

Berechtigungsgrundlagen zur Beantragung und zum Erhalt der SMC-B ORG

Version: 1.0.0
Revision: 200031
Stand: 02.03.2020
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemRL_SMC-B_ORG_BP

Dokumentinformationen

Änderungen zur Vorversion

Erstellung des Dokuments.

Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---------|----------|----------------|---|-------------|
| 0.9.0 | 12/2019 | | Zur Kommentierung freigegeben | gematik |
| 0.9.1 | 01/2020 | | Kommentierungen eingearbeitet | gematik |
| 1.0.0 | 02.03.20 | | freigegeben | gematik |
| | | | | |
| | | | | |

| | |
|--|-----------|
| 1 Einordnung des Dokumentes | 4 |
| 1.1 Zielsetzung | 4 |
| 1.2 Zielgruppe | 4 |
| 1.3 Geltungsbereich | 4 |
| 1.4 Abgrenzung des Dokuments | 4 |
| 2 Einleitung fachlicher Teil..... | 5 |
| 2.1 Überblick | 5 |
| 3 Berechtigung zum Erhalt einer SMC-B ORG | 6 |
| 3.1 Gematik GmbH (gematik) | 6 |
| 4 Identifizierung und Authentifizierung | 7 |
| 4.1 Randbedingungen..... | 7 |
| 5 Format der Zertifikate..... | 8 |
| 5.1 Herausgeber von SMC-B ORG | 8 |
| 5.1.1 X.509 Zertifikatsprofil der SMC-B ORG | 9 |
| 6 Anhang C - Verzeichnisse..... | 13 |
| 6.1 Abkürzungen | 13 |
| 6.2 Glossar | 14 |
| 6.3 Referenzierte Dokumente | 14 |
| 6.4 Dokumente der gematik | 14 |
| 6.5 Tabellenverzeichnis | 14 |

1 Einordnung des Dokumentes

1.1 Zielsetzung

Dieses Dokument beschreibt generisch die Voraussetzungen, anhand welcher unterschiedliche Organisationsformen berechtigt werden, eine SMC-B ORG (TSP-X.509 nonQES) zu beantragen. Die Beschreibung des generischen Profils SMC-B ORG in einem eigenen Dokument dient der Vereinfachung der gematik-internen Prozesse bei der Spezifikation und als Basis für weitere Ausprägungen von SMC-B.

1.2 Zielgruppe

Das Dokument richtet sich in erster Linie an die Kammern, Vereine, Verbände und Gesellschaften, welche den verschiedenen leistungserbringenden Sektoren des Gesundheitswesens vorangestellt sind und an den TSP, der von der gematik GmbH für die Personalisierung und Herausgabe der SMC-B ORG beauftragt wurde.

1.3 Geltungsbereich

Das Dokument betrachtet die im Zusammenhang mit der Telematikinfrastruktur (TI) stehenden Organisationen und bezieht sich insbesondere auf die innerhalb der TI zuzulassenden Systeme.

Detaillierte Prozessbeschreibungen im Zusammenhang mit der TI ebenso wie konkrete Vorgaben sind durch die gematik GmbH (gematik) in zahlreichen gesonderten Dokumenten (Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung ...) beschrieben. Der Geltungsbereich dieses Dokumentes steht in direktem Zusammenhang mit den anderen durch die gematik veröffentlichten Dokumente und muss daher im Gesamtzusammenhang der SMC-B ORG innerhalb der TI betrachtet und verstanden werden, wobei im vorliegenden Dokument die Konkretisierung des SMC-B-ORG-Profiles für die jeweilige Organisation erfolgt.

1.4 Abgrenzung des Dokuments

Im vorliegenden Dokument sind ausschließlich die Grundlagen beschrieben, die im Zusammenhang mit dem Berechtigungserhalt stehen. Darüber hinaus geht das Dokument auf die Befüllung der spezifischen Attribute im Zertifikat ein.

Die für die Beantragung, Erzeugung, Verwaltung und Sperrung von nicht-qualifizierten (nonQES) X.509-Zertifikaten erforderlichen Prozesse im Zusammenhang mit der SMC-B ORG sind in dem gesonderten Dokument [gemRL_AP_SMC-B ORG] beschrieben. Zusätzlich sind für personalisierte SMC-B ORG geltende Anforderungen im Dokument [gemSpec_SMC-B] beschrieben.

2 Einleitung fachlicher Teil

Bei der SMC-B ORG handelt es sich um eine spezielle SMC-B-Variante, die es den Gesellschaftern der gematik und den durch sie vertretenen Organisationen ermöglicht, einen TI-Zugang zu erhalten und bspw. auf TI-Dienste zuzugreifen.

Ein Zugriff auf die eGK (Gesundheitskarte) ist damit ebenso wenig möglich wie auf sonstige Daten oder bspw. die Stammdaten der Versicherten. Der Zugang mittels SMC-B ORG dient primär der Teilnahme an KOM-LE (Kommunikation Leistungserbringer). Sekundär bietet der TI-Zugang den Zugriff auf Monitoring-Systeme zur Betriebsüberwachung technischer Komponenten.

2.1 Überblick

Die SMC-B ORG ist eine spezielle Variante der Security Module Card Typ B (SMC-B). Sie besitzt kein CV-Zertifikat. Mit ihr kann in Verbindung mit einem durch die gematik zugelassenen Konnektor eine IPsec-VPN-Verbindung zwischen der Organisation und zentralen sowie dezentralen Diensten der TI realisiert werden. Die Zugriffsberechtigungen und damit die der jeweiligen Organisation zur Verfügung stehenden Dienste (z.B. KOM-LE, Monitoring-Systeme oder Störungssampel), werden bei der SMC-B ORG allein durch die im X.509-Zertifikat hinterlegten Parameter `professionOID` bzw. `professionItem` gesteuert.

3 Berechtigung zum Erhalt einer SMC-B ORG

Zur Beantragung der SMC-B ORG berechtigt sind die Gesellschafter der gematik und die durch sie vertretenen Organisationen.

Weitere Organisationen können nach Beschluss der Gesellschafterversammlung der gematik berechtigt werden.

Folgende Spitzenverbände sind zum Erhalt einer SMC-B ORG berechtigt:

- Bundesärztekammer (BÄK)
- Bundeszahnärztekammer (BZÄK)
- Kassenzahnärztliche Bundesvereinigung (KZBV)
- Kassenärztliche Vereinigungen (KV)
- Kassenärztliche Bundesvereinigung (KBV)
- Deutscher Apothekerverband e.V. (DAV)
- Spitzenverband Bund der Krankenkassen (GKV-SV)
- Deutsche Krankenhausgesellschaft (DKG)
- Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG)
- Kassenzahnärztliche Vereinigungen (KZV)
- Landesapothekerverbände (LAV)
- Landesärztekammern und berechtigte Bezirksärztekammern (LÄK)
- Landeszahnärztekammern (LZÄK)
- Landesverbände von Krankenhausträgern

3.1 gematik GmbH (gematik)

Die gematik GmbH (ehem. gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) ist durch ihre Gesellschafter beauftragt und gemäß § 291b SGB V befähigt, die Weiterentwicklung der Telematikinfrastruktur zu gewährleisten. Sie tritt ebenfalls als Herausgeber der SMC-B ORG auf.

4 Identifizierung und Authentifizierung

Um die Berechtigung der antragstellenden Akteure sicher zu stellen, müssen diese eindeutig identifiziert werden. Die Identifikation erfolgt im Verlauf der Beantragung bei der Berechtigungsprüfung.

4.1 Randbedingungen

Die Beantragung einer SMC-B ORG ist an unterschiedliche Rahmenbedingungen gebunden. Sowohl die Form der Beantragung als auch die zugelassenen Akteure und deren berechtigte Vertreter müssen bestimmte Kriterien erfüllen, welche im noch zu erstellenden Dokument zur Ausgabe-Policy der SMC-B Org[gemRL_SMC-B_ORG_AP] beschrieben sind.

5 Format der Zertifikate

Herausgeber der Zertifikate sind in jedem Fall die bei der gematik zugelassenen TSP-X.509 nonQES. Die Zertifikate sind gemäß [gemSpec_PKI] Kap. 5.3.4 ff spezifiziert.

Aktuell werden sowohl RSA- als auch ECC-Zertifikate erzeugt und herausgegeben.

Die herausgegebenen Zertifikate besitzen unterschiedliche Ausprägungen, welche immer als Attribute in das Zertifikat eingelassen von einer ausstellenden Zertifizierungsstelle (ROOT- oder SUB-CA) digital signiert werden.

Unterschiedliche Ausprägungen sind insbesondere bei den folgenden Attributen vorgesehen:

Tabelle 1: Attribute der SMB-B-ORG mit unterschiedlichen Ausprägungen

| | |
|--------------------------------|---|
| commonName | Eineindeutiger Bezeichner innerhalb der TI |
| organisationName | Organisationsname (Normallänge) |
| SubjectAltNames | Alternativer Organisationsname (Überlänge) |
| CRLDistributionPoints | Veröffentlichungspunkt der Sperrliste |
| Admission / admissionAuthority | Leitende Organisation für Unterorganisationen des Sektors oder ggf. leitende Organisation für sich selbst |
| Admission / professionItem | Berufsbezeichnung des Sektors ^{*1)} |
| Admission / professionOID | OID für Organisationen ^{*2)} |
| Admission / registrationNumber | im Handelsregister eingetragene Registernummer |

**1) Das professionItem steht für die textuelle Darstellung einer Berufsbezeichnung eines Leistungserbringers in einem Sektor (bspw. professionItem „Zahnarzt“).*

**2) Die professionOID ist ein zahlenbasiertes Identifikationsmerkmal, welches das professionItem maschinenlesbar darstellt.*

Die Wertebereiche variabler Attribute innerhalb der Zertifikate sind durch die Konzeptlage bereits in anderen Dokumenten vorgegeben und sollen hier nicht erneut spezifiziert werden.

5.1 Herausgeber von SMC-B ORG

Aussteller von Zertifikaten (TSP-X.509 nonQES), welche bereits eine Zulassung für die Ausstellung von SMC-B erhalten haben, sind ebenso berechtigt, entsprechende Zertifikate im Zertifikatsprofil SMC-B ORG auszustellen. TSP können berechtigt sein, für mehrere auch unterschiedliche Sektoren TSP-X.509 nonQES-Zertifikate herauszugeben. Die Berechtigung zur Herausgabe von SMC-B ORG in einem Sektor berechtigt ebenfalls auch zur Erzeugung oder Ausstellung von SMC-B ORG für einen anderen Sektor, gleichwohl der TSP-X.509 nonQES berechtigt sein kann, für diesen Sektor andere SMC-B herauszugeben. Berechtigungen werden disjunkt für die einzelnen Typen von SMC-B erteilt. Verwendet werden auf der SMC-B ORG die folgenden Zertifikatstypen (siehe Kap. 6.1 [gemSpec_PKI])

- 5.3.4.1 C.HCI.AUT gemäß Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B
- 5.3.4.2 C.HCI.ENC gemäß Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B
- 5.3.4.3 C.HCI.OSIG gemäß Tab_PKI_240 C.HCI.OSIG Signatur SMC-B

5.1.1 X.509 Zertifikatsprofil der SMC-B ORG

Herausgeberspezifische Ausprägungen zu einzelnen Zertifikatsfeldern sind in einer ergänzenden Tabelle unterhalb des Profils aufgeführt.

Die Kardinalität (Kar.) ist wie folgt zu interpretieren:

- 0 = dieses Attribut DARF NICHT gefüllt sein;
- 0 - 1 = dieses Attribut SOLL bzw. KANN gefüllt sein;
- 1 = dieses Attribut MUSS gefüllt sein.

Besonderheiten in den Ausprägungen der Zertifikate:

Tabelle 2: Tab_SMCB_ORG_Herausgeber - Herausgeberspezifische Felder im SMC-B ORG Profil

| | KZBV | Kar. | KBV | Kar. | GKV-SV | Kar. |
|--------------------------------|---|------|---|------|--|------|
| commonName | Gemäß Freigabedaten der Herausgeberin | 1 | Gemäß Freigabedaten der Herausgeberin | 1 | Gemäß Freigabedaten des Herausgebers | 1 |
| organizationName | Telematik-ID gemäß Freigabedaten der KZBV | 1 | Telematik-ID gemäß Freigabedaten der KBV | 1 | Spitzenverband Bund der Krankenkassen gemäß § 217a SGB V | 1 |
| SubjectAltNames | Komplettangabe zur betreffenden KZV | 0-1 | Komplettangabe zur betreffenden KV | 0-1 | Nicht belegt | 0-1 |
| CRLDistributionPoints | CDP des TSP für das betreffende Zertifikat | 1 | CDP des TSP für das betreffende Zertifikat | 1 | CDP des TSP für das betreffende Zertifikat | 1 |
| Admission / admissionAuthority | admissionAuthority = {O=Kassenzahnärztliche Bundesvereinigung, C=DE} | 1 | admissionAuthority = {O= Kassenärztliche Bundesvereinigung, C=DE} | 1 | admissionAuthority = {O= GKV-Spitzenverband, C=DE} | 1 |
| Admission / professionItem | professionItem = Beschreibung zu <oid_leo_zahnaerzte> gemäß [gemSpec_OID#GS-A_4443] | 1 | professionItem = Beschreibung zu <oid_leo_kassenaerztliche_vereinigung> gemäß [gemSpec_OID#GS-A_4443] | 1 | professionItem = Beschreibung zu <oid_bs_gkv_spitzenverband> gemäß [gemSpec_OID#GS-A_4443] | 1 |

| | | | | | | |
|---------------------------------------|---|-----------------------|---|-----------------------|---|---|
| Admission / professionOID | professionOID = <oid_leo_zahnaerzte> gemäß [gemSpec_OID#GS-A_4443] | 1 | professionOID = <oid_leo_kassenaerztliche_vereinigung> gemäß [gemSpec_OID#GS-A_4443] | 1 | professionOID = <oid_bs_gkv_spitzenverband> gemäß [gemSpec_OID#GS-A_4443] | 1 |
| Admission / registration Number | registrationNumber <Telematik-ID gemäß Freigabedaten der KZBV> | 1 | registrationNumber <Telematik-ID gemäß Freigabedaten der KBV> | 1 | registrationNumber <Telematik-ID gemäß Freigabedaten des GKV-SV> | 1 |
| | DKG (als Herausgeberin für sich selbst) | K ar . | DKG (als Herausgeberin für ihren Sektor) | K ar . | | |
| commonName | Gemäß Freigabedaten der Herausgeberin | 1 | Gemäß Freigabedaten der Herausgeberin | 1 | | |
| organization Name | Telematik-ID gemäß Freigabedaten der DKG | 1 | Telematik-ID gemäß Freigabedaten der DKG | 1 | | |
| SubjectAltNames | Komplettangabe zum betreffenden Krankenhausverband | 0- 1 | nicht belegt | 0- 1 | | |
| CRLDistributionPoints | CDP des TSP für das betreffende Zertifikat | 1 | CDP des TSP für das betreffende Zertifikat | 1 | | |
| Admission / admissionAuthority | admissionAuthority = {O=Deutsche Krankenhausgesellschaft, C=DE} | 1 | admissionAuthority = {O= Deutsche Krankenhausgesellschaft, C=DE} | 1 | | |
| Admission / professionItem | professionItem = Beschreibung zu <oid_leo_krankenhausesverband> gemäß [gemSpec_OID#GS-A_4443] | 1 | professionItem = Beschreibung zu <oid_leo_dkg> oder <oid_leo_dktig> gemäß [gemSpec_OID#GS-A_4443] | 1 | | |
| Admission / professionOID | professionOID = <oid_leo_krankenhausesverband> gemäß [gemSpec_OID#GS-A_4443] | 1 | professionOID = <oid_leo_dkg> oder <oid_leo_dktig> gemäß [gemSpec_OID#GS-A_4443] | 1 | | |

| | | | | | | |
|---------------------------------------|--|-----------------------|---|-----------------------|--|--|
| Admission / registration Number | registrationNumber <Telematik-ID gemäß Freigabedaten der DKG> | 1 | registrationNumber <Telematik-ID gemäß Freigabedaten der DKG> | 1 | | |
| | DAV (als Herausgeber für ihren Sektor) | K ar . | DAV (als Herausgeber für sich selbst) | K ar . | | |
| commonNa me | Gemäß Freigabedaten des Herausgebers | 1 | Gemäß Freigabedaten des Herausgebers | 1 | | |
| organization Name | Telematik-ID gemäß Freigabedaten des DAV | 1 | Telematik-ID gemäß Freigabedaten des DAV | 1 | | |
| SubjectAltN ames | Komplettangabe zum betreffenden Apothekerverband | 0- 1 | nicht belegt | 0- 1 | | |
| CRLDistribut ionPoints | CDP des TSP für das betreffende Zertifikat | 1 | CDP des TSP für das betreffende Zertifikat | 1 | | |
| Admission / admissionAu thority | admissionAuthority = {O=Deutscher Apothekerverband, C=DE} | 1 | admissionAuthority = {O= Deutscher Apothekerverband, C=DE} | 1 | | |
| Admission / professionIt em | professionItem = Beschreibung zu <oid_leo_apotheker verband> gemäß [gemSpec_OID#GS- A_4443] | 1 | professionItem = Beschreibung zu <oid_leo_dav> gemäß [gemSpec_OID#GS- A_4443] | 1 | | |
| Admission / professionOI D | professionOID = <oid_leo_apotheker verband> gemäß [gemSpec_OID#GS- A_4443] | 1 | professionOID = <oid_leo_dav> gemäß [gemSpec_OID#GS- A_4443] | 1 | | |
| Admission / registration Number | registrationNumber <Telematik-ID gemäß Freigabedaten des DAV> | 1 | registrationNumber <Telematik-ID gemäß Freigabedaten des DAV> | 1 | | |

| | BÄK (als Herausgeber für ihren Sektor) | K ar . | BÄK (als Herausgeber für sich selbst) | K ar . | BZÄK | K ar . |
|--------------------------------|---|-----------------------|---|-----------------------|---|-----------------------|
| commonName | Gemäß Freigabedaten der Herausgeberin | 1 | Gemäß Freigabedaten der Herausgeberin | 1 | Gemäß Freigabedaten der Herausgeberin | 1 |
| organizationName | Telematik-ID gemäß Freigabedaten der BÄK | 1 | Telematik-ID gemäß Freigabedaten der BÄK | 1 | Nicht belegt | 1 |
| SubjectAltNames | Komplettangabe zur betreffenden Ärztekammer | 1 | nicht belegt | 0-1 | Komplettangabe zur betreffenden Landes Zahnärztekammer | 1 |
| CRLDistributionPoints | nicht belegt | 0 | nicht belegt | 0 | CDP des TSP für das betreffende Zertifikat | 1 |
| Admission / admissionAuthority | admissionAuthority = {O= Bundesärztekammer, C=DE} | 1 | admissionAuthority = {O= Bundesärztekammer, C=DE} | 1 | admissionAuthority = {O= Bundeszahnärztekammer, C=DE} | 1 |
| Admission / professionItem | professionItem = Beschreibung zu < oid_leo_Aerztekammer > gemäß gemSpec_OID#GS-A_4443 | 1 | professionItem = Beschreibung zu < oid_leo_baek > gemäß gemSpec_OID#GS-A_4443 | 1 | professionItem = Beschreibung zu < oid_leo_Zahnaerztekammer > gemäß gemSpec_OID#GS-A_4443 | 1 |
| Admission / professionOID | professionOID = < oid_leo_Aerztekammer > ; gemäß gemSpec_OID#GS-A_4443 | 1 | professionOID = < oid_leo_baek > ; gemäß gemSpec_OID#GS-A_4443 | 1 | professionOID = < oid_leo_Zahnaerztekammer > ; gemäß gemSpec_OID#GS-A_4443 | 1 |
| Admission / registrationNumber | registrationNumber <Telematik-ID gemäß Freigabedaten der BÄK> | 1 | registrationNumber <Telematik-ID gemäß Freigabedaten der BÄK> | 1 | registrationNumber <Telematik-ID gemäß Freigabedaten der BZÄK> | 1 |

6 Anhang C - Verzeichnisse

6.1 Abkürzungen

| Abkürzung | Bedeutung |
|------------------------|---|
| BÄK | Bundesärztekammer |
| BZÄK | Bundeszahnärztekammer |
| CRL | Certificate Revocation List |
| CV- Zertifikate/CVC | Card Verifiable Certificate |
| DAV | Deutscher Apothekerverband e.V. |
| DKG | Deutsche Krankenhausgesellschaft |
| DKTIG | Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH |
| GKV-SV | Spitzenverband Bund der Krankenkassen |
| KBV | Kassenärztliche Bundesvereinigung |
| KOM-LE | Kommunikation für Leistungserbringer |
| KV | Kassenärztliche Vereinigungen |
| KZBV | Kassenzahnärztliche Bundesvereinigung |
| KZV | Kassenzahnärztliche Vereinigungen |
| LÄK | Landesärztekammern und berechtigte Bezirksärztekammern |
| LAV | Landesapothekerverbände |
| LZÄK | Landeszahnärztekammern |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier (dient zur eindeutigen Referenzierung zu Objekten) |

| | |
|------------------|---|
| SMC-B ORG | Security Module Card vom Type B für Organisationen |
| SMC-B-LEI | Securoty Module Card vom Type B für Leistungserbringerinstitutionen |
| TI | Telematikinfrastruktur |
| TSP-CVC | Trust Service Provider für Karten Validierungs-Zertifikate (siehe CV-Zertifikate) |
| TSP-X.509 nonQES | Trust Service Provider für nicht qualifizierte X.509 Zertifikate |

6.2 Glossar

Das offizielle Glossar der gematik finden Sie unter folgendem Link:
<https://fachportal.gematik.de/glossar/>

6.3 Referenzierte Dokumente

6.4 Dokumente der gematik

| Referenzierung | Dokumentbezeichnung |
|----------------------|--|
| [gemRL_TSL_SP_CP] | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL |
| [gemSpec_OID] | Spezifikation Festlegung von OIDs (gematik) |
| [gemSpec_PKI] | Übergreifende Spezifikation PKI (gematik) |
| [gemRL_SMC-B_ORG_AP] | Dokument wird erst noch erstellt |

6.5 Tabellenverzeichnis

Tabelle 1: Attribute der SMB-B-ORG mit unterschiedlichen Ausprägungen 8

Tabelle 2: Tab_SMCB_ORG_Herausgeber - Herausgeberspezifische Felder im SMC-B ORG Profil 9

|