2.1.4.2.1.

7.1.7 Verwendung von Erweiterungen für Policy Constraints

Keine Bestimmungen.

7.1.8 Syntax und Semantik des Policy Qualifiers

Keine Bestimmungen.

7.1.9 Verarbeitungssemantik für kritische Certificate Policy Extension

Keine Bestimmungen.

7.2 Profil der Revokationslisten

7.2.1 Version

Die vom Trustcenter der DGN Service GmbH ausgestellten Revokationslisten sind X.509v2 CRLs.

7.2.2 CRL und CRL entry extensions

Für die CRLs werden keine Erweiterungen verwendet

7.3 OCSP Profil

7.3.1 OCSP Version

Der OCSP-Responder muss Anfragen akzeptieren, die konform zu RFC2560 gestellt werden, Antworten müssen ebenfalls konform zu RFC2560 sein. Mehrfachanfragen müssen nicht unterstützt werden.

7.3.2 OCSP Extensions

Das Abrufen von Zertifikaten muss gemäß ISIS-MTT Spezifikation unterstützt werden.

8 Konformitätsprüfung

Die Zertifizierungsstelle der DGN Service GmbH verpflichtet sich nach den hier und im CPS beschriebenen Abläufen zu verfahren. Eine Überprüfung der Einhaltung dieser Verpflichtung kann durch Auditierung erfolgen.

8.1 Frequenz und Umstände der Überprüfung

keine Angaben.

8.2 Identität des Überprüfers

Die Audits müssen mindestens im Rahmen einer internen Revision durch den Revisor des Trustcenters durchgeführt werden.

8.3 Verhältnis von Prüfer zu Überprüftem

Der Auditor wird als Revisor des Trustcenters beauftragt. Er darf keine weiteren Aufgaben im operativen Betrieb des Trustcenters wahrnehmen.

8.4 Überprüfte Bereiche

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

8.5 Fehlerkorrektur

Werden Mängel festgestellt, müssen sofort geeignete Maßnahmen zu deren Beseitigung eingeleitet werden. Falls die Sicherheit des Trustcenters gefährdet ist, muss der Betrieb bis zur Beseitigung der Mängel eingestellt werden.

8.6 Veröffentlichung der Ergebnisse

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

9 Sonstige Regelungen

9.1 Gebühren

Die Gebühren für Leistungen des Trustcenters können der jeweils aktuellen Preisliste (unter <http://www.dgnservice.de>) entnommen werden.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Keine Angaben

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 mit Geschäftsinformationen sowie deren Weitergabe erfolgt gemäß Sicherheitseinstufung.

9.4 Schutz personenbezogener Daten (Datenschutz)

Im Rahmen des Betriebs des Trustcenters werden persönliche Daten erhoben. Diese müssen nach den Richtlinien des Bundesdatenschutzgesetzes, der Datenschutzgesetze der Länder und §14 des Signaturgesetzes behandelt werden.

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 Zerti-

fikats (CRLs, OCSP) enthalten sind oder die aus diesen Daten ableitbar sind, öffentlich und damit nicht vertraulich.

9.4.3 Verantwortung für vertraulich zu behandelnde Informationen

Das Trustcenter muss vertrauliche Kundendaten mit derselben Sorgfalt sichern, mit der auch eigene vertrauliche Daten gesichert werden. Eine Weitergabe vertraulicher Daten an Dritte darf nur erfolgen, wenn dazu vorher entsprechend geeignete Vertraulichkeitsvereinbarungen mit dem Empfänger abgeschlossen wurden.

9.5 Urheberrechte

CA-Zertifikate der DGN Service GmbH sowie die zugehörigen privaten und öffentlichen Schlüssel sind Eigentum der DGN Service GmbH.

Ihre Nutzung für Zwecke, die in dieser 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 CP vorgesehen sind, hat der Endteilnehmer durch den Zertifizierungsantrag zugestimmt.

9.6 Verpflichtungen

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

9.6.1 Verpflichtungen des Trustcenters, CA

Die CA als Instanz des Trustcenters verpflichtet sich, nach den Richtlinien dieser CP sowie des CPS und den Vorgaben aus SigG/SigV zu arbeiten. Insbesondere wird dem Schutz des privaten Schlüssels der CA absolute Priorität gegeben. Die CA stellt Zertifikate für Endteilnehmer gemäß dieser CP aus. Dafür vertraut sie der RA und lehnt unautorisierte Anträge ab. Die CA verpflichtet sich, Revokationsanträge unverzüglich zu bearbeiten und 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 Trustcenters, RA

Die RA des Trustcenters verpflichtet sich, nach den Richtlinien dieser CP sowie des CPS und den Vorgaben aus SigG/SigV zu arbeiten und die Identität der Endteilnehmer zuverlässig zu prüfen. Das Trustcenter wird eine entsprechende Verpflichtungserklärung zur Identifizierung der Endteilnehmer auch von jedem beauftragten Dritten einholen. Die Sicherheitsvorkehrungen werden eingehalten.

9.6.3 Verpflichtungen des Endteilnehmers (Zertifikatsinhabers)

Der Endteilnehmer, der ein Zertifikat der hier beschriebenen Zertifikatsklasse beantragt und erhält, verpflichtet sich, diese CP zu lesen und zu akzeptieren. Er verpflichtet sich, sein Zertifikat gemäß der im Zertifikat und in dieser CP angegebenen Zwecke und mit angemessener Vorsicht einzusetzen. Er muss seine SSEE schützen und darf ihn keinesfalls zusammen mit den zugehörigen PINs aufbewahren. Er muss die PINs nach Erhalt seiner SSEE vor der erstmaligen Verwendung unverzüglich ändern.

Der Zertifikatsinhaber muss sein Zertifikat sperren lassen, wenn er den Verdacht hat, dass der Schlüssel kompromittiert, abhanden gekommen oder verloren gegangen ist. Seine PINs muss er ändern, wenn der Verdacht besteht, dass sie anderen Personen bekannt wurden. Er ist verpflichtet, ggf. geänderte persönliche Daten (z.B. Name, Adresse usw.) an das Trustcenter zu melden.

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

Der Endteilnehmer, der ein Zertifikat überprüfen möchte, verpflichtet sich, diese Certification Policy zu lesen und zu akzeptieren. Er verpflichtet sich, das Zertifikat zu prüfen und gemäß der zulässigen Zwecke einzusetzen. Vor der Überprüfung einer Signatur muss er die Gültigkeit des Zertifikats anhand der aktuellen CRL oder über den Online-Statusdienst prüfen.

9.7 Gewährleistung

Das Trustcenter bietet alle Dienstleistungen mit der gesetzlichen Pflicht zur Mängelbeseitigung (Gewährleistung) an.

9.8 Haftungsbeschränkung

Die DGN Service GmbH haftet gemäß den gesetzlichen Bestimmungen sowie den entsprechenden Allgemeinen Geschäftsbedingungen.

9.9 Haftungsfreistellung

Die Verwendung der privaten Schlüssel obliegt ausschließlich dem jeweiligen Zertifikatsinhaber. Dieser haftet somit allein für alle aus der Verwendung resultierenden Schäden und stellt das Trustcenter von eventuellen Ansprüchen frei, die Dritte gegen sie erheben könnten.

9.10 Inkrafttreten und Aufhebung

Diese Certificate Policy wird durch die DGN Service GmbH verwaltet und tritt mit ihrer Veröffentlichung auf den Webseiten der Firma in Kraft.

Sie kann unter Wahrung bestehender Vertragsverhältnisse jederzeit aufgehoben werden. Eine Aufhebung wird unter <http://www.dgnservice.de> bekannt gegeben.

Certificate Policy TypeA-Zertifikate

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Eine individuelle Benachrichtigung oder aktive Kommunikation mit den Teilnehmern ist für diese Zertifikatsklasse 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.dgnservice.de> bekannt gegeben.

Die Bundesnetzagentur wird vorab unverzüglich über Änderungen informiert.

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

Die auf der Signaturkarte aufgebrachten Signaturzertifikate sind qualifizierte Zertifikate im Sinne des deutschen Signaturgesetzes. Mit dem dazugehörigen privaten Schlüssel können fortgeschrittene elektronische Signaturen erzeugt werden können.

9.16 Weitere Regelungen

Keine.

9.17 Andere Regelungen

Keine.