Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

SMC-B

Zulassungsobjekt SMC-B-Objektsystem

Produkttyp Version:	4.5.0-0
Produkttyp Status:	freigegeben

Version:	1.0.0
Revision:	57615
Stand:	26.10.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_SMC-B_ObjSys_G2_1_PTV_4.5.0-0

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]
4.3.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_SMC-B_ObjSys_PTV4.3.0-1]
4.4.0-0	Kartengeneration 2.1	[gemProdT_SMC-B_ObjSys_PTV4.4.0-0]
4.4.1-0	Errata 1.6.4-2	[gemProdT_SMC-B_ObjSys_PTV4.4.1-0]

4.4.1-1	Anpassung an Releasestand 2.1.2	[gemProdT_SMC-B_ObjSys_PTV4.4.1-1]
4.5.0-0	Anpassung an Releasestand 2.1.3	[gemProdT_SMC-B_ObjSys_PTV4.5.0-0]

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	26.10.18		freigegeben	gematik

Inhaltsverzeichnis

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 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 durch die gematik (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.).

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 des 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.

1.4 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 wieder, 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 der Produkttypversion

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.11.0
gemSpec_Karten_Fach_TIP	Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.10.0
gemKPT_Test	Testkonzept der TI	2.1.0
gemSpec_Karten_Fach_TIP_G2_1	Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0
gemSpec_SMC-B_ObjSys	Spezifikation der Security Module Card SMC-B Objektsystem	3.11.0
gemSpec_SMC_OPT	Gemeinsame optische Merkmale der SMC	3.5.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.3.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.0.0
gemSpec_SMC-B_ObjSys_G2_1	Spezifikation der Security Module Card SMC-B Objektsystem	4.3.0

Tabelle 2: Mitgeltende Dokumente

Dokumentenkürzel	Bezeichnung des Dokuments	Version
gemSpec_TLK_COS_G2	gematik: Spezifikation Testlaborkarte COS/Objektsysteme	1.6.0
gemSpec_OID	gematik: Spezifikation Festlegung von OIDs	2.10.0
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_G2.1
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3483-01	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3490	K_Initialisierung: DO_PI_COS in	gemSpec_Karten_Fach_TIP_G2.1

	EF.ATR	
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP_G2.1
GS-A_4377	Card-to-Card-Authentisierung G1	gemSpec_Krypt
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	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_4668	Prüfung der mathematischen Korrektheit bei CV-Zertifikaten der Generation G1	gemSpec_PKI
Card-G2-A_2135	K_Initialisierung: Verwendung von SE	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2136-01	K_Initialisierung: Ordnerattribute	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2139	K_Initialisierung: Wert des Attributes root	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2140-01	K_Initialisierung und K_Personalisierung: Wert des Attributes answerToReset	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2142-01	K_Initialisierung: Inhalt persistentPublicKeyList	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2146	K_Initialisierung: Initialisierte: Attribute von MF	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2147-01	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2154-01	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2156	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_SMC-B_ObjSys_G2.1

Card-G2-A_2158-01	K_Initialisierung: Initialisierte Attribute von MF / EF.Version2	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2160-01	K_Initialisierung: Initialisierte Attribute MF / EF.C.CA_SMC.CS.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2163	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2169	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2171	K_Initialisierung: Initialisierte Attribute von MF / PIN.SMC	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2180-01	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2189	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2192-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2194-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2195-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2196	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2203	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2204	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2207	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2210-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2217-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2220-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys_G2.1

Card-G2-A_2223	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2668	K_Initialisierung und K_Personalisierung: Wert von „positionLogicalEndOfFile“	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2669	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3036	K_SMC-B: USB-Schnittstelle	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3037	K_SMC-B: Vorhandensein einer USB-Schnittstelle	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3039-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3188	K_SMC-B: Vorhandensein Option_Kryptobox	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3189	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3267-01	K_Initialisierung: Wert von pointInTime	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3340	K_Initialisierung und K_Personalisierung: ATR-Kodierung	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3341-01	K_Initialisierung und K_Personalisierung: TC1 Byte im ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3342	K_Initialisierung und K_Personalisierung: Historical Bytes im ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3343	K_Initialisierung und K_Personalisierung: Vorgaben für Historical Bytes	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3344	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3360-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3362-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3649	K_Initialisierung: Herstellerspezifischer FileIdentifier	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3650	K_Personalisierung und K_Initialisierung: TC1 Byte im ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3651	K_Initialisierung: Inhalt der Records	gemSpec_SMC-B_ObjSys_G2.1

	von EF.DIR	
Card-G2-A_3652	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3654	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3656	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3658-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3660-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3662-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3849	K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung	gemSpec_SMC-B_ObjSys_G2.1

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. zusagt.

Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_6517	Eigenverantwortlicher Test: TBV	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test

TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
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
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3648	K_Initialisierung: Fehlender FileIdentifier	gemSpec_SMC-B_ObjSys_G2.1

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_G2.1
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2.1

Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3483-01	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP_G2.1
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_4559	Versionierung der Karten der TI	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
Card-G2-A_2134	K_Initialisierung: Änderung von Zugriffsregeln	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2135	K_Initialisierung: Verwendung von SE	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2136-01	K_Initialisierung: Ordnerattribute	gemSpec_SMC-B_ObjSys_G2.1

Card-G2-A_2137	K_Initialisierung: Dateiattribute	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2138	K_Terminal: Ausschluss kontaktlose Schnittstelle	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2139	K_Initialisierung: Wert des Attributes root	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2140-01	K_Initialisierung und K_Personalisierung: Wert des Attributes answerToReset	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2142-01	K_Initialisierung: Inhalt persistentPublicKeyList	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2146	K_Initialisierung: Initialisierte: Attribute von MF	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2147-01	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2154-01	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2156	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2158-01	K_Initialisierung: Initialisierte Attribute von MF / EF.Version2	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2160-01	K_Initialisierung: Initialisierte Attribute MF / EF.C.CA_SMC.CS.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2163	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2169	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2171	K_Initialisierung: Initialisierte Attribute von MF / PIN.SMC	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2180-01	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2189	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2192-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2194-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2195-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys_G2.1

Card-G2-A_2196	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2203	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2204	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2207	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2210-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2217-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2220-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2223	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2668	K_Initialisierung und K_Personalisierung: Wert von „positionLogicalEndOfFile“	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_2669	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3039-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3187	K_Initialisierung: Größe persistentPublicKeyList	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3189	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3190	K_Initialisierung: Eigenschaften der Objekte in anderen SEs	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3267-01	K_Initialisierung: Wert von pointInTime	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3340	K_Initialisierung und K_Personalisierung: ATR-Kodierung	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3341-01	K_Initialisierung und K_Personalisierung: TC1 Byte im ATR	gemSpec_SMC-B_ObjSys_G2.1

Card-G2-A_3342	K_Initialisierung und K_Personalisierung: Historical Bytes im ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3343	K_Initialisierung und K_Personalisierung: Vorgaben für Historical Bytes	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3344	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3360-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3362-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3652	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3654	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3656	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3658-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3660-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E256	gemSpec_SMC-B_ObjSys_G2.1
Card-G2-A_3662-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.E256	gemSpec_SMC-B_ObjSys_G2.1

3.2.2 CC-Evaluierung

Eine Zertifizierung nach Common Criteria (CC) ist nicht erforderlich.

3.2.3 Herstellererklärung 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 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2330-02	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
GS-A_2350-01	Produktunterstützung der Hersteller	gemSpec_DS_Hersteller
GS-A_2354-01	Produktunterstützung mit geeigneten Sicherheitstechnologien	gemSpec_DS_Hersteller
GS-A_2524-01	Produktunterstützung: Nutzung des Problem-Management-Prozesses	gemSpec_DS_Hersteller
GS-A_2525-01	Hersteller: Schließen von Schwachstellen	gemSpec_DS_Hersteller
GS-A_4944-01	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
GS-A_4945-01	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
GS-A_4947-01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_4363	CV-Zertifikate G1	gemSpec_Krypt
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_4380	Card-to-Server (C2S) Authentisierung und Trusted Channel G2	gemSpec_Krypt
GS-A_4381	Schlüssellängen Algorithmus AES	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt

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 7: 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

4 Produkttypspezifische Merkmale

4.1 Angaben zu EF.Version2

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

4.2 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.

4.3 Variationen

4.3.1 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. Für die Zulassung des Zulassungsobjektes SMC-B-Objektsystem muss 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 dieses Image notwendig.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung