Elektronische Gesundheitskarte und Telematikinfrastruktur

Richtlinie für die Herausgabe der SMC-B ORG

Version:	1.0.0
Stand:	05.10.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemRL_SMC-B_ORG_AP

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	05.10.20		Initiale Erstellung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

In diesem Dokument werden die Festlegungen zur Herausgabe der SMC-B ORG durch die gematik beschrieben. Dazu gehören die Antrags-, Freigabe-, Sperr- und Produktions-Prozesse. Die gematik agiert als Kartenherausgeber und verifiziert die Berechtigung der einzelnen Antragssteller einer SMC-B ORG in Abstimmung mit den verschiedenen attributbestätigenden Stellen.

1.2 Zielgruppe

Das Dokument richtet sich in erster Linie an die Kammern, Vereine und Organisationen, welche den verschiedenen leistungserbringenden Sektoren des Gesundheitswesens vorangestellt sind und zudem ein berechtigtes Interesse für den Zugang zur TI vorweisen können. Insbesondere richtet es sich an jene Nutzerkreise, welche nicht berechtigt sind, über die ihren Sektoren vorangestellten Spitzenverbände eine andere Form der SMC-B zu beantragen.

1.3 Geltungsbereich

Der Geltungsbereich dieses Dokumentes steht in direktem Zusammenhang mit den anderen durch die gematik veröffentlichten Dokumenten und muss daher im Gesamtzusammenhang der SMC-B ORG innerhalb der TI betrachtet und verstanden werden, wobei hier für den Empfänger der Karte relevante Informationen zur Herausgabe aufgezeigt werden.

1.4 Abgrenzung des Dokuments

Die Certificate Policy [gemRL_TSL_SP_CP] der gematik gibt grundsätzliche Sicherheitsanforderungen hinsichtlich der Beantragung, Erzeugung, Verwaltung und Sperrung von nicht-qualifizierten (nonQES) X.509-Zertifikaten wieder.

Die Berechtigung zum Erhalt der SMC-B ORG und die Bedingung, welche Akteure berechtigt sind, eine SMC-B ORG zu beantragen, sind in der Berechtigungs-Policy [gemRL_SMC-B_ORG_BP] beschrieben.

Einheitlich an alle TSP X.509-nonQES gerichtete Anforderungen bzgl. der Beantragung, Erzeugung, Ausgabe und Sperrung von X.509-Organisations-Zertifikaten sowie die Bereitstellung der Zertifikatsstatusinformation sind in [gemSpec_X.509_TSP] beschrieben und werden hier nicht erneut behandelt.

2 Überblick

Die Karte SMC-B ORG ist eine speziell ausgestattete SMC-B mit der Besonderheit, dass sie keine Zugriffsrechte auf die Anwendungen der elektronischen Gesundheitskarte (eGK) nach § 291a Abs. 2 und 3 SGB V besitzt. Diese Zugriffseinschränkung wird durch den Verzicht auf die CV-Rollenzertifikate, welche den Zugriff auf die eGK steuern, realisiert. Ein Zugriff auf die eGK (elektronische Gesundheitskarte) ist damit ebenso nicht möglich, wie der Zugriff auf Stammdaten oder sonstige Daten eines Versicherten. Der TI-Zugang mittels SMC-B ORG dient primär der Nutzung der Fachanwendung KIM (Kommunikation im Medizinwesen). Sekundär bietet der TI-Zugang über die SMC-B ORG die Möglichkeit, auf Monitoring-Systeme zur Betriebsüberwachung technischer Komponenten zuzugreifen. Mit der SMC-B ORG kann nur an rein technischen Fachdiensten teilgenommen werden, welche selbst keine direkte Verbindung zu Versichertendaten und medizinischen Anwendungen herstellen können.

Die Zugriffsberechtigungen und damit die der jeweiligen Organisation zur Verfügung stehenden Dienste (z.B. KIM, Monitoring-Zugänge und weitere Anwendungen des Gesundheitswesens) werden durch die Erweiterung *Admission* im Zertifikat gesteuert.

Mit der Karte SMC-B ORG kann in Verbindung mit einem durch die gematik zugelassenen Konnektor eine IPsec-VPN-Verbindung zwischen der Organisation und den zentralen sowie den dezentralen Diensten der TI realisiert werden.

Die Nutzung der SMC-B ORG kann durch Kartensperrung unterbunden werden.

Im Verlauf des Dokuments bezeichnet der Ausdruck „SMC-B ORG“ je nach Zusammenhang entweder eine oder die Karte (Singular) oder die Karten SMC-B ORG (Plural).

3 Identifizierung und Authentifizierung

Es gelten die Festlegungen für produktive SMC-B zu

- Namenregeln
- Überprüfung der Identität
- Identifizierung und Authentifizierung von Organisationen

gemäß [gemRL_TSL_SP_CP] und [D-TRUST_CPS] des Anbieters SMC-B ORG.

4 Zentraler Herausgabeprozess

4.1 Rollen und Aufgaben

Die Rollen und ihre Aufgaben sind in der folgenden Abbildung dargestellt:

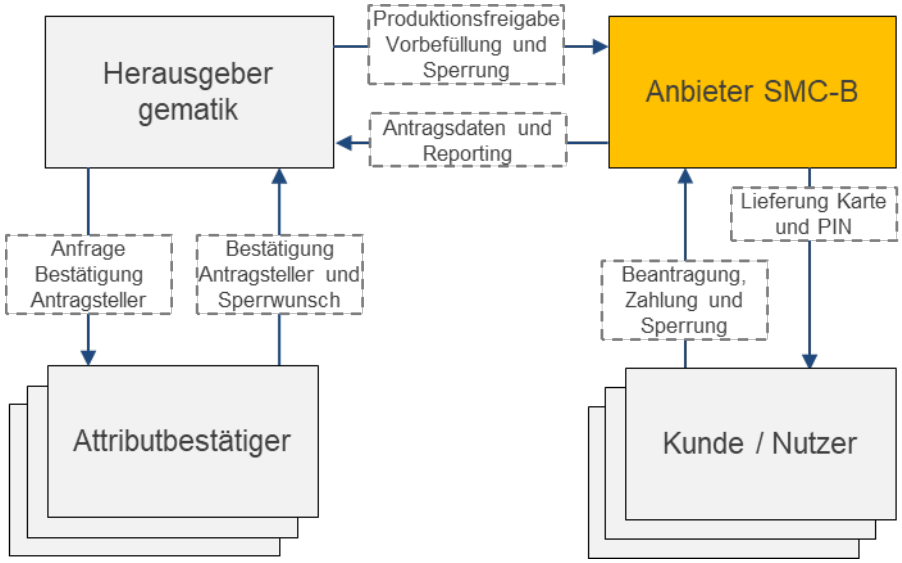

Abbildung 1: Rollen und Aufgaben

Folgende Akteure sind an den Herausgabeprozessen beteiligt:

Tabelle 1: Akteure

Akteur	Beschreibung
Antragsteller (Kunde/Nutzer)	Handelt im Namen einer Institution, welche den legitimen Bedarf zum Einsatz einer SMC-B ORG hat. Berechtigte Institutionen und die für diese handelnden Personen, welche eine SMC-B ORG beantragen dürfen, sind der attributbestätigenden Stelle bekannt.
Attributbestätigende Stelle	Besitzt die notwendigen Informationen, um den Antragsteller zu identifizieren und seinen legitimen Bedarf zu verifizieren. Regelt Vergabe/Bestätigung der institutionsspezifischen Attribute.
Anbieter SMC-B	Produziert die SMC-B ORG im Auftrag der gematik. Verantwortet den Betrieb der PKI (RA, CA, OCSP), stellt die Schnittstellen für die Kartenpersonalisierung bereit und übernimmt den Vertrieb der SMC-B ORG gegenüber dem Antragsteller im Auftrag der gematik.
Kartenherausgeber/ gematik	Die gematik übernimmt die Rolle der zentralen Herausgabeinstitution. Sie steuert die Freigabe von Anträgen gegenüber dem beauftragten Anbieter der SMC-B ORG auf Basis der Informationen der attributbestätigenden Stelle.

4.2 Herausgabeprozesse und das Zusammenspiel der beteiligten Akteure

Im Folgenden werden die Prozessen und das Zusammenspiel der ab der Herausgabe beteiligten Akteure beschrieben:

Antragstellung

Der Antragsteller stellt im Namen seiner Institution beim Anbieter SMC-B einen Antrag auf Ausstellung einer SMC-B ORG und akzeptiert die Vertragsbedingungen inkl. Kosten und sonstigen Bedingungen (Datenübermittlung an attributbestätigende Stelle und gematik zur Freigabe).

Freigabe der Produktion SMC-B ORG

Die gematik spricht in Abstimmung mit der attributbestätigenden Stelle eine Produktionsfreigabe aus.

Produktion und Versand von Karte und PIN-Brief

Der Anbieter SMC-B prüft die erhaltenen Daten und erzeugt die kartenspezifischen Zertifikate. Die SMC-B ORG werden personalisiert und fertiggestellte Karten vom Anbieter SMC-B an die angegebene Lieferanschrift des Antragstellers versendet. Zeitversetzt zum Kartenversand versendet der Anbieter SMC-B den PIN/PUK-Brief an den Antragsteller.

Freischaltung

Der Anbieter SMC-B schaltet nach Bestätigung des Antragstellers über die erfolgreiche Übergabe/Inbetriebnahme der Karten die Zertifikate frei. Die Institution des Antragstellers kann die beantragte Karte verwenden. Der Anbieter SMC-B meldet der gematik die ordnungsgemäße Auslieferung der SMC-B ORG für die Administration des Verzeichnisdienstes.

Sperrung

Auf Antrag des Karteninhabers, bei Wegfall der zugrundeliegenden Berechtigung und weiteren Gründen (z.B. Zahlungsausfall) können alle Zertifikate einer Karte gesperrt werden.

4.3 Freigabedaten der gematik

Die gematik übernimmt im Rahmen ihres gesetzlichen Auftrages die Herausgeberrolle für SMC-B ORG.

4.3.1 Festlegung der Telematik-ID

Als Freigabedaten legt die gematik in der Herausgabeverantwortung die Telematik-ID gemäß [gemSpec_PKI#4.7] der folgenden grundsätzlichen Bildungsregel fest:

- Präfix = 9
- Separator = "-"
- Fortsatz

Der Fortsatz der Telematik-ID wird wie folgt gebildet:

<Karten-/Identtyp>.<Kennzeichnung Nutzerkreis/Bestätigende Stelle>.<Fortlaufende Nummer>

Tabelle 2: Fortsatz der Telematik-ID der durch die gematik herausgegebenen Karten

<Karten-/Identtyp>	1 Stelle • Person/(Heil-)Berufsausweis/(H)BA = 1 • Organisationskarte/Institutionskarte/SMC-B = 2
<Kennzeichnung Nutzerkreis/ attributbestätigende Stelle>	3 Stellen • Wertebereich "0123456789" • letzte 3 Stellen der ProfessionOID gemäß Freigabedaten der gematik
<Fortlaufende Nummer>	8 Stellen • Wertebereich "0123456789" gemäß Freigabedaten der gematik

Beispiel für die Telematik-ID einer SMC-B ORG der Bundesärztekammer:

9-2.229.00008731

4.3.2 Festlegung Zertifikatserweiterung ‚Admission'

Die Festlegung der ProfessionOID der einzelnen Nutzerkreise der SMC-B ORG ist [gemSpec_OID] und [gemRL_SMC-B_ORG_BP#5] zu entnehmen.

4.4 Auftragsdaten der attributbestätigenden Stellen

Die folgenden Daten sind im Rahmen der Freigabe in Abstimmung zwischen gematik (Herausgeber) und attributbestätigenden Stellen gemäß [gemRL_SMC-B_ORG_BP] festzulegen:

- **Common Name**
  - verpflichtend
  - eineindeutiger Bezeichner innerhalb der TI
  - wird von der attributbestätigenden Stelle gewählt/festgelegt
  - relevant für den VZD-Eintrag, da es von E-Mail Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet wird
  - Beispiel: <Organisationsname**>**
- SubjectAltName
  - optional
  - alternativer Organisationsname
  - gemäß [gemRL_SMC-B_ORG_BP] für die jeweilige Betriebsstätte der attributbestätigenden Stelle zu füllen.

5 Sicherheitsmaßnahmen

5.1 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Nutzungsdauer von Zertifikaten soll nach [gemSpec_Krypt] auf maximal 5 Jahre beschränkt werden. Diese Vorgabe wird für die Endbenutzerzertifikate der SMC-B ORG ebenfalls umgesetzt. Die Gültigkeit der CA- und Endbenutzerzertifikate kann zudem durch die Verwendung einer TSL während des laufenden Betriebs weiter eingeschränkt werden, da die TSL in diskreten Zeitabständen aktualisiert und veröffentlicht wird. Hierdurch kann ein zu einer kürzeren Gültigkeitsdauer der Zertifikate äquivalentes Sicherheitsniveau erreicht werden.

Weitere Vorgaben zu Sicherheitsmaßnahmen sind den entsprechenden Kapiteln aus [gemRL_TSL_SP_CP] der gematik und [D-TRUST_CPS] des Anbieters SMC-B ORG zu entnehmen.

6 Betriebliche Maßnahmen

Es gelten die Festlegungen für produktive SMC-B gemäß [gemRL_TSL_SP_CP].

6.1 Zertifikatsausgabe

Die X.509-Zertifikate einer SMC-B ORG werden nicht von einer separaten SubCA abgeleitet, sondern sie können analog zu anderen SMC-B von den bestehenden CAs des Anbieters SMC-B bestätigt werden.

6.2 Zertifikats- und Schlüsselerneuerung (re-keying)

Die Erneuerung der Zertifikate der SMC-B ORG basierend auf den jeweils bestehenden Schlüsseln ist nicht vorgesehen.

Eine Schlüsselerneuerung ist gleichbedeutend mit der erneuten Produktion von Zertifikaten und Schlüsseln sowie einer entsprechenden SMC-B ORG für denselben Karteninhaber.

6.3 Zertifikatsänderung

Eine Zertifikatsänderung ist für SMC-B ORG nicht vorgesehen.

6.4 Sperrung und Suspendierung/Desuspendierung von Zertifikaten

Eine Suspendierung/Desuspendierung von Zertifikaten der SMC-B ORG ist nicht vorgesehen.

Nur Sperrberechtigte dürfen eine Sperrung von Endanwenderzertifikaten vornehmen. Sperrberechtigt sind der Empfänger der SMC-B ORG, die gematik als Herausgeber und – über eine Meldung bei der gematik – die verantwortliche attributbestätigende Stelle.

Der Karteninhaber kann über das Antragsportal die Sperrung beantragen. Der TSP X.509 nonQES prüft vor der Sperrung eines Zertifikats die Berechtigung des Sperrantragstellers.

Nach erfolgter Sperrung werden der Inhaber- und der Herausgeber der SMC-B ORG über die Sperrung informiert.

6.5 Bedingung für eine Sperrung

Die gematik als Herausgeber kann die Zertifikate einer SMC-B ORG bei Hinweisen auf einen Missbrauch sperren.

Die zuständige attributbestätigende Stelle kann bei Wegfall oder Entzug geforderter Eigenschaften der Empfängerorganisation eine Sperrung durch die gematik veranlassen.

Der Karteninhaber ist verpflichtet, bei Verlust einer oder mehrerer SMC-B ORG dieses unverzüglich an den Anbieter SMC-B zu melden und eine Sperrung zu veranlassen. Er ist generell befugt, seine SMC-B ORG jederzeit ohne Angabe von Gründen zu sperren.

6.6 Verfahren für einen Sperrantrag

Detaillierte Festlegungen zum Sperrverfahren wie

- Fristen für einen Sperrantrag

- Authentifizierung der Sperrberechtigten
- die Bearbeitungsdauer des Sperrantrags etc.

können dem [D-TRUST_CPS] des Anbieters SMC-B ORG entnommen werden.

6.7 Bereitstellung von Statusauskünften

Der Anbieter SMC-B ORG stellt Statusauskünfte per Sperrlisten (CRLs) und OCSP zur Statusprüfung der Zertifikate der SMC-B ORG zur Verfügung. Sperrlisten können jeweils von einer ausstellenden SubCA oder an der Herausgabe SMC-B ORG beteiligten SubCAs (indirect CRLs) bereitgestellt werden.

Detaillierte Vorgaben zu Sperrlisten und zum OCSP-Statusprüfdienst sind dem Dokument [gemSpec_PKI#10.7] und [D-TRUST_CPS] des Anbieters SMC-B ORG zu entnehmen.

6.7.1 Aktualisierung und Veröffentlichung von Sperrlisten

Die Zertifikate einiger Empfängerkreise (siehe gemRL_SMC-B_ORG_BP) sind im Internet über die Sperrlisten des Anbieters SMC-B ORG prüfbar. Dieser Anwendungsfall hat für die TI keine Relevanz und wird auch nicht detaillierter betrachtet.

Festlegungen zur Gültigkeitsdauer von Sperrlisten sind dem Dokument [gemSpec_PKI#10.7] und [D-TRUST_CPS] des Anbieters SMC-B ORG zu entnehmen.

6.7.2 Online-Verfügbarkeit von OCSP-Statusinformationen

Der Anbieter SMC-B ORG stellt einen OCSP-Responder in der TI (OCSP-Responder sind in der TSL-Datei mit dem „ServiceTypeIdentifier" "http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP" markiert) und im Internet (die zu ermittelnde OCSP-Adresse für die OCSP-Anfrage ist im AIA-Feld des anfragenden Zertifikats hinterlegt) zur Statusprüfung bereit. Die in der SMC-B ORG personalisierten X.509-Zertifikate sind während ihres Gültigkeitszeitraumes jederzeit mittels OCSP innerhalb und außerhalb der TI validierbar.

6.8 Verzeichnisdienste und Veröffentlichungen

Die gematik als Herausgeber SMC-B ORG verantwortet die Befüllung des Verzeichnisdienstes (VZD) der TI. Grundlage bilden die Attribute des X.509-ENC-Zertifikates der SMC-B ORG, welche nach Speicherung im VZD u.a. mittels LDAP-Clients abgefragt werden können.

Einträge des VZD werden durch die gematik als Herausgeber oder durch den beauftragten Anbieter SMC-B ORG erstellt und gepflegt.

Zu den verpflichtenden VZD-Einträgen gehören die Freigabedaten der gematik (Telematik-ID und ProfessionOIDs, vgl. Kapitel 4.3) und die zwischen der gematik und den attributbestätigenden Stellen abgestimmten Auftragsdaten (CommonName, vgl. Kapitel 4.4).

Vorgaben zu Schnittstellen und Sicherheitsanforderungen sind [gem_VZD] und [gemILF_Pflege_VZD] zu entnehmen.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AIA	Authority Info Access
CV-Zertifikate	Card Verifiable (verwendet zum Freischalten der eGK)
CA/SubCA	Certificate Authority (Zertifizierungsstelle)
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Zertifikatsperrliste)
eGK	elektronische Gesundheitskarte
EE-Zertifikat	End-Entity certificate (Endanwender-Zertifikat)
OCSP	Online Certificate Status Protocol
OID	Object-Identifier (dient zur eineindeutigen Referenzierung zu Objekten
PIN	Personal Identification Number (persönliche Identifikationsnummer)
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key (persönliche Entsperrschlüssel)
RA	Registration Authority (Registrierungsstelle)
SGB	Sozialgesetzbuch
SMC-B	Security Module Card, Typ B
SMC-B ORG	SMC-B für Organisationen ohne Zugriff auf medizinische Daten der eGK
TI	Telematikinfrastruktur
VPN	Virtual Private Network
TSP X.509 nonQES	Trust Service Provider für nicht qualifizierte X.509-Zertifikate
VZD	Verzeichnisdienst

A2 – Glossar

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

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

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 ist in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

Quelle	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemRL_TSL_SP_CP	gematik: Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_PKI]	gematik: Übergreifende Spezifikation PKI
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_VZD]	Spezifikation Verzeichnisdienst
[gemILF_Pflege_VZD]	gematik: Implementierungsleitfaden zur Pflege der Daten des Verzeichnisdienstes
[gemSpec_X.509_TSP]	gematik: Spezifikation Trust Service Provider X.509
[gemRL_SMC-B_ORG_BP]	gematik: Berechtigungsgrundlagen zur Beantragung und zum Erhalt der SMC-B ORG

A5.2 – Weitere Dokumente

Quelle	Herausgeber (Erscheinungsdatum): Titel
[D-TRUST_CPS]	Certification Practice Statement, D-TRUST Telematikinfrastruktur Version 2.0 https://www.d-trust.net/pdf-download/D-TRUST_TSP-TI_CPS_v2.0.pdf