

Certificate-Policy für SMC Typ B Version 1.0

des Krankenhaus-Sektors

Stand: 20090313h

1	EINLEITUNG	4
1.1	Überblick	4
1.2	Identifikation des Dokuments	4
1.3	Teilnehmer der Zertifizierungsinfrastruktur.....	4
1.3.1	Zertifizierungsstellen (Certification Authorities)	4
1.3.2	SMC-Herausgeber (Registration Authorities)	4
1.3.3	Zertifikatsinhaber (Subscribers).....	4
1.3.4	Anwender (Relying Parties)	5
1.4	Anwendungsbereich.....	5
1.5	Pflege der Richtlinie	5
1.6	Definitionen und Abkürzungen	5
2	VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST	6
2.1	Verzeichnisdienst.....	6
2.2	Zugriffsberechtigung auf den Verzeichnisdienst	6
3	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG.....	7
3.1	Authentifizierung einer Organisation	7
3.2	Authentifizierung natürlicher Personen als Antragsteller.....	7
3.3	Ergänzende Unterlagen	7
3.4	Identifizierung und Authentifizierung bei Folgeanträgen	7
4	ABLAUFORGANISATION	8
4.1	Zertifikatsantrag	8
4.1.1	Antragsberechtigung	8
4.1.2	Verfahren und Verantwortung.....	8
4.2	Durchführung der Identifizierung und Authentifizierung	9
4.2.1	Identifizierung und Authentifizierung bei Neu- und Folgeanträgen	9
4.2.3	Identifizierung und Authentifizierung bei befristeter oder dauerhafter Sperrung.....	9

4.3 Durchführung der Zertifizierung	9
4.4 Zertifikatsakzeptanz bzw. Veröffentlichung des Zertifikates.....	10
4.5 Zertifikatserneuerung	10
4.6 Widerruf von Zertifikaten	10
4.6.1 Gründe für einen Widerruf	10
4.6.2 Ablauf eines Widerrufs	11
4.7 Dienst zur Statusabfrage von Zertifikaten (OCSP).....	11
4.8 Schlüsselhinterlegung und –wiederherstellung	11
5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMABNAHMEN	12
5.1 Archivierung	12
6 PROFILE FÜR ZERTIFIKATE, SPERRLISTEN UND ONLINE- STATUSABFRAGEN.....	13
6.1 Zertifikatsprofil.....	13
7 ANDERE GESCHÄFTLICHE UND RECHTLICHE ANGELEGENHEITEN.....	14
7.1 Verpflichtungen	14
7.1.1 Verpflichtungen der Zertifizierungsstellen.....	14
7.1.2 Verpflichtungen des SMC-Herausgebers	14
7.1.3 Verpflichtungen des Krankenhauses als Zertifikatsinhaber	15
7.2 Gewährleistungen	15
7.3 Haftungsbeschränkung und – freistellung	15
7.4 Änderungen der Richtlinie.....	16
7.4.1 Vorgehen bei Änderungen.....	16
7.4.2 Änderungen des Richtlinienbezeichners (OID).....	16
8 REFERENZVERZEICHNIS	17

1 EINLEITUNG

1.1 Überblick

Diese Zertifizierungsrichtlinie (Certificate Policy, CP) beschreibt die Anforderungen an die PKI für SMC Typ B des Krankenhausesektors.

Der Inhalt und Aufbau der Certificate Policy orientiert sich am RFC 3647.

Die in Abschnitt 8 referenzierten Dokumente bestimmen den Rahmen, nach denen SMCs vom Typ B ausgegeben werden dürfen.

1.2 Identifikation des Dokuments

Dokument

Dokumententyp: Certificate Policy

Name: Certificate-Policy für SMC Typ B Version 1.0

OID: 1.2.276.0.76.3.1.49.2.1

Referenz: [CP-SMKB-KH]

Version: 1.0

Datum: 13.03.2009

URL: <http://www.dkg-ev.de/dkg.php/cat/120/title/SMC-Policy>

1.3 Teilnehmer der Zertifizierungsinfrastruktur

1.3.1 Zertifizierungsstellen (Certification Authorities)

Zertifizierungsstellen (CAs) sind Stellen, die Zertifikate für SMCs vom Typ B nach den Regeln dieser Policy ausstellen. Zertifizierungsstellen werden von Zertifizierungsdiensteanbietern (ZDA) betrieben.

1.3.2 SMC-Herausgeber (Registration Authorities)

SMC-Herausgeber ist die Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG). Die DKTIG nimmt die Anträge entgegen und führt die Registrierung in einem mit dem ZDA abgestimmten Verfahren durch. Die DKTIG führt als Registration Authority die Identifizierung und Authentifizierung der beantragenden Organisation (Krankenhaus) sowie des Antragstellers (gesetzlicher Vertreter des Krankenhauses) durch und leitet die überprüften Anträge zur Zertifizierung an den ZDA weiter.

1.3.3 Zertifikatsinhaber (Subscribers)

Antragsteller ist der gesetzliche Vertreter der juristischen Person Krankenhaus (§§ 108, 109 SGB V, § 30 GewO). Dieser stellt den Antrag zur Ausgabe einer SMC Typ B persönlich bei der DKTIG.

Karteninhaber ist der gesetzliche Vertreter des Krankenhauses. Dieser nimmt die Verwaltung der SMC Typ B (übergeordnete Sachherrschaft) wahr. Er kann die Verwaltung der SMC Typ B durch Einräumen untergeordneter Sachherrschaft krankenhausesintern delegieren. Eine Delegation entbindet den Karteninhaber nicht von seiner Verantwortung für die ordnungsgemäße Verwendung der SMC Typ B.

Zertifikatsinhaber ist die juristische Person Krankenhaus, für welche die Zertifikate auf der SMC Typ B ausgestellt werden.

1.3.4 Anwender (Relying Parties)

Anwender sind Personen oder Dienste, die Zertifikate und kryptografische Schlüssel verwenden, die nach dieser Policy erstellt wurden.

1.4 Anwendungsbereich

Die vorliegende Richtlinie (Certificate Policy) stellt ein Regelwerk mit Anforderungen für den Krankenhaussektor dar. Sie regelt die Antragstellung, Erstellung von Zertifikaten, Ausgabe von Chipkarten (SMC Typ B) und deren Verwendung.

1.5 Pflege der Richtlinie

Die Pflege der Richtlinie (Policy) erfolgt durch den Policy-Herausgeber, die Deutsche Krankenhausgesellschaft (DKG), Wegelystraße 3, 10623 Berlin. Ansprechpartner für diese Policy ist seitens des Policy-Herausgebers das Dezernat III.

1.6 Definitionen und Abkürzungen

CA:	Certification Authority (Zertifizierungsstelle)
CHA:	Certificate Holder Authorization (Berechtigung des Karteninhabers)
CP:	Certificate Policy (Zertifizierungsrichtlinie)
CPS:	Certificate Practice Statement (Erklärung zum Zertifizierungsbetrieb)
gematik:	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
OCSP:	Online Certificate Status Protocol
OID:	Object Identifier (Objektidentifikator)
SMC Typ B:	Security Module Card (Sicherheitsmodulkarte) Typ B
TSL:	Trust-Service Status List
URL:	Uniform Resource Locator
ZDA:	Zertifizierungsdiensteanbieter

2 VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST

2.1 Verzeichnisdienst

Für organisationsbezogene Zertifikate wird ein Verzeichnisdienst betrieben.

2.2 Zugriffsberechtigung auf den Verzeichnisdienst

Alle Teilnehmer der Telematikinfrastruktur sind im Rahmen ihres anwendungsbezogenen Informationsbedarfs berechtigt, auf den Verzeichnisdienst zur Zertifikatssuche für die X.509-Zertifikate der SMC Typ B zuzugreifen.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Authentifizierung einer Organisation

Die Identität und der rechtliche Status des Krankenhauses, für das eine SMC Typ B beantragt wird, ist durch Bescheid der zuständigen Behörde (Aufnahme in den Krankenhausplan, hochschulrechtliche Anerkennung, Genehmigung des Versorgungsvertrages) gem. §§ 108, 109 SGB V oder Konzession gem. § 30 GewO nachzuweisen. Dem Antrag ist eine Kopie des Bescheids der zuständigen Behörde beizufügen.

3.2 Authentifizierung natürlicher Personen als Antragsteller

Natürliche Personen werden gemäß den Vorgaben des [SigG] identifiziert.

Der Antragsteller weist die ihm zustehende Vertretungsmacht für das Krankenhaus durch geeignete Unterlagen nach (z. B. Auszug aus dem Handelsregister). Dem Antrag ist eine Kopie der Legitimationsunterlage beizufügen.

3.3 Ergänzende Unterlagen

Auf gesondertes Verlangen der DKTIG ist dieser

- die Eigenschaft als Krankenhaus i. S. d. §§ 108, 109 SGB V, § 30 GewO,
- die Vertretungsmacht des Antragstellers

durch amtliche Beglaubigung der maßgeblichen Legitimationsurkunden nachzuweisen.

3.4 Identifizierung und Authentifizierung bei Folgeanträgen

Für Folgeanträge gelten die gleichen Anforderungen wie für Erstanträge.

4 ABLAUFORGANISATION

4.1 Zertifikatsantrag

4.1.1 Antragsberechtigung

Zulässig sind ausschließlich von dem gesetzlichen Vertreter des Krankenhauses persönlich gestellte Anträge zum Erhalt einer SMC Typ B. Eine Vertretung oder Delegation bei der Antragstellung ist unzulässig.

4.1.2 Verfahren und Verantwortung

Für die Zertifizierung sind folgende Unterlagen mit der Antragstellung beizubringen:

- a) Identifizierung und Authentifizierung der Organisation:
 - Bescheid der zuständigen Behörde (Aufnahme in den Krankenhausplan, hochschulrechtliche Anerkennung, Genehmigung des Versorgungsvertrages) gem. §§ 108, 109 SGB V oder Konzession gem. § 30 GewO
- b) Identifizierung und Authentifizierung des gesetzlichen Vertreters des Krankenhauses:
 - Identifikation des Antragstellers als natürliche Person nach den Vorgaben des SigG
 - Kopie der die Vertretungsmacht für das Krankenhaus ausweisenden Urkunde (z. B. Handelsregisterauszug).
- c) Zertifizierungsantrag mit
 - Institutionskennzeichen des Krankenhauses
 - Name des Krankenhauses
 - Anschrift des Krankenhauses
 - Name des gesetzlichen Vertreters des Krankenhauses (entsprechend den im Personalausweis geführten Angaben)
 - Kontaktdaten des gesetzlichen Vertreters
 - Kommunikationskennwort für Sperrungen
 - Benennung des zu beauftragenden ZDA, ggf. Vertrag mit dem ZDA.

Der Zertifizierungsantrag ist durch den gesetzlichen Vertreter des Krankenhauses als Antragsteller rechtsgültig zu unterzeichnen und an die DKTIG als SMC-Herausgeber zu übersenden.

Der Antragsteller ist zu wahren und vollständigen Angaben im Zertifikatsantrag verpflichtet. Die im Antrag aufgeführten Angaben sind Gegenstand der Registrierung. Die Identifikation des Karteninhabers gilt als abgeschlossen, wenn keine begründeten Zweifel an dessen Identität bestehen. Alle Angaben werden archiviert und sind über das Institutionskennzeichen identifizierbar. Liegt der DKTIG ein ordnungsgemäßer Zertifizierungsantrag vor, wird ein Zertifizierungsauftrag an den Zertifizierungsdiensteanbieter (ZDA) erteilt.

4.2 Durchführung der Identifizierung und Authentifizierung

4.2.1 Identifizierung und Authentifizierung bei Neu- und Folgeanträgen

Bei Neu- und auch Folgeanträgen zur Zertifikatserneuerung sind der DKTIG die unter Punkt 4.1.2 genannten Dokumente zu übersenden:

Postanschrift:
DKTIG
Talstraße 30
66119 Saarbrücken

Kontaktinformationen:
Tel.: 0681 / 5 88 16 10
Fax: 0681 / 5 89 69 09
E-Mail: mail@dktig.de
www.dktig.de

4.2.3 Identifizierung und Authentifizierung bei befristeter oder dauerhafter Sperrung

Ein Antrag auf befristete oder dauerhafte Sperrung kann sowohl schriftlich als auch (fern-)mündlich gestellt werden. Hierfür sind folgende Angaben erforderlich:

- Name des Zertifikatsinhabers (Krankenhausname)
- Institutionskennzeichen des Krankenhauses
- Seriennummer des Zertifikates
- Kommunikationskennwort für Sperrungen aus dem Zertifizierungsantrag
- Grund für die Sperrung .

Die Aufforderung zur Sperrung von SMC-Typ B (Clientzertifikaten) erfolgt gegenüber dem nachstehenden Adressaten:

Postanschrift:
DKTIG
Talstraße 30
66119 Saarbrücken

Kontaktinformationen:
Tel.: 0681 / 5 88 16 10
Fax: 0681 / 5 89 69 09
E-Mail: mail@dktig.de
www.dktig.de

4.3 Durchführung der Zertifizierung

Nach Weiterleitung des geprüften Zertifikatsantrags durch die DKTIG an den Zertifizierungsdiensteanbieter (ZDA) werden die beantragten Zertifikate vom Zertifizierungsdiensteanbieter (ZDA) produziert, sofern keine sonstigen Gründe einer Pro-

duktion entgegenstehen. Die Zertifizierung erfolgt nach Maßgabe der gesetzlichen Anforderungen.

4.4 Zertifikatsakzeptanz bzw. Veröffentlichung des Zertifikates

Die vom Zertifizierungsdiensteanbieter (ZDA) personalisierte Chipkarte (SMC Typ B) wird postalisch im PostIdent-Verfahren der Deutschen Post AG dem Antragsteller zugestellt oder ihm übergeben.

Die zugehörigen Zertifikate werden nach Vorliegen der Empfangsbestätigung des Antragstellers im Verzeichnisdienst des ZDA veröffentlicht, um allen Teilnehmern an der Telematikinfrastruktur einen Zugriff auf die X.509-Zertifikate der SMC Typ B zu ermöglichen.

Das Krankenhaus als Zertifikatsinhaber versichert, vertreten durch den Antragsteller, mit der Annahme des Zertifikats den Wahrheitsgehalt sämtlicher im Zertifikat enthaltenen Angaben und die Verwendung der SMC Typ B nach Maßgabe der vorliegenden Policy. Der Zertifikatsinhaber sichert zu, den privaten Schlüssel vor unbefugten Zugriffen zu sichern und geschützt aufzubewahren.

Für den Fall eines Kartenverlusts, der möglichen Kompromittierung des privaten Schlüssels oder einer notwendigen Änderung der Angaben des Zertifikats, hat der Zertifikatsinhaber unverzüglich die Sperrung der Zertifikate (Revokation) zu beantragen.

4.5 Zertifikatserneuerung

Eine Zertifikatserneuerung erfolgt zwingend, wenn sich die Angaben im Zertifikat innerhalb einer Gültigkeitsperiode geändert haben.

Eine Zertifikatserneuerung wird vom Zertifikatsinhaber durch dessen gesetzlichen Vertreter unter Vorlage der erforderlichen Legitimationsunterlagen beantragt (vgl. Punkt 4.1.2).

Bei jeder Zertifikatserneuerung wird eine neue Chipkarte mit neuem Zertifikat produziert und dem Antragsteller durch Post-Ident oder persönlich übermittelt.

4.6 Widerruf von Zertifikaten

4.6.1 Gründe für einen Widerruf

Antragsteller, Zertifikats- und Karteninhaber, SMC-Herausgeber und ZDA tragen in ihrem jeweiligen Verantwortungsbereich dafür Sorge, dass eine SMC Typ B nicht rechtswidrig verwendet wird. Bei Vorliegen eines Sperrgrundes sind die X.509-Zertifikate auf der SMC Typ B vom ZDA unverzüglich dauerhaft oder befristet zu sperren. CV-Zertifikate auf gesperrten SMC Typ B sind nachweislich vom weiteren Gebrauch auszuschließen. Bei dauerhafter Sperrung ist die Chipkarte nach Möglichkeit einzuziehen.

Ein Sperrgrund liegt insbesondere dann vor, wenn

- der Betrieb als Krankenhaus (§§ 108, 109 SGB V, § 30 GewO) endet, oder

- eine in den Zertifikaten bestätigte Eigenschaft nicht oder nicht mehr vorliegt, oder
- seitens des Krankenhauses im Antragsverfahren unwahre Tatsachen übermittelt wurden, oder
- sonstige zwingende Umstände bekannt werden, die eine Sperrung notwendig machen, oder
- durch ein Unterlassen der Sperrung eine Gefahr für den Schutz personenbezogener Daten entsteht.

Die befristete Sperrung eines Zertifikats hat für einen Zeitraum von bis zu 14 Tagen Geltung, um innerhalb dieses Zeitraums das tatsächliche Vorliegen von Sperrgründen zu prüfen. Wird die befristete Sperrung nicht innerhalb der 14 Tage ausdrücklich zurückgenommen, geht sie in eine dauerhafte Sperrung über.

4.6.2 Ablauf eines Widerrufs

Das Krankenhaus als Zertifikatsinhaber oder eine vom gesetzlichen Vertreter legitimierte Person innerhalb des Krankenhauses können unter Angabe der in Punkt 4.2.3 aufgeführten Informationen ein veröffentlichtes Zertifikat widerrufen.

Nach ordnungsgemäßer Prüfung des Widerrufs durch die DKTIG wird die sofortige dauerhafte oder befristete Sperrung des Zertifikats durch den Zertifizierungsdiensteanbieter (ZDA) veranlasst. Das Zertifikat wird entsprechend dem gestellten Antrag befristet oder dauerhaft aus dem Verzeichnisdienst herausgenommen und in einer von allen Teilnehmern der Telematikinfrastruktur über OCSP-Responder abfragbaren Statusliste veröffentlicht.

SMC-Herausgeber und Zertifizierungsdiensteanbieter können die befristete oder dauerhafte Sperrung eines Zertifikates veranlassen, sofern ein hinreichender Verdacht auf Kompromittierung des Schlüssels oder ein wesentlicher Verstoß gegen die der Zertifizierung zugrundeliegenden vertraglichen Verpflichtungen vorliegt.

4.7 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Durch den ZDA wird ein OCSP-Dienst zur Statusabfrage von Zertifikaten eingerichtet.

4.8 Schlüssel hinterlegung und –wiederherstellung

Eine Hinterlegung oder Sicherungsarchivierung privater Schlüssel der Zertifikate erfolgt nicht.

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMÄßNAHMEN

5.1 Archivierung

Die DKTIG und der ZDA stellt eine ordnungsgemäße Archivierung der Antragsunterlagen sicher.

Alle infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen, die der Zertifizierung, Verwaltung des Schlüsselmanagements sowie der Archivierung dienen, werden im Sicherheitskonzept des ZDA detailliert beschrieben.

6 PROFILE FÜR ZERTIFIKATE, SPERRLISTEN UND ONLINE-STATUSABFRAGEN

6.1 Zertifikatsprofil

Die optionalen Attribute title, givenName und surname im subject werden im Krankenhaussektor nicht verwendet und dürfen nicht in eine SMC Typ B eingebracht werden.

Die optionalen Attribute streetAddress, postalCode, localityName und stateOrProvinceName im subject müssen in jede SMC Typ B eingebracht werden.

Das Attribut serialNumber im subject (auch subject-serialNumber, kurz ssN genannt) muss im Krankenhaussektor bei der Zertifikatserstellung verwendet werden. Im Attribut subject-serialNumber muss das Institutskennzeichen des Krankenhauses gespeichert werden, für das die Zertifikate bestimmt sind.

Das Attribut BasicConstraints muss verwendet werden. Nach dieser Policy dürfen nur End-Entity-Zertifikate erstellt werden.

Die OID für den Zertifikatstyp, die OID für die Certificate Policy der gematik-TSL und die OID dieser Certificate Policy müssen in die Zertifikate eingebracht werden.

Die Bezeichnung und die OID für den Institutionstyp müssen in die Zertifikate eingebracht werden. Die OID für den Institutionstyp mit der Bezeichnung Krankenhaus ist 1.2.276.0.76.4.53.

Die Telematik-ID des Krankenhauses, auch Organisations-ID genannt, muss im vorgesehenen Attribut gespeichert werden. Telematik-ID im Krankenhaussektor beginnen mit dem Präfix 5, gefolgt vom Separator „-“ und dem sektorspezifisch definierten Fortsatz.

Der Telematik-ID Fortsatz für Zertifikate, die nach dieser Policy erzeugt werden, beginnt mit der Ziffer 1. Auf die erste Ziffer des Fortsatzes folgt ein eindeutiger, zweistelliger, alphanumerischer Identifikator für den ZDA, der die Telematik-ID vergeben hat. Die DKTIG vergibt die Identifikatoren und erstellt weitere Vorgaben für ZDAs zur Sicherstellung der Eindeutigkeit von Telematik-IDs, die mit „5-1“ beginnen.

Bestätigte Eigenschaften in den X.509-Zertifikaten der SMC Typ B sind nach dieser Policy im X.509-subject die Inhalte der Attribute commonName, streetAddress, postalCode, localityName, stateOrProvinceName, organisationName, countryName und (subject)serialNumber, in den extensions die Telematik-ID und im CV-Zertifikat die CHA.

Attribute oder Anwendungen, die in den Spezifikationen der gematik nicht vorgesehen sind, dürfen nach dieser Policy nicht in die Zertifikate der SMC Typ B eingebracht werden.

7 ANDERE GESCHÄFTLICHE UND RECHTLICHE ANGELEGENHEITEN

7.1 Verpflichtungen

7.1.1 Verpflichtungen der Zertifizierungsstellen

ZDA sind verpflichtet, ihre Zertifizierungsdienstleistungen gemäß dieser Certificate Policy (CP) zu erbringen.

Der ZDA beschreibt die Umsetzung der Verpflichtungen aus dieser Policy in einem Certificate Practice Statement (CPS).

Die Umsetzung der Verpflichtungen aus dieser Policy wird durch eine Aufnahme der OID dieser Policy in die Endnutzerzertifikate der SMC Typ B bestätigt.

Der ZDA identifiziert den Antragsteller im Rahmen der Übergabe der SMC Typ B gemäß [SigG].

Auf begründetes Verlangen eines zum Widerruf oder zur Suspendierung Berechtigten sperrt der ZDA die X.509-Zertifikate der SMC Typ B unverzüglich.

Wird dem ZDA ein Sperrgrund bekannt, sperrt er selbst unverzüglich die X.509-Zertifikate der betroffenen SMC Typ B. Der ZDA hat die Chipkarte nach Möglichkeit einzuziehen oder den Zertifikatsinhaber auffordern, die Chipkarte gesichert zu entsorgen.

Der ZDA informiert den Zertifikatsinhaber und den SMC-Herausgeber unverzüglich über die Sperrung der X.509-Zertifikate einer SMC Typ B und den Sperrgrund.

Für die Sperrung von X.509-Zertifikaten betreibt der ZDA OCSP-Responder.

7.1.2 Verpflichtungen des SMC-Herausgebers

Die DKTIG als SMC-Herausgeber erbringt ihre Dienstleistungen gemäß dieser Certificate Policy (CP). Dabei sind die Festlegungen der gematik in der jeweils gültigen Version zu beachten.

Die DKTIG erstellt mit den zur Erstellung von CV-Zertifikaten qualifizierten und von der Bundesnetzagentur akkreditierten ZDA ein Notfallkonzept, ein Betriebskonzept und ein Sicherheitskonzept nach den Vorgaben dieser Policy und den Vorgaben der gematik. Der ZDA gibt die vorgeschriebene Selbsterklärung gegenüber der gematik ab und wird durch diese registriert.

Für die Erstellung von Zertifikaten nach dieser Policy bedient sich die DKTIG akkreditierter ZDA, die von der DKTIG für die Erstellung von CV-Zertifikaten für den Krankenhaussektor qualifiziert werden.

Die DKTIG übersendet die geprüften Zertifikatsanträge an den ZDA, der die beantragten Zertifikate erstellt.

Die DKTIG muss belegen können, an welchen Antragsteller welche Chipkarte ausgegeben wurde. Zu einer ausgegebenen ICCSN muss die DKTIG nach Aufforderung

durch einen Zertifikats-Sperrberechtigten den Karteninhaber benennen. Die DKTIG kann diese Pflicht an den ZDA übertragen.

Die DKTIG muss belegen können, für welchen Antragsteller welche Telematik-ID vergeben wurde. Die eindeutige Zuordnung jeder Telematik-ID zu ausschließlich einem Krankenhaus ist sicherzustellen. Die DKTIG kann diese Verpflichtung an den ZDA übertragen.

Das Krankenhaus als Zertifikatsinhaber muss Folgekarten mit unveränderter Telematik-ID erhalten können. Bei einer Übertragung der Verwaltung der Telematik-ID an den ZDA ist vertraglich sicherzustellen, dass der Zertifikatsinhaber Folgekarten mit unveränderter Telematik-ID von allen im Krankenhaussektor zur Ausgabe von SMC-Typ-B berechtigten ZDA erhalten kann.

Eine Kopie des CPS wird der DKG als Policy-Herausgeber nach der Erstellung und jeder Änderung des CPS zur Verfügung gestellt.

Wird der DKTIG ein Sperrgrund bekannt, ist der ZDA darüber unverzüglich in Kenntnis zu setzen.

7.1.3 Verpflichtungen des Krankenhauses als Zertifikatsinhaber

Der Antragsteller verpflichtet das Krankenhaus als Zertifikatsinhaber im Rahmen seiner Vertretungsmacht zur Umsetzung der in dieser Policy aufgeführten Anforderungen und versichert die Umsetzung dieser Anforderungen mit seiner Unterschrift.

Das Krankenhaus als Zertifikatsinhaber stellt unabhängig von Wechseln in der natürlichen Person des gesetzlichen Vertreters sicher, dass die Verwendung der SMC Typ B im Rahmen des rechtlich Zulässigen erfolgt.

Die interne Wahrnehmung von Verpflichtungen des Krankenhauses als Zertifikatsinhaber durch andere natürliche Personen als den gesetzlichen Vertreter des Krankenhauses ist zu dokumentieren und auf Verlangen der DKTIG zu belegen. Die Verantwortung des gesetzlichen Vertreters des Krankenhauses für die SMC Typ B bleibt von einer internen Delegation unberührt.

Wird dem gesetzlichen Vertreter des Krankenhauses ein Sperrgrund bekannt, ist der ZDA darüber unverzüglich in Kenntnis zu setzen.

Der gesetzliche Vertreter des Krankenhauses hat die SMC Typ B auf Verlangen der DKTIG oder des ZDA zurückzugeben bzw. gesichert zu entsorgen, sofern ein Sperrgrund vorliegt.

7.2 Gewährleistungen

Sowohl die DKTIG als auch der Zertifizierungsdiensteanbieter (ZDA) bieten alle Dienstleistungen mit der gesetzlichen Pflicht zur Gewährleistung an.

7.3 Haftungsbeschränkung und – freistellung

Die DKTIG und der ZDA haften gemäß den gesetzlichen Bestimmungen sowie den entsprechenden Allgemeinen Geschäftsbedingungen.

Die Verwendung der privaten Schlüssel obliegt ausschließlich dem jeweiligen Zertifikatsinhaber. Dieser haftet allein für alle aus einer rechts- oder vertragswidrigen Verwendung der Schlüssel resultierenden Schäden und stellt die DKTIG und den ZDA von eventuellen Ansprüchen Dritter unverzüglich frei.

7.4 Änderungen der Richtlinie

7.4.1 Vorgehen bei Änderungen

Geänderte Versionen dieser Policy übermittelt die DKG als Policy-Herausgeber der DKTIG als SMC-Herausgeber.

7.4.2 Änderungen des Richtlinienbezeichners (OID)

Jede neue Version dieser Policy erhält von der DKG als Policy-Herausgeber eine neue OID.

8 REFERENZVERZEICHNIS

Die Festlegungen der gematik sind in der jeweils gültigen Version zu beachten:

gemSpec_TLK Spezifikation für Testlaborkarten (eGK, HBA, SMC) Version 2.0.0, Stand 15.05.2007

gemSpec_MK Spezifikation für Musterkarten und Testkarten (eGK, HBA, SMC) Version 2.7.1, Stand 22.08.2008

gemX.509-SMCB Festlegung zu den X.509-Zertifikaten der SMC Typ B Version 1.4.0, Stand 27.06.2008

gemSpec_SMC_OPT Gemeinsame optische Merkmale der SMC Version 1.0.0, Stand 22.08.2008

German Health Professional Card and Security Module Card, Part 1: Commands, Algorithms and Functions of the COS Platform Version 2.3.0, Stand 04.07.2008

German Health Professional Card and Security Module Card, Part 2: HPC Applications and Functions, Version 2.3.0, Stand 04.07.2008

German Health Professional Card and Security Module Card, Part 3: SMC Applications and Functions Version 2.3.0, Stand 04.07.2008

gemX.509_TSP PKI für X.509-Zertifikate Registrierung eines Trust Service Provider (TSP) Version 1.2.0, Stand 19.03.2008

gemTSL-SP_CP Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten Version 1.3.0, Stand 16.06.2008

gemSpec_TID Spezifikation des Aufbaus der Telematik-ID für HBA und SMC Version 1.0.0, Stand 22.08.2008

gemFK_X.509 PKI für die X.509-Zertifikate Grobkonzept Version 1.3.0, Stand 18.06.2008

gemPKI_CVCGK PKI für CV-Zertifikate Grobkonzept Version 1.5.0, Stand 16.06.2008

gemPKI_Reg PKI für CV-Zertifikate Registrierung einer CVC-CA der zweiten Ebene Version 1.7.0, Stand 27.06.2008

gemPKI_VerzD Verzeichnisdienstkonzept der gematik-Bridge-CA Version 1.2.0, Stand 15.07.2008

gemPKI_Mon PKI für das System und Service Level Monitoring – Lastenheft Version 1.2.0, Stand 30.06.2008

gemX.509-TSL Festlegungen einer einheitlichen X.509-Zertifikatsinfrastruktur für die Telematik im Gesundheitswesen Version 1.0.0, Stand 12.12.2005

gemVerw_Zert_TI Verwendung von Zertifikaten in der Telematikinfrastruktur Version
1.2.0, Stand 16.07.2008

gemSiKo Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version
2.4.0, Stand 05.09.2008

SigG Gesetz über Rahmenbedingungen für elektronische Signaturen und zur
Änderung weiterer Vorschriften vom 16. Mai 2001