

Einführung der Gesundheitskarte

Produkttypsteckbrief

Prüfvorschrift

SMC-B

Zulassungsobjekt SMC-B-Objektsystem

Produkttypversion: 4.3.0

Produkttypstatus: freigegeben

Version: 1.0.0

Revision: \main\rel_ors1\4

Stand: 24.07.2015

Status: freigegeben

Klassifizierung: öffentlich

Referenz: [gemProdT_SMC-B_ObjSys_PTV4.3.0]

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die Anforderungslage für den Produkttyp ändert und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttypversion	Beschreibung der Änderung	Referenz
2.0.0	Initiale Version G2-Karten für Vergabeverfahren	[gemProdT_SMC-B_PTV2.0.0]
2.0.1	Anpassung Produkttypversion auf Stand ORS1 vom 22.04.13	[gemProdT_SMC-B_PTV2.0.1]
2.0.2	Anpassung an G2 Los 1 / 2 Iteration 1	[gemProdT_SMC-B_ObjSys_PTV2.0.2]
4.0.0	Anpassung an G2 Iteration 2	[gemProdT_SMC-B_ObjSys_PTV4.0.0]
4.0.1	Anpassung an G2 Iteration 2b	[gemProdT_SMC-B_ObjSys_PTV4.0.1]
4.1.0	Anpassung an G2 Iteration 3	[gemProdT_SMC-B_ObjSys_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4	[gemProdT_SMC-B_ObjSys_PTV4.2.0]
4.3.0	Einarbeitung der Errata R1.4.1 bis R1.4.6	[gemProdT_SMC-B_ObjSys_PTV4.3.0]

Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	24.07.15		freigegeben	gematik

Änderungen zur Vorversion [gemProdT_SMC-B_ObjSys_PTV4.2.0] V1.0.1:

- 1) Farbige Markierungen und Kommentare aus Dokument entfernt.
- 2) Deckblatt und Historie und Versionsnummern in Kapitel 2 aktualisiert.
- 3) Durch Errata geänderte Anforderungen gelb markiert.
- 4) Text in 5.3.1 wegen LA Beschluss zu D_1064 überarbeitet.

Inhaltsverzeichnis

Historie Produkttypversion und Produkttypsteckbrief	2
Inhaltsverzeichnis	3
1 Einführung.....	5
1.1 Zielsetzung und Einordnung des Dokumentes	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzung des Dokumentes	6
1.5 Methodik.....	6
2 Dokumente	7
3 Blattanforderungen.....	8
3.1 Anforderungen zur funktionalen Eignung	8
3.1.1 Produkttest / Produktübergreifender Test	8
3.1.2 Herstellererklärung funktionale Eignung	11
3.2 Anforderungen zur sicherheitstechnischen Eignung	12
3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie ..	12
3.2.2 CC-Evaluierung	15
3.2.3 Sicherheitsgutachten	15
3.2.4 Sicherheitsbestätigung	15
3.2.5 Herstellerklärung sicherheitstechnische Eignung.....	15
3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	16
3.4 Anforderungen zur betrieblichen Eignung	16
3.4.1 Prozessprüfung betriebliche Eignung	17
3.4.2 Herstellererklärung betriebliche Eignung	17
4 Umsetzungsanforderungen	18
5 Produkttypspezifische Merkmale	19
5.1 Angaben zu EF.Version2.....	19
5.2 Optionale Ausprägungen	19
5.3 Variationen	19
5.3.1 Freischaltung der SMC-B durch andere Karten	19
Anhang A - Verzeichnisse	20
A1 - Abkürzungen.....	20

A2 – Tabellenverzeichnis.....	20
A3 - Referenzierte Dokumente.....	20

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an die Herstellung des Zulassungsobjektes SMC-B-Objektsystem in der Produkttypversion 4.3.0 oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen ¹ durch die gematik.

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief für das Zulassungsobjekt SMC-B-Objektsystem richtet sich an SMC-B-Objektsystem-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- akkreditierten Materialprüflaboren
- Auditoren

Die Anforderungen beziehen sich auf den Hersteller des Zulassungsobjektes SMC-B-Objektsystem.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekannt gegeben.

¹ Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.

1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für das Zulassungsobjekt SMC-B-Objektsystem sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten Anforderungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

Afo-ID: Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Afo-Bezeichnung: Gibt den Titel einer Anforderung informativ wider, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der Anforderung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die Anforderung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für das Zulassungsobjekt SMC-B-Objektsystem normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu dem Zulassungsobjekt

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemSpec_Krypt	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.4.0
gemSpec_OM	gematik: Spezifikation Operations und Maintenance (Fehlermanagement, Versionierung, Monitoring)	1.6.0
gemSpec_PKI	gematik: Spezifikation PKI	1.7.0
gemSpec_Sich_DS	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen	1.2.0
gemSpec_SMC-B_ObjSys	gematik: Spezifikation der Security Module Card SMC-B Objektsystem	3.8.0
gemSpec_Karten_Fach_TIP	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI	2.4.1

Tabelle 2: Mitgeltende Dokumente

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemSpec_TLK_COS_G2	gematik: Spezifikation Testlaborkarte COS / Objektsysteme	1.5.0
gemSpec_OID	gematik: Spezifikation Festlegung von OIDs	2.8.0
TR-03143	BSI: eHealth G2-COS Konsistenz-Prüftool	1.0

Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für das Zulassungsobjekt SMC-B-Objektsystem normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Zulassungsobjektes SMC-B-Objektsystem notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest / Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Zulassungsobjektes SMC-B-Objektsystem verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

**Tabelle 3: Anforderungen zur funktionalen Eignung
"Produkttest / Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3483	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP
GS-A_4377	Card-to-Card-Authentisierung G1	gemSpec_Krypt
GS-A_4379	Card-to-Card-Authentisierung G2	gemSpec_Krypt
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	gemSpec_OM
GS-A_4668	Prüfung der mathematischen Korrektheit bei CV-Zertifikaten der Generation G1	gemSpec_PKI
GS-A_5009	Prüfung der mathematischen Korrektheit von CV-Zertifikate der Generation 2	gemSpec_PKI
GS-A_5010	Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers	gemSpec_PKI
GS-A_5011	Prüfung der Gültigkeit von CV-Zertifikaten der Generation G2	gemSpec_PKI
GS-A_5012	Prüfung von CV-Zertifikaten der Generation 2	gemSpec_PKI
Card-G2-A_2196	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_SMC-B_ObjSys
Card-G2-A_2138	K_Terminal: Ausschluss kontaktlose Schnittstelle	gemSpec_SMC-B_ObjSys
Card-G2-A_3036	K_SMC-B: USB-Schnittstelle	gemSpec_SMC-B_ObjSys
Card-G2-A_3037	K_SMC-B: Vorhandensein einer USB-Schnittstelle	gemSpec_SMC-B_ObjSys
Card-G2-A_3188	K_SMC-B: Vorhandensein Option_Kryptobox	gemSpec_SMC-B_ObjSys
Card-G2-A_2134	K_Initialisierung: Änderung von Zugriffsregeln	gemSpec_SMC-B_ObjSys
Card-G2-A_2135	K_Initialisierung: Verwendung von SE	gemSpec_SMC-B_ObjSys
Card-G2-A_3189	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys
Card-G2-A_3190	K_Initialisierung: Eigenschaften der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys
Card-G2-A_2136	K_Initialisierung: Ordnerattribute	gemSpec_SMC-B_ObjSys
Card-G2-A_2137	K_Initialisierung: Dateiattribut	gemSpec_SMC-B_ObjSys
Card-G2-A_2668	K_Initialisierung und K_Personalisierung: Wert von „positionLogicalEndOfFile“	gemSpec_SMC-B_ObjSys
Card-G2-A_2669	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_SMC-B_ObjSys
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys
Card-G2-A_2139	K_Initialisierung: Wert des Attributes root	gemSpec_SMC-B_ObjSys
Card-G2-A_2140	K_Initialisierung und K_Personalisierung: Wert des Attributes answerToReset	gemSpec_SMC-B_ObjSys
Card-G2-A_2142	K_Initialisierung: Inhalt persistentPublicKeyList	gemSpec_SMC-B_ObjSys
Card-G2-A_3187	K_Initialisierung: Größe persistentPublicKeyList	gemSpec_SMC-B_ObjSys
Card-G2-A_3267	K_Initialisierung: Wert von pointInTime	gemSpec_SMC-B_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3340	K_Initialisierung und K_Personalisierung: ATR-Kodierung	gemSpec_SMC-B_ObjSys
Card-G2-A_3341	K_Initialisierung und K_Personalisierung: TC1 Byte im ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3342	K_Initialisierung und K_Personalisierung: Historical Bytes im ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3343	K_Initialisierung und K_Personalisierung: Vorgaben für Historical Bytes	gemSpec_SMC-B_ObjSys
Card-G2-A_2143	K_ K_Initialisierung und K_Personalisierung: Kompatibilität zu G1-Karten	gemSpec_SMC-B_ObjSys
Card-G2-A_2146	K_Initialisierung: Initialisierte: Attribute von MF	gemSpec_SMC-B_ObjSys
Card-G2-A_2147	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3344	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_2154	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_SMC-B_ObjSys
Card-G2-A_2156	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_SMC-B_ObjSys
Card-G2-A_2158	K_Initialisierung: Initialisierte Attribute von MF / EF.Version2	gemSpec_SMC-B_ObjSys
Card-G2-A_2159	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2160	K_Initialisierung: Initialisierte Attribute MF / EF.C.CA_SMC.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2162	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2163	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2169	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2171	K_Initialisierung: Initialisierte Attribute von MF / PIN.SMC	gemSpec_SMC-B_ObjSys
Card-G2-A_2173	K_Initialisierung: Freischaltung der SMC-B einer Institution (PrK.SMC.AUTR_CVC.R2048)	gemSpec_SMC-B_ObjSys
Card-G2-A_3352	K_Initialisierung: Freischaltung für PrK.SMC.AUTR_CVC.R2048 der SMC-B	gemSpec_SMC-B_ObjSys
Card-G2-A_2176	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2177	K_Initialisierung: Freischaltung der SMC-B einer Institution (PrK.SMC.AUTR_CVC.E256)	gemSpec_SMC-B_ObjSys
Card-G2-A_3354	K_Initialisierung: Freischaltung für PrK.SMC.AUTR_CVC.E256 der SMC-B	gemSpec_SMC-B_ObjSys
Card-G2-A_2180	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2189	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2191	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.R2048	gemSpec_SMC-B_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_2192	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3039	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2194	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_2195	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3360	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3362	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_2197	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA	gemSpec_SMC-B_ObjSys
Card-G2-A_2198	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / EF.SMD	gemSpec_SMC-B_ObjSys
Card-G2-A_2199	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / EF.CONF	gemSpec_SMC-B_ObjSys
Card-G2-A_2200	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / EF.NET	gemSpec_SMC-B_ObjSys
Card-G2-A_2201	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / PIN.CONF	gemSpec_SMC-B_ObjSys
Card-G2-A_2202	K_Initialisierung: Länge der PUK für PIN.Conf	gemSpec_SMC-B_ObjSys
Card-G2-A_2203	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN	gemSpec_SMC-B_ObjSys
Card-G2-A_2204	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2207	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2210	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2217	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2220	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2223	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Zulassungsobjektes SMC-B-Objektsystem verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zugesagt.

Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Prüfung gemäß Technischer Richtlinie TR-03144 nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Zertifikates nach TR-03144.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3483	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	gemSpec_OM
Card-G2-A_2196	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_SMC-B_ObjSys
Card-G2-A_2138	K_Terminal: Ausschluss kontaktlose Schnittstelle	gemSpec_SMC-B_ObjSys
Card-G2-A_2134	K_Initialisierung: Änderung von Zugriffsregeln	gemSpec_SMC-B_ObjSys
Card-G2-A_2135	K_Initialisierung: Verwendung von SE	gemSpec_SMC-B_ObjSys
Card-G2-A_3189	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys
Card-G2-A_3190	K_Initialisierung: Eigenschaften der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys
Card-G2-A_2136	K_Initialisierung: Ordnerattribute	gemSpec_SMC-B_ObjSys
Card-G2-A_2137	K_Initialisierung: Dateiattribute	gemSpec_SMC-B_ObjSys
Card-G2-A_2668	K_Initialisierung und K_Personalisierung: Wert von „positionLogicalEndOfFile“	gemSpec_SMC-B_ObjSys
Card-G2-A_2669	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_SMC-B_ObjSys
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys
Card-G2-A_2139	K_Initialisierung: Wert des Attributes root	gemSpec_SMC-B_ObjSys
Card-G2-A_2140	K_Initialisierung und K_Personalisierung: Wert des Attributes answerToReset	gemSpec_SMC-B_ObjSys
Card-G2-A_2142	K_Initialisierung: Inhalt persistentPublicKeyList	gemSpec_SMC-B_ObjSys
Card-G2-A_3187	K_Initialisierung: Größe persistentPublicKeyList	gemSpec_SMC-B_ObjSys
Card-G2-A_3267	K_Initialisierung: Wert von pointInTime	gemSpec_SMC-B_ObjSys
Card-G2-A_3340	K_Initialisierung und K_Personalisierung: ATR-Kodierung	gemSpec_SMC-B_ObjSys
Card-G2-A_3341	K_Initialisierung und K_Personalisierung: TC1 Byte im ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3342	K_Initialisierung und K_Personalisierung: Historical Bytes im ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3343	K_Initialisierung und K_Personalisierung: Vorgaben für Historical Bytes	gemSpec_SMC-B_ObjSys
Card-G2-A_2143	K_Initialisierung und K_Personalisierung: Kompatibilität zu G1-Karten	gemSpec_SMC-B_ObjSys
Card-G2-A_2146	K_Initialisierung: Initialisierte Attribute von MF	gemSpec_SMC-B_ObjSys
Card-G2-A_2147	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3344	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_2154	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_SMC-B_ObjSys
Card-G2-A_2156	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_SMC-B_ObjSys
Card-G2-A_2158	K_Initialisierung: Initialisierte Attribute von MF / EF.Version2	gemSpec_SMC-B_ObjSys
Card-G2-A_2159	K_Initialisierung: Initialisierte Attribute von MF / EF.CA_SMC.CS.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2160	K_Initialisierung: Initialisierte Attribute MF / EF.CA_SMC.CS.E256	gemSpec_SMC-B_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_2162	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2163	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2169	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2171	K_Initialisierung: Initialisierte Attribute von MF / PIN.SMC	gemSpec_SMC-B_ObjSys
Card-G2-A_2173	K_Initialisierung: Freischaltung der SMC-B einer Institution (PrK.SMC.AUTR_CVC.R2048)	gemSpec_SMC-B_ObjSys
Card-G2-A_3352	K_Initialisierung: Freischaltung für PrK.SMC.AUTR_CVC.R2048 der SMC-B	gemSpec_SMC-B_ObjSys
Card-G2-A_2176	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2177	K_Initialisierung: Freischaltung der SMC-B einer Institution (PrK.SMC.AUTR_CVC.E256)	gemSpec_SMC-B_ObjSys
Card-G2-A_3354	K_Initialisierung: Freischaltung für PrK.SMC.AUTR_CVC.E256 der SMC-B	gemSpec_SMC-B_ObjSys
Card-G2-A_2180	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2189	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2191	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2192	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3039	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_2194	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_2195	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3360	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3362	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_2197	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA	gemSpec_SMC-B_ObjSys
Card-G2-A_2198	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / EF.SMD	gemSpec_SMC-B_ObjSys
Card-G2-A_2199	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / EF.CONF	gemSpec_SMC-B_ObjSys
Card-G2-A_2200	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / EF.NET	gemSpec_SMC-B_ObjSys
Card-G2-A_2201	K_Initialisierung: Initialisierte Attribute von MF / DF.SMA / PIN.CONF	gemSpec_SMC-B_ObjSys
Card-G2-A_2202	K_Initialisierung: Länge der PUK für PIN.Conf	gemSpec_SMC-B_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_2203	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN	gemSpec_SMC-B_ObjSys
Card-G2-A_2204	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2207	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2210	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2217	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2220	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2223	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys

3.2.2 CC-Evaluierung

Eine Zertifizierung nach ITSEC [ITSEC] oder Common Criteria ist nicht erforderlich.

3.2.3 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Anforderungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor.	

3.2.4 Sicherheitsbestätigung

Eine Sicherheitsbestätigung gemäß Signaturgesetz [SigG01] und Signaturverordnung [SigV01] ist nicht erforderlich.

3.2.5 Herstellerklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_4363	CV-Zertifikate G1	gemSpec_Krypt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4364	CV-CA-Zertifikate G1	gemSpec_Krypt
GS-A_4365	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_4380	Card-to-Server (C2S) Authentisierung und Trusted Channel G2	gemSpec_Krypt
GS-A_4381	Schlüssellängen Algorithmus AES	gemSpec_Krypt
GS-A_2524	Produktunterstützung: Nutzung des Problem-Management-Prozesses	gemSpec_Sich_DS
GS-A_2525	Hersteller: Schließen von Schwachstellen	gemSpec_Sich_DS
GS-A_2354	Produktunterstützung mit geeigneten Sicherheits-Technologien	gemSpec_Sich_DS
GS-A_2350	Produktunterstützung der Hersteller	gemSpec_Sich_DS

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Der Produkttyp erfordert den Nachweis der elektrischen, mechanischen und physikalischen Eignung. Sofern dabei spezifische Anforderungen der gematik zu beachten sind, werden diese nachfolgend aufgeführt. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3478	Elektrophysikalische Eigenschaften des Kartenkörpers der (g)SMC	gemSpec_SMC_OPT
Card-G2-A_3513	Bemaßung der Kontakte der (g)SMC	gemSpec_SMC_OPT

3.4 Anforderungen zur betrieblichen Eignung

Anforderungen zur betrieblichen Eignung wenden sich an Anbieter von Diensten zu dem Produkttyp (Service Provider).

3.4.1 Prozessprüfung betriebliche Eignung

Sofern in diesem Abschnitt Anforderungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss deren Erfüllung im Rahmen von Prozessprüfungen nachgewiesen werden.

Tabelle 9: Anforderungen zur betrieblichen Eignung "Prozessprüfung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor.	

3.4.2 Herstellererklärung betriebliche Eignung

Sofern in diesem Abschnitt Anforderungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch eine Herstellererklärung bestätigen bzw. zusagen.

Tabelle 10: Anforderungen zur betrieblichen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor.	

4 Umsetzungsanforderungen

Für die folgenden dargestellten Anforderungen (Umsetzungsanforderungen) ist eine Verfeinerung und Konkretisierung zu Blattanforderungen erforderlich, bevor die konkrete und vollständige Herstellung und der Betrieb von Produkten des Zulassungsobjektes SMC-B-Objektsystem möglich ist. Die Umsetzungsanforderungen werden in einer zukünftigen Version des Produkttypsteckbriefs durch neue verfeinerte und konkretisierte Blattanforderungen in Kapitel 3 ersetzt.

Tabelle 11: Offene Umsetzungsanforderungen an das Zulassungsobjekt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor.	

5 Produkttypspezifische Merkmale

5.1 Angaben zu EF.Version2

Die detaillierte Versionskennzeichnung der SMC-B wird im Dokument [gemSpec_Karten_Fach_TIP] festgelegt.

5.2 Optionale Ausprägungen

In diesem Kapitel werden die optionalen Ausprägungen des Produkttyps SMC-B-Objektsystem beschrieben. Die Spezifikationen des COS und des Objektsystems der SMC-B-Objektsystem lassen folgende Optionen zu:

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec_SMC-B_ObjSys#4.3.2]
- Bereitstellung der Funktion Kryptobox gemäß [gemSpec_SMC-B_ObjSys#4.3.3]

Die SMC-B kann gemäß [gemSpec_SMC-B_ObjSys#2] als Testkarte ausgestaltet werden.

5.3 Variationen

5.3.1 Freischaltung der SMC-B durch andere Karten

Gemäß Card-G2-A_2192 ist der Wert der Flaglist im CHAT fälschlicherweise so gesetzt, dass eine Freischaltung der SMC-B durch andere Karten nicht möglich ist. Dieser Fehler wird nicht behoben und eine SMC-B ist demzufolge stets per PIN.SMC freizuschalten. Gemäß Card-G2-A_2176, Card-G2-A_2180 und Card-G2-A_2184 gibt es für das Zulassungsobjekt Objektsystem SMC-B sechs verschiedene Möglichkeiten, die AUTR-Schlüssel einer SMC-B durch eine andere Karte freischalten zu können (Freischaltung durch die PIN.SMC oder durch eines der Profile 2A, 2ZA, 3, 4, 5 oder Freischaltung nur durch die PIN.SMC für die Profile 1, 7-10). Für die Zulassung des Zulassungsobjektes SMC-B-Objektsystem muss für jede der sechs Möglichkeiten ein separates ein Image in der Variante Profile 2A zum Test an die gematik übermittelt werden. Für die Zulassung des Zulassungsobjektes SMC-B-Objektsystem ist ein positives Testergebnis für alle sechs dieses Images notwendig.

Anhang A - Verzeichnisse

A1 - Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

A2 – Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu dem Zulassungsobjekt.....	7
Tabelle 2: Mitgeltende Dokumente.....	7
Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"	8
Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"	12
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie"	12
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"...	15
Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"	15
Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	16
Tabelle 9: Anforderungen zur betrieblichen Eignung "Prozessprüfung"	17
Tabelle 10: Anforderungen zur betrieblichen Eignung "Herstellererklärung"	17
Tabelle 11: Offene Umsetzungsanforderungen an das Zulassungsobjekt.....	18

A3 - Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[BSI_2006a]	BSI (29.09.2006): Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria) https://www.bsi.bund.de/Schutzprofile
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung

Produkttypsteckbrief
SMC-B-Objektsystem
Produkttypversion: 4.3.0

[Quelle]	Herausgeber: Titel, Version
[ITSEC]	BMI bzw. GMBI: (28.06.1991): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik („Information Technology Security Evaluation Criteria) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile
[SigG01]	Bundesgesetzblatt I (2001), S.876: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)