Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Certificate Policy

Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL

Sektorspezifische Präzisierung für SMC-B-Zertifikate in Erprobungsphase ORS1

Version:	1.2.0
Revision:	\main\rel_online\rel_ors1\7
Stand:	17.06.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemRL_SMC-B_ORS1]

Dokumenteninformationen

Dieses Dokument wird geführt unter dem Titel:

Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL – Sektorspezifische Präzisierung für SMC-B-Zertifikate in Erprobungsphase ORS1

Object Identifier (OID) dieser Version des Dokumentes:

1.2.276.0.76.4.170

Soll die OID in anderen Dokumenten versionsunabhängig referenziert werden, so ist die Kennung <oid_policy_gem_or_cp_smcb_erprobung> zu verwenden. Die Ermittlung der relevanten OID ist dann über das Dokument [gemSpec_OID] möglich.

Änderungen zur Vorversion

Kontaktdaten auf KBV geändert (Kap. 1.4.2.1 und 1.4.2.3)

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Ersterstellung	P77
	27.05.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare	P77
1.0.0 RC	19.06.13		zur Freigabe empfohlen	PL P77
			Einarbeitung Kommentare	P77
1.0.0	04.07.13		freigegeben	gematik
1.0.1	08.08.13		Einarbeitung gemäß Änderungsliste	PL P77
1.1.0	15.08.13		freigegeben	gematik
			Kontaktdaten auf KBV ändern	P77
1.2.0	17.06.14		freigegeben	gematik

Inhaltsverzeichnis

Dokumenteninformationen **2**

Inhaltsverzeichnis **3**

1 Einordnung des Dokumentes **6**

1.1 Überblick 6
1.2 Teilnehmer der Zertifizierungsinfrastruktur (PKI) 6
1.2.1 Zertifizierungsstellen, Trust Service Provider (TSP) 7
1.2.2 Registrierungsstellen 7
1.2.3 Zertifikatsnehmer (Subscribers) 8
1.2.4 Zertifikatsprüfer (Relying Parties) 8
1.2.5 Attributbestätigende Stellen / SMC-B-Herausgeber 8
1.2.6 Praxisregister für Ärzte und Psychotherapeuten 8
1.2.7 Weitere Teilnehmer 8
1.3 Anwendungs- und Geltungsbereich 9
1.3.1 Geeignete Zertifikatsnutzung 9
1.3.2 Untersagte Zertifikatsnutzung 9
1.4 Verwaltung der Zertifizierungsrichtlinie 9
1.4.1 Änderungsmanagement 9
1.4.2 Ansprechpartner 9
1.4.3 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie 10
1.4.4 Verfahren zur Anerkennung von Regelungen für den Zertifizierungsbetrieb (CPS) 11
1.5 Definitionen und Abkürzunge 11
1.5.1 SMC-B 11
1.5.2 Online-Rollout Stufe 1 (ORS1) 11
1.5.3 Erprobungsphase 11
1.5.4 Karteninhaber / Zertifikatsinhaber (Inhaber) 11
1.5.5 Attributbestätigende Stelle und Zertifikatsherausgeber 12

2 Veröffentlichungen und Verzeichnisdienst **13**

2.1 Verzeichnisdienste 13
2.2 Veröffentlichung von Zertifizierungsinformationen 13
2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz) 13
2.4 Zugangskontrolle zu Verzeichnisdiensten 13

3 Identifizierung und Authentifizierung **14**

3.1 Namen 14
3.1.1 Namensformen 14
3.1.2 Aussagekraft von Namen 14
3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber 14

3.1.4 Regeln zur Interpretation verschiedener Namensformen 14
3.1.5 Eindeutigkeit von Namen 14
3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen 14
3.2 Identitätsüberprüfung bei Neuantrag 14
3.2.1 Nachweis des Besitzes des privaten Schlüssels 14
3.2.2 Authentifizierung einer Organisation 15
3.2.3 Authentifizierung natürlicher Personen 15
3.2.4 Nicht überprüfte Teilnehmerangaben 15
3.2.5 Überprüfung der Berechtigung 15
3.2.6 Kriterien für Zusammenarbeit 15
3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung (SMC-B-Folgekarte) 15
3.3.1 Routinemäßige Zertifikatserneuerung 15
3.3.2 Zertifikatserneuerung nach einer Sperrung 15
3.4 Identifizierung und Authentifizierung von Sperranträgen 15

4 Ablauforganisation (Certificate Lifecycle) 16

4.1 Zertifikatsantrag 16
4.1.1 Wer kann ein SMC-B Zertifikat beantragen? 17
4.1.2 Verfahren und Verantwortungen 19
4.2 Bearbeitung von Zertifikatsanträgen 25
4.2.1 Sektorspezifische Festlegungen zu Antragsdaten 25
4.2.2 Durchführung von Identifikation und Authentifizierung 26
4.2.3 Annahme oder Ablehnung von Zertifikatsanträgen 26
4.2.4 Bearbeitungsdauer bei Zertifikatsanträgen 27
4.3 Zertifikatserstellung 27
4.3.1 Aufgaben der Zertifizierungsstelle 27
4.3.2 Benachrichtigung des Antragstellers 27
4.4 Zertifikatsakzeptanz 27
4.4.1 Annahme des Zertifikats 27
4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle 27
4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle 27
4.5 Verwendung des Schlüsselpaares und des Zertifikats 28
4.5.1 Nutzung durch den Zertifikatsinhaber 28
4.5.2 Nutzung des Zertifikats durch die Relying Party 29
4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung) 29
4.7 Schlüssel- und Zertifikatserneuerung (Re-key) 29
4.8 Zertifikatsmodifizierung 29
4.9 Widerruf / Sperrung und Suspendierung von Zertifikaten 29
4.9.1 Gründe für Widerruf / Sperrung 29
4.9.2 Wer kann Widerruf / Sperrung beantragen 29
4.9.3 Ablauf von Widerruf / Sperrung 31
4.9.4 Fristen für den Zertifikatsinhaber 31
4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle 31
4.9.6 Anforderung zu Sperrprüfungen durch eine Relying Party 31
4.9.7 Häufigkeit der Sperrlistenveröffentlichung 31
4.9.8 Maximale Latenzzeit für Sperrlisten 31
4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP) 31
4.9.10 Anforderungen an Online-Statusabfragen (OCSP) 31

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung 31
4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln 32
4.9.13 Gründe für eine Suspendierung 32
4.9.14 Wer kann Suspendierung beantragen 32
4.9.15 Ablauf einer Suspendierung 32
4.9.16 Maximale Sperrdauer bei Suspendierung 32
4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP) 32
4.11 Beendigung des Vertragsverhältnisses 32
4.12 Schlüsselhinterlegung und –wiederherstellung (Key Escrow und Recovery) ... 32

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen 33

6 Technische Sicherheitsmaßnahmen 34

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen 35

7.1 Zertifikatsprofil 35
7.1.1 Versionsnummer 35
7.1.2 Zertifikatserweiterungen 35
7.1.3 Algorithmus Bezeichner (OID) 35
7.1.4 Namensformen 35
7.1.5 Namensbeschränkungen 35
7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID) 35
7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints) 36
7.1.8 Syntax und Semantik von Policy Qualifiern 36
7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies) 36
7.2 Sperrlistenprofil 36
7.2.1 Versionsnummer 36
7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen 36
7.3 OCSP-Profil 36
7.3.1 Versionsnummer 36
7.3.2 OCSP-Erweiterungen 36

8 Konformitätsprüfung (Compliance Audit, Assessments) 37

9 Andere geschäftliche und rechtliche Angelegenheiten 38

10 Informationen zum Dokument 39

Anhang A - Verzeichnisse 40

A1- Abkürzungen 40
A2 – Glossar 40
A3 – Abbildungsverzeichnis 41
A4 – Tabellenverzeichnis 41
A5 - Referenzierte Dokumente 41

1 Einordnung des Dokumentes

1.1 Überblick

Das vorliegende Dokument beschreibt die Regelungen zur Beantragung, Herausgabe und Verwendung von SMC-B-Zertifikaten während der Erprobungsphase „Online-Rollout (Stufe 1)“ zur Einführung der Gesundheitskarte.

Die hierin getroffenen Regelungen bilden widerspruchsfrei zur „Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL“[1] als sektorspezifische Präzisierung diejenigen Sachverhalte ab, die für Vergabe- und Auftragserteilung in ORS1 relevant sind.

Es werden die übergreifenden Regelungen beschrieben, wie sie für alle Teilnehmer der Telematikinfrastruktur einheitlich gelten. Der Geltungsbereich umfasst die TSP, die der gematik Root-CA nachgeordnet sind (TSP-X.509 nonQES). Sowie auch den TSP, der CV-Zertifikate für die Ausstattung der SMC-B herausgibt.

In Tabellen oder Unterkapiteln (4. Gliederungsebene) sind jeweils sektorspezifische Ausprägungen der Policy, hinsichtlich technischer Attribute in den Zertifikatsprofilen wie auch hinsichtlich spezifischer Prozessabläufe und Verantwortlichkeiten des jeweiligen Sektors, aufgeführt.

Sofern in dieser Richtlinie Anforderungen an einzelne Sicherheitsmaßnahmen nicht spezifiziert werden und nicht durch andere normative Dokumente der gematik gefordert werden, sind diese mindestens an die entsprechenden Maßnahmenkataloge des [BSI_2005] oder international vergleichbarer Rahmenwerke wie [ISO17799] und [ISO27001] anzulehnen.

Hinweis-1:
Der Begriff „Arzt“ umfasst im Dokument explizit nur Ärzte und keine Zahnärzte.

Hinweis-2:
Die Erprobung in der Projektphase ORS1 berücksichtigt keine privat abrechnenden Ärzte. Die Erwähnung in diesem Dokument erfolgt lediglich der Vollständigkeit halber.

1.2 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

Die Definition und Abgrenzung der Teilnehmer in der PKI der TI erfolgt im Rahmen von [gemKPT_PKI_TIP#2.7.1], [gemSpec_PKI#8.1]. In diesem Dokument erfolgt eine kurze Darstellung der in ORS1 relevanten Teilnehmer.

[1] [gemRL_TSL_TSP_CP]

1.2.1 Zertifizierungsstellen, Trust Service Provider (TSP)

Trust Service Provider (TSP) stellen für den Einsatz in der Telematikinfrastruktur X.509- und CV-Zertifikate für natürliche und juristische Personen (medizinische Institutionen) aus sowie für zentrale Dienste, fachanwendungsspezifische Dienste und technische Komponenten. Neben anderen Aufgaben sind TSP somit immer auch Zertifikatsherausgeber.

Als TSP in der TI sind definiert[2]:

(1) gematik Root-CA

(2) CVC-Root-CA

(3) TSP-X.509 QES (auch als ZDA bezeichnet)

(4) TSP-X.509 nonQES

(5) TSP-CVC

Für die Herausgabe der SMC-B sind die TSP (4) und (5) relevant, so dass in der weiteren Darstellung nur diese berücksichtigt werden.

1.2.2 Registrierungsstellen

Die Registrierungsstellen sind den TSP zuzuordnen und decken folgende Aufgabenbereiche ab:

(1) Identifizierung der Zertifikatsantragsteller

(2) Erfassung und Prüfung der Antragsdaten

(3) Einholung von Attribut und Produktionsfreigabe durch die attributbestätigende Stelle (Standesorganisation der Leistungserbringer, Kostenträgerorganisation)

(4) Übermittlung der Daten an den Erstellungsdienst des TSP

(5) Entgegennahme und Prüfung von Empfangsbestätigungen für die SMC-B

(6) Veranlassung der „Freischaltung“ von Zertifikaten (Einstellung der Statusinformationen in den OCSP-Dienst des TSP)

(7) Archivierung der Antragsdaten

(8) Annahme, Prüfung und Umsetzung von Sperraufträgen

(9) Betreiben einer Kundenschnittstelle für Anfragen und Sperraufträge

Registrierungsstellen bilden die Kundenschnittstelle einer PKI zu den Zertifikatsnehmern.

[2] [gemKPT_Arch_TIP]

1.2.3 Zertifikatsnehmer (Subscribers)

Der Zertifikatsnehmer einer SMC-B ist die medizinische Institution, die über die Zertifikate der SMC-B repräsentiert wird.

Antragsteller der SMC-B und somit der enthaltenen Zertifikate ist immer eine natürliche Person, die für die medizinische Institution vertretungs- und zeichnungsberechtigt ist.

1.2.4 Zertifikatsprüfer (Relying Parties)

Anwendungen und Dienste in der TI und im Internet können die Zertifikate der SMC-B prüfen und deren Inhalte verwenden. Hierfür stellt der TSP-X.509 nonQES die Statusauskünfte zu diesen Zertifikaten in der TI und im Internet bereit.

1.2.5 Attributbestätigende Stellen / SMC-B-Herausgeber

Die Hoheit zur Verwaltung und Vergabe der institutionsspezifischen X.509-Attribute und die Herausgabe der SMC-B obliegt den vertretungsberechtigten Organisationen der medizinischen Institutionen.

- KBV – Bestätigt die institutionsspezifischen Attribute der SMC-B für Praxen der Vertragsärzte, privat abrechnender Ärzte und der Vertragspsychotherapeuten[3]
- KZV – Bestätigt die institutionsspezifischen Attribute der SMC-B für Zahnarztpraxen
- DKTIG – Bestätigt die institutionsspezifischen Attribute der SMC-B für Krankenhäuser

Siehe auch Kap 1.5.5

1.2.6 Praxisregister für Ärzte und Psychotherapeuten

Die Herausgabe der SMC-B für Ärzte und Psychotherapeuten wird operativ über ein Verzeichnis aller Betriebsstätten sowie deren Verantwortlichen organisiert. In diesem System werden die SMC-B-Anträge, deren Bearbeitungsstatus sowie die Karten selbst verwaltet. Das so genannte Praxisregister wird als zentrale, mandantenfähige Web-Applikation betrieben. Zur Datenpflege werden eine Web-Schnittstelle sowie eine Web-Service-Schnittstelle angeboten. Für die Pflege der Daten innerhalb des Praxisregisters sind die KVen verantwortlich.

1.2.7 Weitere Teilnehmer

Keine Vorgaben in diesem Dokument

[3] Durch die KVen werden die Niederlassungen der Berufsgruppen der „Psychologischen Psychotherapeuten“ und der „Kinder- und Jugendlichenpsychotherapeuten“ vertreten. Im Dokument werden diese beiden Professionen der besseren Lesbarkeit wegen unter der Kurzbezeichnung „Psychotherapeuten“ geführt.

1.3 Anwendungs- und Geltungsbereich

Alle Beschreibungen und sektorspezifischen Präzisierungen der übergreifenden Policy gelten für den Zeitraum und die Anwendungsbereiche des ORS1.

Mit den Ergebnissen aus ORS1 werden die Policy-Dokumente je nach Bedarf aktualisiert und mit Aufnahme des TI-Produktivbetriebes in einer neuen Version publiziert.

Die während der Phase ORS1 herausgegebenen Zertifikate und Karten behalten bis zum regulären zeitlichen Ablauf ihre volle Gültigkeit.

1.3.1 Geeignete Zertifikatsnutzung

Keine Vorgaben in diesem Dokument

1.3.2 Untersagte Zertifikatsnutzung

Keine Vorgaben in diesem Dokument

1.4 Verwaltung der Zertifizierungsrichtlinie

Die übergreifenden Regelungen und Anforderungen der Telematikinfrastruktur an Anbieter, Inhaber und Zertifikatsprüfer von Zertifikaten[4] für die SMC-B gelten auch für die Erprobungsphase in ORS1. Diese Regelungen sind unter http://www.gematik.de/ abrufbar.

Die vorliegende SMC-B-Ergänzungspolicy präzisiert die o.g. Regelungen hinsichtlich spezifischer Ausgabe- und Sperrregelungen für die Teilnehmer der Erprobungsphase. Abweichungen und Ergänzungen von Regelungen der Telematikinfrastruktur können in dieser Policy definiert werden, sofern diese nicht im Widerspruch zu den Regelungen für nicht-qualifizierte Zertifikate der Telematikinfrastruktur stehen.

1.4.1 Änderungsmanagement

Änderungen des Dokuments erfolgen über die gematik als gesamtbetriebsverantwortliche Instanz der TI.

Änderungen der sektorspezifischen Ausprägungen erfolgen durch die jeweiligen Sektoren. Diese Änderungen werden nach Prüfung auf Widerspruchsfreiheit zur übergeordneten Policy durch die gematik in dieses Dokument eingepflegt, und dieses dann mit einer neuen Versionsnummer veröffentlicht.

1.4.2 Ansprechpartner

Für alle Anliegen, dieses Dokument betreffend, gilt als koordinierender Ansprechpartner:

[4] [gemRL_TSL_TSP_CP]

gematik GmbH, PKI
Friedrichstrasse 136, DE 10117 Berlin

1.4.2.1 Sektor: Institutionen der Ärzteschaft

KBV, federführend für die KVen der niedergelassenen Vertragsärzte sowie die KBV der privat abrechnenden Ärzte.

Christian Straßburg
IT-Architekt

Kassenärztliche Bundesvereinigung
Herbert-Lewin-Platz 2, 10623 Berlin
Postfach 12 02 64, 10592 Berlin

Tel: +49 511 380 36 20
E-Mail: christian.strassburg@kvn.de

1.4.2.2 Sektor: Institutionen der Vertragszahnärzteschaft

Kassenzahnärztliche Bundesvereinigung
Dipl. Informatiker Dieter Reul

Universitätsstrasse 73
50931 Köln

Tel.: 0221 4001 272
E-Mail: d.reul@kzbv.de

1.4.2.3 Sektor: Institutionen der Psychotherapeuten

KBV, federführend für die KVen der Psychologischen Psychotherapeuten sowie der Kinder- und Jugendlichenpsychotherapeuten.

s.o. Kap 1.4.2.1

1.4.2.4 Sektor: Krankenhäuser

Deutsche Krankenhausgesellschaft
Ingo Meyer, Referent

Wegelystraße 3
10623 Berlin

Telefon: +49 (30) 39801-1324
E-Mail: I.Meyer@dkgev.de

1.4.3 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie

Keine Vorgaben in diesem Dokument

1.4.4 Verfahren zur Anerkennung von Regelungen für den Zertifizierungsbetrieb (CPS)

Keine Vorgaben in diesem Dokument

1.5 Definitionen und Abkürzunge

1.5.1 SMC-B

Die SMC-B (Security Module Card Typ B) ist eine PIN-geschützte Smartcard zur sicheren Speicherung und Verwendung von kryptographischen Schlüsseln und X.509-Zertifikaten, die einer medizinischen Institution (z. B. Praxis, Apotheke, Krankenhaus) des Gesundheitswesens eindeutig zugeordnet werden können.

Die SMC-B dient z. B. als Ausweis der Organisation gegenüber der elektronischen Gesundheitskarte sowie anderen Komponenten und Anwendungen der TI.

Tabelle 1: Tab_PKI_960 Sektorinterne Alternativbezeichnung der SMC-B

Sektor	Sektorinterne Bezeichnung / Alternativbezeichnung der SMC-B
Vertragsärzte, Vertragspsychotherapeuten	Institutionsausweis
Zahnärzteschaft	Praxisausweis
Krankenhäuser	SMC-B

1.5.2 Online-Rollout Stufe 1 (ORS1)

ORS1 ist eine definierte Phase zur Einführung der Telematikinfrastruktur, in der Aufbau, Test und Erprobungsbetrieb der dezentralen und der zentralen Produkte der TI erfolgen.

1.5.3 Erprobungsphase

Die Erprobung ist ein Teil der Einführungsphase der Telematikinfrastruktur (TI) mit eingeschränkter Teilnehmerzahl. Ziel dieser Phase ist die Betriebseignung aller Elemente der TI unter realen Bedingungen zu prüfen, so dass Betriebsprobleme bereits vor der Aufnahme des Wirkbetriebs im Vollausbau entdeckt und behoben werden können.

Die Erprobungsphase erfolgt in der Wirkbetriebs-, Test- und Referenzumgebung der TI mit echten Smartcards (eGK, HBA, SMC-B, gSMC-x) und Echtdaten für Versicherte und Leistungserbringer.

1.5.4 Karteninhaber / Zertifikatsinhaber (Inhaber)

Karten- und Zertifikatsinhaber kann sowohl eine Einzelperson als Betreiber einer medizinischen Institution (Praxis) sein, wie auch eine juristische Person (Gemeinschaftspraxis, Klinik) jeweils mit standesrechtlicher Zulassung sein. Im Falle

einer juristischen Person muss die Beantragung durch eine nachgewiesen vertretungs- und zeichnungsberechtigte natürliche Person erfolgen. Der Karteninhaber ist verantwortlich für die ordnungs- und vertragsgemäße Nutzung der jeweiligen SMC-B.

Die Begriffe Karteninhaber und Zertifikatsinhaber sind in diesem Dokument gleichgesetzt.

1.5.5 Attributbestätigende Stelle und Zertifikatsherausgeber

Die X.509-Zertifikate der SMC-B enthalten eine definierte Beschreibung der beantragenden medizinischen Institution im Zertifikatsattribut „Profession Item“. Die Eintragung dieses Attributes muss durch eine zuständige Standesorganisation in jedem Einzelfall geprüft und genehmigt werden.

Tabelle 2: Tab_PKI_961 Übersicht der Attributbestätigenden Stellen / SMC-B-Herausgeber

Sektor	Attributbestätigende Stelle / SMC-B-Herausgeber
Niedergelassene Vertragsärzte Vertragspsychotherapeuten Psychologische Psychotherapeuten Kinder- und Jugendlichen-psychotherapeuten	Kassenärztliche Vereinigung (KV dezentral)
Vertragszahnärzte	Kassenzahnärztliche Vereinigung (KZV dezentral)
Nicht-Vertragsärzte (privat abrechnende Ärzte) und Psychotherapeuten)	Kassenärztliche Bundesvereinigung (KBV zentral)
Krankenhaus	Deutsche Krankenhaus TrustCenter und Informations-verarbeitung GmbH (DKTIG zentral)

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienste

Keine Vorgaben in diesem Dokument

2.2 Veröffentlichung von Zertifizierungsinformationen

Keine Vorgaben in diesem Dokument

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Keine Vorgaben in diesem Dokument

2.4 Zugangskontrolle zu Verzeichnisdiensten

Keine Vorgaben in diesem Dokument

3 Identifizierung und Authentifizierung

3.1 Namen

Siehe [gemRL_TSL_SP_CP#4.1]

3.1.1 Namensformen

Siehe [gemRL_TSL_SP_CP#4.1.2]

3.1.2 Aussagekraft von Namen

Siehe [gemRL_TSL_SP_CP#4.1.3]

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Keine Vorgaben in diesem Dokument

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Vorgaben in diesem Dokument

3.1.5 Eindeutigkeit von Namen

Keine Vorgaben in diesem Dokument

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Keine Vorgaben in diesem Dokument

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Die Zustellung der SMC-B erfolgt über das PostIdent-Verfahren (oder ein sicherheitstechnisch gleichwertiges Verfahren) an den im Antrag ausgewiesenen Empfangsberechtigten der medizinischen Institution. Durch die damit verbundene, persönlich unterzeichnete Empfangsbestätigung für die Karte wird der Nachweis über den Besitz der Privaten Schlüssel der SMC-B erbracht und an die Herausgeberorganisation übermittelt.

3.2.2 Authentifizierung einer Organisation

Keine Vorgaben in diesem Dokument

3.2.3 Authentifizierung natürlicher Personen

Keine Vorgaben in diesem Dokument

3.2.4 Nicht überprüfte Teilnehmerangaben

Keine Vorgaben in diesem Dokument

3.2.5 Überprüfung der Berechtigung

Die Überprüfung der Berechtigung einer medizinischen Institution zum Erhalt und zur Verwendung einer SMC-B wird durch die jeweils zuständige Vereinigung dieser Institutionen durchgeführt.

Die Überprüfung der Berechtigung einer natürlichen Person zur Beantragung einer SMC-B namens und im Auftrag einer medizinischen Institution, wird durch die jeweils zuständige Vereinigung dieser Institutionen durchgeführt. Die Person muss dort als vertretungsberechtigt eingetragen sein.

3.2.6 Kriterien für Zusammenarbeit

Keine Vorgaben in diesem Dokument

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung (SMC-B-Folgekarte)

Keine Vorgaben in diesem Dokument, da nicht Gegenstand von ORS1

3.3.1 Routinemäßige Zertifikatserneuerung

Keine Vorgaben in diesem Dokument

3.3.2 Zertifikatserneuerung nach einer Sperrung

Keine Vorgaben in diesem Dokument

3.4 Identifizierung und Authentifizierung von Sperranträgen

Keine Vorgaben in diesem Dokument

4 Ablauforganisation (Certificate Lifecycle)

4.1 Zertifikatsantrag

Beschrieben werden diejenigen Daten und Abläufe, die bei der Antragstellung vom Antragsteller eingegeben werden müssen und von der zuständigen Stelle im Rahmen der Attributbestätigung benötigt werden.

Nicht berücksichtigt sind demnach solche Daten, die ausschließlich zur Auftragsabwicklung benötigt werden (z. B. "Bankverbindung").

Tabelle 3: Tab_ PKI_962 Erforderliche Antragsdaten

	KZV	KV, KBV	DKTIG
Antrag			
Art des Antrags	Auswahl: Erstantrag Folgeantrag	Auswahl: Erstantrag Folgeantrag Löschantrag	
Antragsteller			
Name	Name (optional: Titel)		
Vorname	Vorname(n)		
Geburtsdatum	Datum		
Meldeanschrift	Strasse Hausnummer Postleitzahl Ort		
Legitimationsnachweis	- - -	- Vorlage amtl. Lichtbildausweis - Nachweis der Approbation	
Medizinische Institution			
Name	Name (optional: Namenszusatz)		
Rechtsform	- - -	Auswahl: Einzelgesellschaft GmbH	

	KZV	KV, KBV	DKTIG
		AG Sonstige …	
Organisationsform der medizinischen Institution	Auswahl: Einzelpraxis BAG ÜBAG KÜBAG MVZ		
Namen aller Gesellschafter (bei Nicht-Ein-Personen-Praxen)	Name(n) (optional: Titel)		
Zuständige Stelle	Auswahl: Zuständige KZV		
Institutionsnummer bei der zuständigen Stelle	Nummer		
Abrechnungsnummer bei der zuständigen Stelle	Nummer		
Anschrift	Strasse Hausnummer Postleitzahl Ort		
Lieferanschrift (falls abweichend; optional)	Strasse Hausnummer Postleitzahl Ort		
E-Mail-Adresse	E-Mail-Adresse gem. RFC-822		

4.1.1 Wer kann ein SMC-B Zertifikat beantragen?

Antragsberechtigt sind Institutionen (juristische Personen) des Gesundheitswesens, vertreten durch nachgewiesen vertretungs- / zeichnungsberechtigte natürliche Personen.

Die Berechtigung der Institution zur Teilnahme an der TI wird dieser zugewiesen durch die Bestätigung eines qualifizierenden Rollenattributs (z. B. „Arztpraxis“, „Zahnarztpraxis“, „Krankenhaus“ o. ä.) einer anerkannten Standesorganisation.[5]

[5] [gemSpec_PKI], Kap 6.3, GS-A_4621 und Tab_PKI_254

Antragsberechtigt in diesem Sinne sind die Institutionen gemäß

- [gemSpec_OID#3.5.1]

Sektorübergreifend übernimmt der Antragsteller mit der Beantragung einer SMC-B im folgende Aufgaben und Verpflichtungen:

Im Zuge der Beantragung bestätigt der Antragsteller, dass

- die erforderlichen Angaben vollständig und korrekt gemacht wurden,
- die Verantwortung für den Schutz der privaten Schlüssel vor Missbrauch durch Unbefugte übernommen wird,
- die Passwörter (PINs) zum Schutz der privaten Schlüssel nur Nutzungsberechtigten bekannt gegeben werden,
- bei Preisgabe oder Verdacht der Preisgabe einer PIN an nicht nutzungsberechtigte Personen diese unverzüglich geändert wird und
- bei Kompromittierung oder Verlust eines privaten Schlüssels unverzüglich die Sperrung des zugehörigen Zertifikates veranlasst wird,
- bekannt ist, dass die zuständige Standesorganisation sperrberechtigt ist.

Im Zuge der Beantragung erklärt der Antragsteller im Namen der antragstellenden Institution das Einverständnis

- mit der Weiterleitung aller zur Identifizierung und Attributvergabe erforderlichen Daten sowie der X.509-Zertifikate an die zuständige Standesorganisation
- zur Nutzung der X.509-Zertifikate durch die zuständige Standesorganisation
- zur Veröffentlichung der Zertifikate in öffentlichen Verzeichnisdiensten auch außerhalb der Telematikinfrastruktur (optional)

4.1.1.1 Sektor: Institutionen der Ärzteschaft

- Niedergelassene Vertragsärzte sind berechtigt zur Beantragung einer SMC-B bei der zuständigen KV
- Privat abrechnende niedergelassene Ärzte sind berechtigt zur Beantragung einer SMC-B bei der KBV.
- Die SMC-B eines in eigener Praxis eigenverantwortlich tätigen Vertragsarztes repräsentiert die entsprechende Praxis. Karteninhaber ist der Vertragsarzt.
- Im Falle einer Praxisgemeinschaft mit vertragsärztlicher Tätigkeit durch mehrere Ärzte repräsentiert die SMC-B die gemeinschaftlich betriebene Praxis. Karteninhaber ist die Praxisgemeinschaft.

4.1.1.2 Sektor: Vertragszahnärzteschaft

- Nur Vertragszahnärzte sind berechtigt zur Antragstellung einer SMC-B.
- Antragsteller der SMC-B für Vertragszahnärzte ist eine natürliche Person.
- Die SMC-B eines in eigener Praxis eigenverantwortlich tätigen Vertragszahnarztes repräsentiert die entsprechende Praxis. Karteninhaber ist der Vertragszahnarzt.
- Im Falle einer gemeinsamen Ausübung der vertragszahnärztlichen Tätigkeit (ÜBAG/BAG) repräsentiert die SMC-B für Vertragszahnärzte die gemeinschaftlich betriebene Praxis. Jeder in einer (Ü)BAG als Vertragszahnarzt tätige Zahnarzt ist zur Antragstellung berechtigt. Karteninhaber ist die vertragszahnärztliche BAG in ihrer Gesamtheit.
- Für Praxisgemeinschaften gelten hinsichtlich der SMC-B die Regelungen für Einzelpraxen.
- Im Fall eines von einer KZV zugelassenen MVZ repräsentiert die SMC-B das MVZ. Antragsberechtigt ist eine vertretungsberechtigte natürliche Person des MVZ. Karteninhaber ist somit das MVZ als juristische Person; handelt es sich um eine Personengesellschaft, gelten die Festlegungen zur BAG/ÜBAG entsprechend.

4.1.1.3 Sektor: Institutionen der Psychotherapeuten

Es gelten die Regelungen für Ärzte analog; siehe Kap 4.1.1.1

4.1.1.4 Sektor: Krankenhäuser

Keine Vorgaben in diesem Dokument.

4.1.2 Verfahren und Verantwortungen

4.1.2.1 Generisches Antragsverfahren SMC-B

Der Antragsprozess realisiert folgenden Ablauf (siehe auch Abb. 1):

(1) Antragstellung wird durch den Antragsteller im SMC-B-Antragsportal des TSP gestartet (ggf. Vorbefüllung des Antrages durch die zuständige Stelle, d.h. den eigentlichen Herausgeber der Karte)

(2) Antragsteller füllt den elektronischen Antrag im Antragsportal aus oder vervollständigt ihn und bestätigt die Antragstellung elektronisch

(3) TSP bearbeitet die Antragsdaten

(4) TSP stellt den bearbeiteten Antrag zur Prüfung und Freigabe durch die zuständige Stelle in das Freigabeportal

(5) Zuständige Stelle gibt Anträge frei bzw. lehnt unberechtigte Anträge ab

(6) Nach Antragsfreigabe durch die zuständige Stelle erfolgt die Kartenproduktion und anschließende Kartenauslieferung an den berechtigten Empfänger durch den TSP oder beauftragte Logistiker im Auftrag des TSP.

(7) Die Auslieferung der Karte erfolgt ausschließlich an den Antragsteller der SMC-B nach dessen persönlicher Identifizierung bei der Übergabe.

(8) Der Empfang der SMC-B muss vom Antragsteller dem TSP gegenüber schriftlich bestätigt werden. Erst nach Eingang und Prüfung dieser Empfangsbestätigung werden die betreffenden Zertifikate in den OCSP-Dienst eingestellt (Freischaltung).

(9) Der PIN-Brief wird zeitlich versetzt und getrennt von der Kartenzustellung an den Antragsteller zugestellt.

(10) Nach erfolgreicher Zustellung von Karte und PIN-Brief an den berechtigten Empfänger sowie der Freischaltung der zugehörigen Zertifikate benachrichtigt der TSP die zuständige Stelle des Kartenherausgebers.

(11) Muss das Verfahren aus irgendwelchen Gründen abgebrochen werden, benachrichtigt der TSP die zuständige Stelle des Kartenherausgebers.

Hinweis: Für den auf die Erprobungsphase ORS1 folgenden Produktivbetrieb können geänderte oder zusätzliche Anforderungen der zuständigen Stellen an das Antragsverfahren definiert werden.

Auf der Folgeseite ist der generische Prozess vom Antrag bis zur Empfangsbestätigung an die zuständige Stelle in einer Grafik dargestellt.

HINWEIS: In der Grafik auf der Folgeseite ist die technische Instanz des Praxisregisters als Schnittstelle zwischen den herausgebenden ärztlichen Organisationen und den TSP bzw. ZDA nicht explizit ausgewiesen, da hierdurch keine Verschiebung der Verantwortlichkeiten verbunden ist.

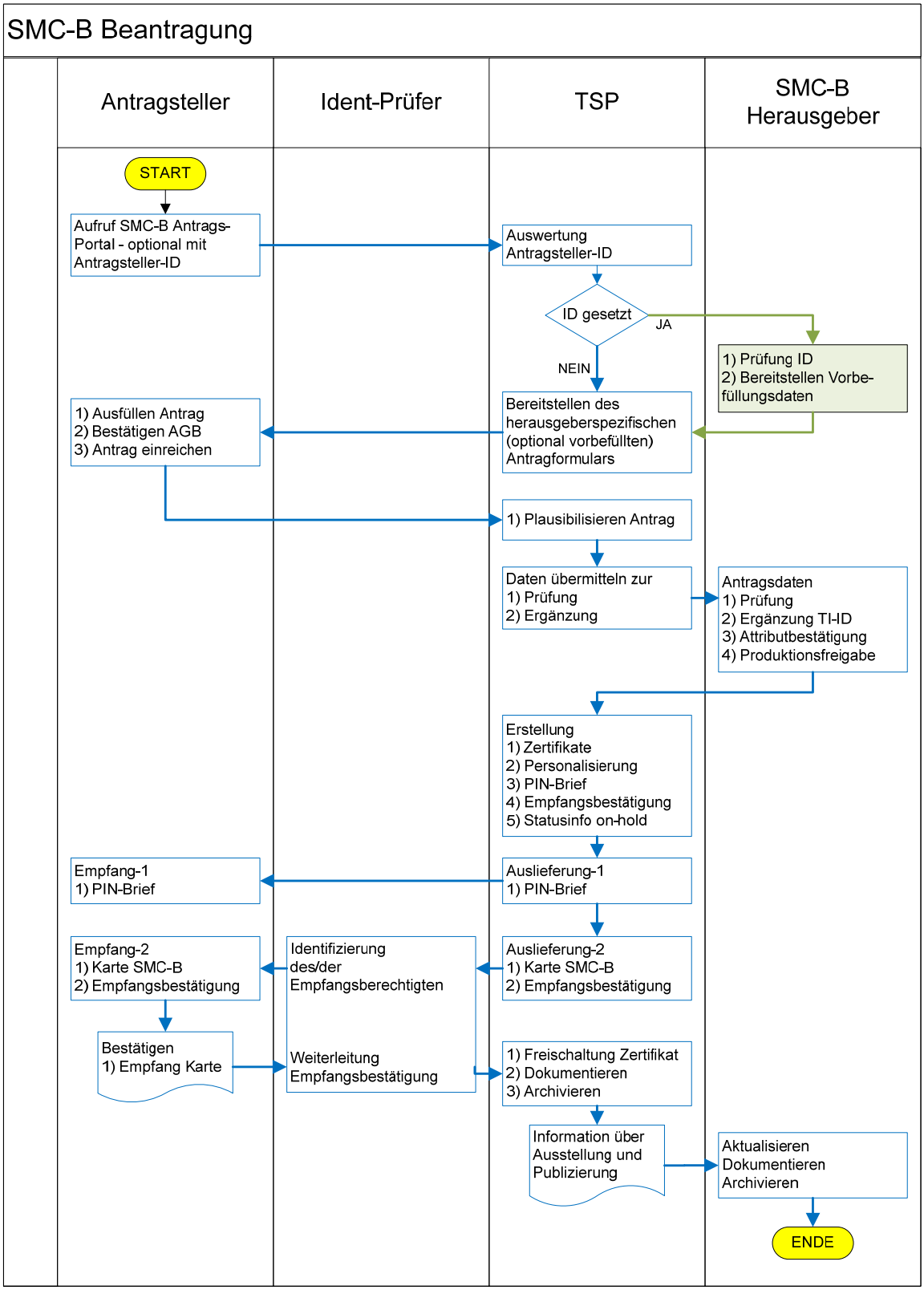

Abbildung 1: Antragsprozess SMC-B (generisch)

4.1.2.2 Sektor: Institutionen der Ärzteschaft

Der Ausgabeprozess über die KV / KBV sieht folgenden Ablauf unter Einbeziehung eines übergreifenden Praxisregisters vor:

(1) Der SMC-B-Antrag einer Arztpraxis wird von der zuständigen KV (bzw. KBV für Privatärzte) entgegengenommen,

(2) auf Vollständigkeit und Korrektheit geprüft und

(3) in das Praxisregister eingepflegt sowie als Kartenproduktionsauftrag freigegeben.

(4) Das Praxisregister stellt dem ZDA die aktuellen Kartenproduktionsaufträge zum Abruf zur Verfügung.

(5) Dieser produziert die Karte,

a. verschickt einen PIN/PUK-Brief an den Arzt,

b. verschickt zeitverzögert separat die Karte per PostIdent an den Arzt und

c. aktualisiert das Praxisregister mit den entsprechenden Karteninformationen.

(6) Der Arzt identifiziert sich und bestätigt oder verweigert den Empfang der Karte (PostIdent).

(7) Die KV / KBV erhält den Status der Kartenübergabe und pflegt den Status in das Praxisregister ein.

(8) Der ZDA erhält den Status der Kartenübergabe über das Praxisregister und veranlasst

a. beim positivem Ergebnis eine Freischaltung der X.509-Zertifikate im Verzeichnisdienst und

b. eine Aktualisierung des Praxisregisters über den Status der Freischaltung.

(9) Die SMC steht nun dem Arzt zur Nutzung zur Verfügung.

Bei fehlgeschlagenen Zustellversuchen erfolgt eine Rücksendung an die herausgebende KV bzw. KBV, wo über die weitere Verfahrensweise im Einzelfall entschieden wird.

Für den Antragsprozess gemäß den Punkten (1) bis (3) der obigen Abfolge sind noch folgende Differenzierungen vorgesehen, von denen im vorliegenden Dokument jedoch nur die Version c) adressiert wird:

Antragsverfahren Privatpraxis:

a) Papierbasiert Offline (nicht Gegenstand von ORS1)

b) Elektronisch Online (nicht Gegenstand von ORS1)

Antragsverfahren Vertragspraxis:

c) Papierbasiert Offline

d) Elektronisch Online (nicht Gegenstand von ORS1)

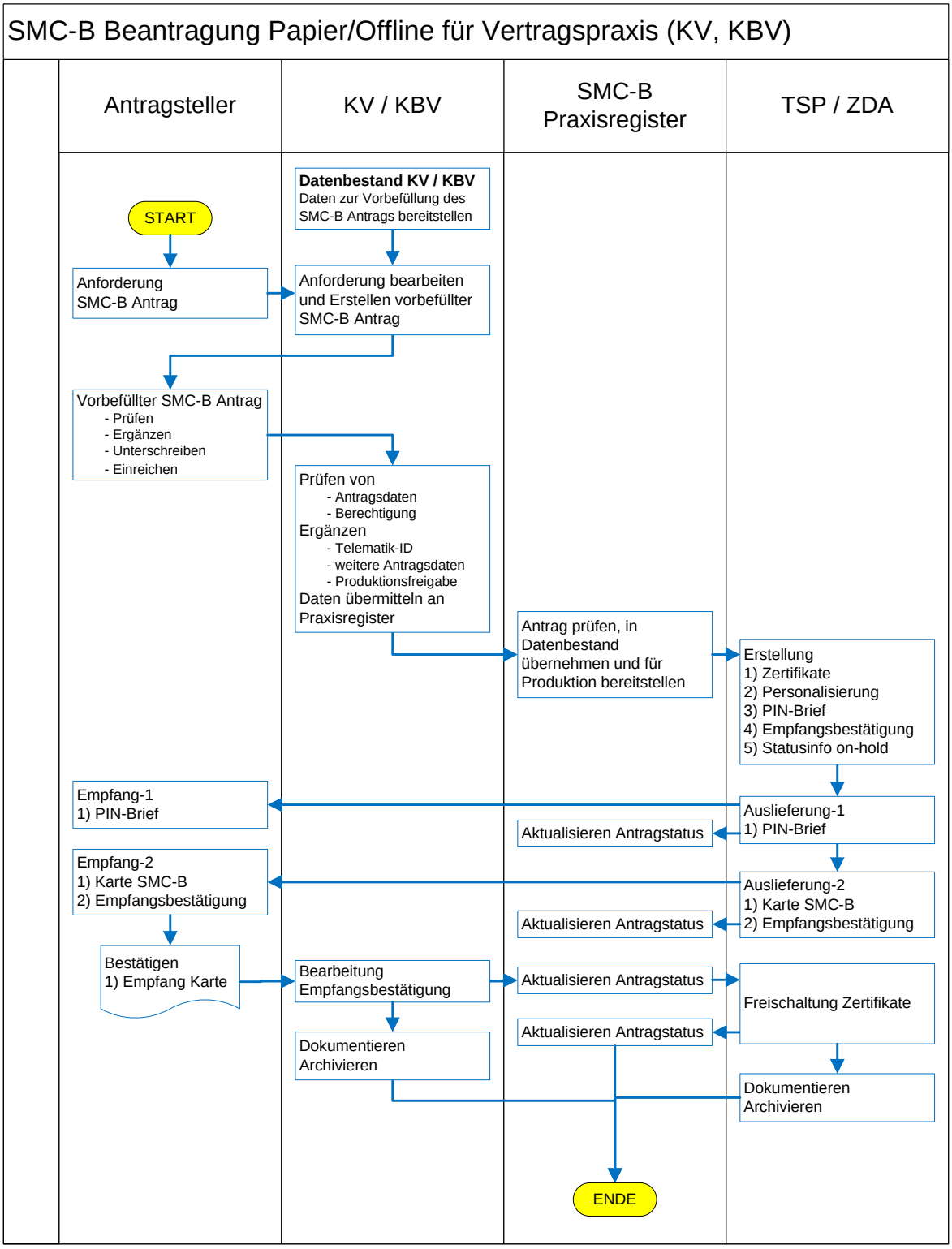

Abbildung 2: Antragsprozess SMC-B Vertragspraxis KV / KBV

4.1.2.3 Sektor: Vertragszahnärzteschaft

Zuständig für Freigabe und Sperrung von Zertifikaten auf der SMC-B ist die für den Vertragszahnarzt / die Vertragszahnärzte / das Medizinische Versorgungszentrum (MVZ) zuständige Kassenzahnärztliche Vereinigung am Sitz des entscheidungsbefugten Zulassungsausschusses.

Der Ablauf der Antragstellung verläuft analog wie in 4.1.2.1 beschrieben.

4.1.2.4 Sektor: Institutionen der Psychotherapeuten

Es gelten die Regelungen für Ärzte analog; siehe Kap 4.1.2.2

4.1.2.5 Sektor: Krankenhäuser

Keine Vorgaben in diesem Dokument.

4.2 Bearbeitung von Zertifikatsanträgen

Alle Antragsdaten zu einer SMC-B werden vom Herausgeber (Attributbestätigende Stelle) geprüft und im positiven Fall zur Produktion der SMC-B freigegeben.

Im Zuge dieser Freigabe sind neben den vom Antragsteller eingereichten Daten ggf. noch weitere Daten durch den Herausgeber zu ergänzen.

4.2.1 Sektorspezifische Festlegungen zu Antragsdaten

4.2.1.1 Sektor: Institutionen der Ärzteschaft

Keine Vorgaben in diesem Dokument.

4.2.1.2 Sektor: Institutionen der Vertragszahnärzteschaft

Online-Kennung

> Präfix vorkonfiguriert/Plausibilitätsprüfung/durch KZV änderbar
>
> Die Online-Kennung kann für eine Antragsvorbefüllung bereits von der KZV geliefert werden. Falls keine Antragsvorbefüllung erfolgt, ist die Online-Kennung als Default-Wert im Freigabeportal anzuzeigen (siehe: Online-Kennung in elektronischen Ausweisen der Zahnärzteschaft, Version 3.0):
>
> **`(2-2.[KZV-NR].2.[Nummernkreis].[ID-String])`**
>
> Die Online-Kennung kann durch die für den Antragsteller zuständige KZV geändert werden (u. U. Anpassung an KZV-eigene Struktur). Der ID-String als Default-Wert muss als eine für den KZV-Bereich eindeutige fortlaufende Nummer generiert werden.

commonName des Antragstellers (AS)

Vorbelegt mit "Zahnarztpraxis ASTitel ASVorname(n) ASNachname" (ggf. sinnvolle Kürzung/Änderung durch KZV-Mitarbeiter möglich).

subjectAlternateName des Antragstellers

E-Mail-Adresse der Zahnarztpraxis, die falls erforderlich, durch den zuständigen KZV-Mitarbeiter an eine KZV-eigene Struktur anpassbar sein muss.

Die Attributbestätigung und Freigabe des Antrages wird per QES im Freigabeportal durch einen berechtigten KZV-Mitarbeiter durchgeführt. Der dabei zu signierende Text muss die folgende Passage enthalten:

Antragsnummer: <Antrags-ID>

Es wird bestätigt, dass die

<Feldwert CommonName>

<Straße, Hausnr.>

<PLZ ORT>

berechtigt ist, einen Praxisausweis gemäß den gemeldeten Policies mit dem Attribut "Zahnarztpraxis" sowie dem CVC-Rollenprofil "2" bzw. dessen technischer Abbildung im G2 CV-Zertifikat zu erhalten.

Folgende Online-Kennung wurde vergeben: <Feldwert Online-Kennung>

Berechtigter Empfänger der SMC-B ist:

<ASTitel ASVorname(n) ASNachname

Meldeanschrift Antragsteller:

Straße, Hausnummer

Postleitzahl, Ort>

4.2.1.3 Sektor: Institutionen der Psychotherapeuten

Keine Vorgaben in diesem Dokument.

4.2.1.4 Sektor: Krankenhäuser

Keine Vorgaben in diesem Dokument.

4.2.2 Durchführung von Identifikation und Authentifizierung

Keine Vorgaben in diesem Dokument

4.2.3 Annahme oder Ablehnung von Zertifikatsanträgen

Keine Vorgaben in diesem Dokument

4.2.4 Bearbeitungsdauer bei Zertifikatsanträgen

Keine Vorgaben in diesem Dokument

4.3 Zertifikatserstellung

Keine Vorgaben in diesem Dokument

4.3.1 Aufgaben der Zertifizierungsstelle

Keine Vorgaben in diesem Dokument

4.3.2 Benachrichtigung des Antragstellers

Keine Vorgaben in diesem Dokument

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Der Antragsteller hat den Erhalt der SMC-B gegenüber dem Herausgeber zu bestätigten.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Der Status aller X.509-Zertifikate einer SMC-B wird durch die Zertifizierungsstelle in einem Verzeichnis geführt.

Mit der Beantragung einer SMC-B wird vom Antragsteller die Zustimmung zur Veröffentlichung der Statusauskünfte zur betreffenden SMC-B erklärt.

Tabelle 4: Tab_PKI_963 Bereitstellung der SMC-B-Statusauskünfte

	KZV	KV, KBV	DKTIG
Innerhalb der TI	OCSP	OCSP	OCSP
Internet	CRL, OCSP	CRL	-

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Die Zertifizierungsstellen informieren die Herausgeber der SMC-B über

- Auftragsstatus
    - Eingang / Bearbeitung des SMC-B-Antrags
        - Vom Antragsteller bearbeitet

        - Eingang des Papierantrags
        - Zur Freigabe
        - Freigegeben
    - Auslieferung
        - Karte ausgeliefert
        - Empfangsbestätigung für Karte erhalten
- Zertifikatsstatus
    - Freischaltung der Zertifikate
        - Zertifikate freigeschaltet
    - Statusänderung der Zertifikate
        - Zertifikate endgültig nicht freigeschaltet
        - Zertifikate gesperrt
        - Zertifikate abgelaufen

Die Benachrichtigung erfolgt entweder direkt an den Herausgeber oder über das Praxisregister.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Die Übergabe der SMC-B an den Antragsteller erfolgt auf sichere Art und Weise (PostIdent-Verfahren oder vergleichbares Verfahren) durch den Herausgeber bzw. dessen Dienstleister, so dass gewährleistet ist, dass nur der Antragsteller die SMC-B, insbesondere den darin enthaltenen privaten Schlüssel des CV-Zertifikates, erstmalig in Betrieb nehmen kann.

4.5.1 Nutzung durch den Zertifikatsinhaber

Die Nutzung der SMC-B sowie der darauf enthaltenen Zertifikate erfolgt im Rahmen der vom Herausgeber der SMC-B vorgegebenen Zwecke.

Nach Ablauf des Gültigkeitszeitraums oder nach Sperrung der SMC-B dürfen die zugehörigen privaten Schlüssel nicht mehr genutzt werden. Der Karteninhaber muss auch nach Ablauf des Gültigkeitszeitraums dafür sorgen, dass die privaten Schlüssel nicht missbräuchlich verwendet werden können. Bei Entsorgung muss die SMC-B sicher vernichtet bzw. unbrauchbar gemacht werden (beispielsweise durch physische Zerstörung der SMC-B).

4.5.2 Nutzung des Zertifikats durch die Relying Party

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

Für alle Unterkapitel keine Vorgaben in diesem Dokument

4.7 Schlüssel- und Zertifikatserneuerung (Re-key)

Für alle Unterkapitel keine Vorgaben in diesem Dokument

4.8 Zertifikatsmodifizierung

Für alle Unterkapitel keine Vorgaben in diesem Dokument

4.9 Widerruf / Sperrung und Suspendierung von Zertifikaten

Eine Suspendierung der SMC-B-X.509-Zertifikate ist nicht möglich.

SMC-B-X.509-Zertifikate können durch die Berechtigten gemäß Tab_PKI_964 gesperrt werden, so dass eine Statusprüfung dieser Zertifikate diese als gesperrt ausweist.

4.9.1 Gründe für Widerruf / Sperrung

Eine Sperrung der SMC-B bzw. der darauf befindlichen X.509-Zertifikate muss unverzüglich erfolgen, wenn

- eine Kompromittierung eines auf der Karte gespeicherten Schlüssels vorliegt,
- die eindeutige Zuordnung des Zertifikatsnehmers zu seinem Zertifikat nicht mehr gegeben ist,
- das Zertifikat Angaben enthält, die nicht oder nicht mehr gültig sind,
- die eindeutige Verbindung zwischen Zertifikat und Schlüssel nicht mehr gegeben ist,
- der Karteninhaber seinen Vertrag kündigt

4.9.2 Wer kann Widerruf / Sperrung beantragen

Für PKI-funktional oder -organisatorisch bedingte Sperrgründe und -berechtigungen gilt die nachfolgende Übersicht.

Tabelle 5: Tab_PKI_964 SMC-B – Sperrberechtigte und Sperrgründe

Sperrberechtigte Stellen *)	Zertifikate der Kartenarten				
	eGK	HBA nonQES	**SMC-B**	gSMC-K	FD, ZD
Praxis / med. Institution			**1**		
KV / KZV / KBV / DKTIG			**2, 4**		
gematik			**3**		

1) Jederzeit ohne Angabe von Gründen

2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß Ausgabepolicy

3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung

4) Wegfall oder Entzug geforderter Eigenschaften des ZDA/TSP gemäß Beauftragung bzw. sektoraler Zulassung

4.9.2.1 Sektor: Institutionen der Ärzteschaft

Keine Vorgaben in diesem Dokument.

4.9.2.2 Sektor: Institutionen der Vertragszahnärzteschaft

Ein Sperrauftrag für die Zertifikate der SMC-B kann a) durch den Vertretungsberechtigten der Praxis bei der zuständigen KZV veranlasst werden sowie b) durch die KZV selbst in Auftrag gegeben werden, sofern institutionelle Gründe dies erfordern, wie nachfolgend ausgeführt.

Vertragszahnärztliche Einzelpraxis:
Verliert ein in einer Einzelpraxis tätiger Zahnarzt seine vertragszahnärztliche Zulassung, so wird jede zu diesem Zahnarzt zugehörige SMC-B für Vertragszahnärzte durch die zuständige KZV gesperrt.
Die Änderung des Praxisstatus eines Zahnarztes führt ebenfalls zur Sperrung jeder zu diesem Zahnarzt zugehörigen SMC-B.

Vertragszahnärztliche (Ü)BAG:
Ändert sich die vertragszahnärztliche Zusammensetzung der ÜBAG, so wird jede zu dieser (Ü)BAG zugehörige SMC-B für Vertragszahnärzte durch die zuständige KZV gesperrt.

Vertragszahnärztliche Praxisgemeinschaft:
Regelungen analog derjenigen für die Einzelpraxis.

Vertragszahnärztliches MVZ:
Verliert ein MVZ seine vertragszahnärztliche Zulassung, so wird jede zu diesem MVZ zugehörige SMC-B für Vertragszahnärzte durch die zuständige KZV gesperrt. Die Sperrung von Zertifikaten eines MVZ zwischen Ärzten und Zahnärzten ist nicht Gegenstand des vorliegenden Dokumentes.

Wechsel des Praxissitzes:
Wechselt eine Vertragszahnarztpraxis den KZV-Bereich, wird die bisherige SMC-B durch die für den bisherigen Praxisort zuständige KZV gesperrt.

4.9.2.3 Sektor: Institutionen der Psychotherapeuten

Keine Vorgaben in diesem Dokument.

4.9.2.4 Sektor: Krankenhäuser

Keine Vorgaben in diesem Dokument.

4.9.3 Ablauf von Widerruf / Sperrung

Keine Vorgaben in diesem Dokument.

4.9.4 Fristen für den Zertifikatsinhaber

Keine Vorgaben in diesem Dokument.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Keine Vorgaben in diesem Dokument.

4.9.6 Anforderung zu Sperrprüfungen durch eine Relying Party

Keine Vorgaben in diesem Dokument.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

Keine Vorgaben in diesem Dokument.

4.9.8 Maximale Latenzzeit für Sperrlisten

Keine Vorgaben in diesem Dokument.

4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP)

Keine Vorgaben in diesem Dokument.

4.9.10 Anforderungen an Online-Statusabfragen (OCSP)

Keine Vorgaben in diesem Dokument.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Keine Vorgaben in diesem Dokument.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Keine Vorgaben in diesem Dokument.

4.9.13 Gründe für eine Suspendierung

Keine Vorgaben in diesem Dokument.

4.9.14 Wer kann Suspendierung beantragen

Keine Vorgaben in diesem Dokument.

4.9.15 Ablauf einer Suspendierung

Keine Vorgaben in diesem Dokument.

4.9.16 Maximale Sperrdauer bei Suspendierung

Keine Vorgaben in diesem Dokument.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

4.11 Beendigung des Vertragsverhältnisses

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

4.12 Schlüsselhinterlegung und –wiederherstellung (Key Escrow und Recovery)

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

6 Technische Sicherheitsmaßnahmen

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatsprofil

Die X.509-Zertifikatsprofile für die SMC-B sind definiert in [gemSpec_PKI#5.3.4].

Das CV-Zertifikatsprofil zur Rollenauthentisierung einer SMC-B ist definiert in [gemSpec_PKI#6.3.1].

Nachfolgend werden nur diejenigen Profilattribute beschrieben, die zwischen den einzelnen Sektoren verschieden genutzt werden.

7.1.1 Versionsnummer

Keine Vorgaben in diesem Dokument.

7.1.2 Zertifikatserweiterungen

Als sektorspezifische Inhalte der v3-Extension Admission gelten die Festlegungen in [gemSpec_PKI#4.8.3.2] und [gemSpec_OID#3.5.1].

7.1.3 Algorithmus Bezeichner (OID)

Keine Vorgaben in diesem Dokument.

7.1.4 Namensformen

Keine Vorgaben in diesem Dokument.

7.1.5 Namensbeschränkungen

Keine Vorgaben in diesem Dokument.

7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID)

Die sektorspezifische Zertifizierungsrichtlinie ergänzt die übergreifende Policy der gematik[6].

Im vorliegenden Dokument [gemRL_SMC-B_ORS1] sind die sektorspezifischen Ausprägungen der Zertifizierungsprozesse für die Phase „Online-Rollout (Stufe 1)“ für alle Sektoren zusammengefasst. Aus diesem Grund enthalten alle SMC-B-Zertifikate

[6] [gemRL_TSL_SP_CP]

während dieser Projektphase im Feld certificatePolicies einheitlich die OID dieses Dokuments.

Mit Übergang zum Regelbetrieb können hierzu Änderungen erfolgen. Bis dahin ausgegebene Zertifikate behalten ihre Gültigkeit bis zu ihrem regelmäßigen Ablauf.

Übergreifend gelten die technischen Regelungen in [gemSpec_PKI#4.8.3.3] und [gemSpec_OID#3.5.1].

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

7.1.8 Syntax und Semantik von Policy Qualifiern

Siehe Kap 7.1.6

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies)

Keine Vorgaben in diesem Dokument.

7.2 Sperrlistenprofil

Keine Vorgaben in diesem Dokument.

7.2.1 Versionsnummer

Keine Vorgaben in diesem Dokument.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Keine Vorgaben in diesem Dokument.

7.3 OCSP-Profil

Keine Vorgaben in diesem Dokument.

7.3.1 Versionsnummer

Keine Vorgaben in diesem Dokument.

7.3.2 OCSP-Erweiterungen

Keine Vorgaben in diesem Dokument.

8 Konformitätsprüfung (Compliance Audit, Assessments)

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

9 Andere geschäftliche und rechtliche Angelegenheiten

Für alle Unterkapitel keine Vorgaben in diesem Dokument.

10 Informationen zum Dokument

Anhang A - Verzeichnisse

A1- Abkürzungen

Kürzel	Erläuterung
TSL	Trust-service Status List
OID	Object Identifier
TI	Telematikinfrastruktur
TSP	Trust Service Provider
SMC-B	Sicherheitsmodul vom Typ B
OCSP	Online Certificate Status Protocol
CV-Zertifikate	Card Verifiable-Zertifikate
eGK	Elektronische Gesundheitskarte
HBA	Heilberufsausweis
KV	Kassenärztliche Vereinigung
PIN	Personal Identification Number
QES	Qualifizierte elektronische Signatur
PKI	Public Key Infrastructure
ZDA	Zertifizierungsdiensteanbieter
CA	Certificate Autority
CVC	Card Verifiable Certificate
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH
DKG	Deutsche Krankenhausgesellschaft
KBV	Kassenärztliche Bundesvereinigung
KZV	Kassenzahnärztliche Vereinigung

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

Abbildung 1: Antragsprozess SMC-B (generisch) 21
Abbildung 2: Antragsprozess SMC-B Vertragspraxis KV / KBV 24

A4 – Tabellenverzeichnis

Tabelle 1: Tab_PKI_960 Sektorinterne Alternativbezeichnung der SMC-B 11
Tabelle 2: Tab_PKI_961 Übersicht der Attributbestätigenden Stellen / SMC-B-Herausgeber 12
Tabelle 3: Tab_ PKI_962 Erforderliche Antragsdaten 16
Tabelle 4: Tab_PKI_963 Bereitstellung der SMC-B-Statusauskünfte 27
Tabelle 5: Tab_PKI_964 SMC-B – Sperrberechtigte und Sperrgründe 30

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_TSL_SP_CP]	gematik: Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_OID]	gematik: Spezifikation OID (bis Release 0.5.3: Spezifikation: Festlegung von OIDs)
[gemSpec_PKI]	gematik: Spezifikation PKI

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber: Titel
[BSI_2005]	BSI (2005): IT-Grundschutz-Kataloge (11. Ergänzungslieferung 12/2008) https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[ISO17799]	ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management
[ISO27001]	ISO/IEC 27001:2005 Specification for an Information Security Management System, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques