

Einführung der Gesundheitskarte

Produkttypsteckbrief

Prüfvorschrift

SMC-B

Produkttypversion: 4.4.0-2

Produkttypstatus: freigegeben

Version: 1.0.0
Revision: \main\rel_opb1\10
Stand: 21.04.2017
Status: freigegeben
Klassifizierung: öffentlich
Referenz: [gemProdT_SMC-B_PTV4.4.0-2]

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 und 2a	[gemProdT_SMC-B_PTV2.0.2]
4.0.0	Anpassung an G2 Iteration 2b	[gemProdT_SMC-B_PTV4.0.0]
4.1.0	Anpassung an G2 Iteration 3 und Release 1.3.0	[gemProdT_SMC-B_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4 und Release 1.4.0	[gemProdT_SMC-B_PTV4.2.0]
4.3.0	Einarbeitung der Errata R1.4.1 bis R1.4.6	[gemProdT_SMC-B_PTV4.3.0]
4.3.1	Anpassung Produkttypversion auf Stand OPB1 vom 25.04.16	[gemProdT_SMC-B_PTV4.3.1]
4.4.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_SMC-B_PTV4.4.0-1]
4.4.0-2	Anpassung auf Releasestand 1.6.4	[gemProdT_SMC-B_PTV4.4.0-2]

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.

Versio n	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	21.04.17		freigegeben	gematik

Inhaltsverzeichnis

Historie Produkttypversion und Produkttypsteckbrief	2
Inhaltsverzeichnis	3
1 Einführung.....	4
1.1 Zielsetzung und Einordnung des Dokumentes	4
1.2 Zielgruppe	4
1.3 Geltungsbereich	4
1.4 Abgrenzung des Dokumentes	5
1.5 Methodik.....	5
2 Dokumente	6
3 Blattanforderungen.....	7
3.1 Anforderungen zur funktionalen Eignung	7
3.1.1 Produkttest / Produktübergreifender Test	7
3.1.2 Herstellererklärung funktionale Eignung	9
3.2 Anforderungen zur sicherheitstechnischen Eignung	11
3.2.1 CC-Evaluierung	11
3.2.2 Sicherheitsgutachten	11
3.2.3 Herstellererklärung sicherheitstechnische Eignung.....	15
3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	16
4 Produkttypspezifische Merkmale	17
4.1 Angaben zu EF.Version2.....	17
4.2 Optionale Ausprägungen	17
4.3 Variationen	17
4.3.1 Freischaltung der SMC-B durch andere Karten	17
Anhang A – Verzeichnisse.....	19
A1 – Abkürzungen.....	19
A2 – Tabellenverzeichnis.....	19
A3 – Referenzierte Dokumente.....	19

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps SMC-B (personalisiert und bedruckt) in der Produkttypversion 4.4.0-2 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. Bestätigungen¹ 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 richtet sich an SMC-B-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 Produkttyps SMC-B.

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 den Produkttyp SMC-B 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 den Produkttyp SMC-B normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemKPT_Test	Testkonzept	1.10.0
gemRL_TSL_SP_CP	Certificate Policy	1.8.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.8.1
gemSpec_DSM	Spezifikation koordinierendes DSM	1.3.1
gemSpec_ISM	Spezifikation koordinierendes ISM	1.4.1
gemSpec_Karten_Fach_TIP	Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0
gemSpec_Krypt	Spezifikation kryptographischer Algorithmen in der TI	2.8.0
gemSpec_OM	Spezifikation Operations und Maintenance	1.8.0
gemSpec_PINPUK_TI	Übergreifende Spezifikation PIN/PUK	1.2.0
gemSpec_PKI	Spezifikation PKI (mit Anhang A)	1.12.0
gemSpec_SiBetrUmg	Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung	1.4.0
gemSpec_Sich_DS	Spezifikation Sicherheits-/Datenschutzanforderungen	1.4.1
gemSpec_SMC-B_ObjSys	Spezifikation der SMC-B Objektsystem	3.10.0
gemSpec_SMC_OPT	Gemeinsame Merkmale der SMC	3.5.0

Tabelle 2: Mitgeltende Dokumente

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemSpec_OID	gematik: Spezifikation Festlegung von OIDs	2.12.0

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 den Produkttypen SMC-B normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps SMC-B notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage einer 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 Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

Die Anforderungen werden ebenfalls als Teil der Personalisierungsvalidierung anhand von Echtkarten geprüft.

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5020	Einbringung des Komponentenzertifikats durch den Kartenherausgeber	gemRL_TSL_SP_CP
TIP1-A_2578	Korrekte ICCSN der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2589	Personalisierung des CVC-CA-Zertifikats	gemSpec_CVC_TSP
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_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3492	K_Personalisierung: DO_PT_Pers in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3494	K_Personalisierung: DO_PI_Kartenkörper in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP
Card-G2-A_3495	K_Personalisierung: DO_PI_Personalisierung in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP
Card-G2-A_3496	K_Initialisierung: Weitere Datenobjekte in DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3497	K_Personalisierung: Vollständige Befüllung von EF.ATR	gemSpec_Karten_Fach_TIP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
		P
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TI P
GS-A_4377	Card-to-Card-Authentisierung G1	gemSpec_Krypt
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	gemSpec_OM
GS-A_4560	Versionierung von Datenstrukturen der Karten der TI	gemSpec_OM
GS-A_4585	Typ der Organisation/Einrichtung des Gesundheitswesens für SMC-B	gemSpec_PKI
GS-A_4587	Gesamtlänge der Telematik-ID	gemSpec_PKI
GS-A_4710	Präfix der Telematik-ID	gemSpec_PKI
GS-A_4711	Separator der Telematik-ID	gemSpec_PKI
GS-A_4974	CV-Ausstattung von Smartcards der TI	gemSpec_PKI
GS-A_4621	Zugriffsprofil von HBA und SM-B (SMC-B, HSM-B)	gemSpec_PKI
GS-A_4624	Zugriffsprofil einer SM-B	gemSpec_PKI
Card-G2-A_2668	K_Initialisierung und K_Personalisierung: Wert von „positionLogicalEndOfFile“	gemSpec_SMC-B_ObjSys
Card-G2-A_2140	K_Initialisierung und K_Personalisierung: Wert des Attributes answerToReset	gemSpec_SMC-B_ObjSys
Card-G2-A_3035	Absicherung der Kartenadministration	gemSpec_SMC-B_ObjSys
Card-G2-A_2141	K_Personalisierung: Wert des Attributes iccsn8	gemSpec_SMC-B_ObjSys
Card-G2-A_3341	K_Initialisierung und K_Personalisierung: TC1 Byte im ATR	gemSpec_SMC-B_ObjSys
Card-G2-A_3472	K_Personalisierung: personalisierter 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_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_2157	K_Personalisierung: Personalisiertes Attribut von EF.GDO	gemSpec_SMC-B_ObjSys
Card-G2-A_3346	K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3347	K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3388	K_Personalisierung: Festlegung von CHR in MF / EF.C.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3348	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3389	K_Personalisierung: Festlegung von CHR in MF /	gemSpec_SMC-B_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	EF.C.SMC.AUTR_CVC.E256	
Card-G2-A_3349	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3390	K_Personalisierung: Festlegung von CHR in MF / EF.C.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3350	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3374	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	gemSpec_SMC-B_ObjSys
Card-G2-A_3373	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten	gemSpec_SMC-B_ObjSys
Card-G2-A_3371	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3365	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3366	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2009	Layout Vorderseite SMC-B	gemSpec_SMC_OPT
Card-G2-A_2011	Layout Vorderseite SMC-B, Gültigkeitszeitraum	gemSpec_SMC_OPT
Card-G2-A_2012	Layout Vorderseite SMC-B, Profil	gemSpec_SMC_OPT
Card-G2-A_2014	Layout Vorderseite SMC-B, ID-000-Bereich	gemSpec_SMC_OPT

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps SMC-B 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)
TIP1-A_6516	Eigenverantwortlicher Test: Test & Transitionmanager	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_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6525	Produkttypen: Testziele	gemKPT_Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_6531	Zulassung eines neuen Produkts: Aufgaben des TBV	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_6535	Zulassung eines geänderten Produkts: Aufgaben des TBV	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_2575	Zugelassenes Zugriffsprofil im CV-Rollen-Zertifikat	gemSpec_CVC_TSP
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_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys
Card-G2-A_3524	K_Personalisierung: Schlüsselgenerierung auf der Karte	gemSpec_SMC-B_ObjSys
Card-G2-A_3588	Symmetrische Kartenadministration	gemSpec_SMC-B_ObjSys
Card-G2-A_3351	K_Personalisierung: Personalisierte Attribute von MF / PIN.SMC	gemSpec_SMC-B_ObjSys
Card-G2-A_2172	K_Personalisierung: Länge der PUK für der SMC-B	gemSpec_SMC-B_ObjSys
Card-G2-A_3353	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3355	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3356	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3357	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3358	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3359	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3361	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3363	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3587	K_Personalisierung: Keine Personalisierung der PIN.Conf @deprecated	gemSpec_SMC-B_ObjSys
Card-G2-A_3367	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3368	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3369	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_2008	Formfaktor SMC-B	gemSpec_SMC_OPT
Card-G2-A_2010	Layout Vorderseite SMC-B, Ausweisnummer	gemSpec_SMC_OPT
Card-G2-A_2013	Ausrichtung Text Regionen 1-3 SMC-B	gemSpec_SMC_OPT
Card-G2-A_2015	Schriftgröße ID-000 SMC-B	gemSpec_SMC_OPT

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Der Produkttyp erfordert eine Zertifizierung nach ITSEC [ITSEC] oder Common Criteria (CC) [BSI_2006a] auf der Grundlage des Protection Profiles.

Für die Evaluierung sind die Inhalte der Schutzprofile normativ führend. Der Nachweis der im Folgenden aufgeführten Anforderungen erfolgt implizit durch die Vorlage des IT-Sicherheitszertifikats bei der gematik.

3.2.2 Sicherheitsgutachten

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

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2579	Korrektur privater Schlüssel in der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2580	Erzeugung des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2582	Vertraulichkeit des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	gemSpec_CVC_TSP
TIP1-A_2584	Schlüsselpaare und CV-Zertifikate	gemSpec_CVC_TSP
TIP1-A_2586	Personalisierung von CV-Zertifikaten für ein Sicherheitsmodul vom Typ B	gemSpec_CVC_TSP
TIP1-A_4222	Authentizität des öffentlichen Root-Schlüssels	gemSpec_CVC_TSP
TIP1-A_2590	Vernichtung fehlerhafter Chipkarten vor deren Ausgabe	gemSpec_CVC_TSP
TIP1-A_2591	Ausgabe fehlerfreier Chipkarten	gemSpec_CVC_TSP
GS-A_4473	kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß § 42a BDSG bzw. § 83a SGB X	gemSpec_DSM
GS-A_4474	kDSM: Nutzung des Incident Managements der gematik	gemSpec_DSM
GS-A_4475	kDSM: Stellungnahme bei gravierenden Datenschutzverstößen gemäß § 42a BDSG bzw. § 83a SGB X	gemSpec_DSM
GS-A_4529	Meldung von schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_5338	HBA/SMC-B - Erzeugung asymmetrischer Schlüsselpaare auf der jeweiligen Karte selbst	gemSpec_Krypt
GS-A_5386	kartenindividuelle geheime und private Schlüssel G2-Karten	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4386	TLS-Verbindungen, optional Version 1.1	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_2229	Prozesse und Maßnahmen zur Aushändigung von Karte und PIN/PUK-Brief	gemSpec_PINPUK_TI
GS-A_2227	Keine Kartendubletten	gemSpec_PINPUK_TI
GS-A_2228	Trennung von Karte und PIN/PUK-Brief	gemSpec_PINPUK_TI
GS-A_2232	PIN/PUK-Erzeugung: Verfahren für PIN/PUK-Auswahl	gemSpec_PINPUK_TI
GS-A_2239	PIN/PUK-Erzeugung: Ableitung von PIN im Sicherheitsmodul	gemSpec_PINPUK_TI
GS-A_2234	PIN/PUK-Erzeugung: Zufallsgenerator für PIN/PUK	gemSpec_PINPUK_TI
GS-A_2235	PIN/PUK-Erzeugung: Ableitung von PIN	gemSpec_PINPUK_TI
GS-A_2236	PIN/PUK-Erzeugung: Ableitung der PIN aus eindeutig dem Versicherten zugeordneten Daten	gemSpec_PINPUK_TI
GS-A_2237	PIN/PUK-Erzeugung: kein Rückschluss von PIN/PUK auf Schlüssel	gemSpec_PINPUK_TI
GS-A_2230	PIN/PUK-Erzeugung: Länge PIN/PUK (Kartenherausgeber)	gemSpec_PINPUK_TI
GS-A_2238	PIN/PUK-Erzeugung: Informationen an Karteninhaber bei selbstständiger Wahl der PIN	gemSpec_PINPUK_TI
GS-A_5209	PIN/PUK-Speicherung: PIN/PUK unverzüglich löschen	gemSpec_PINPUK_TI
GS-A_2240	PIN/PUK-Speicherung: Verschlüsselung der PIN außerhalb von Sicherheitsmodulen	gemSpec_PINPUK_TI
GS-A_2242	PIN/PUK-Speicherung: Integrität der PIN außerhalb von	gemSpec_PINPUK_TI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Sicherheitsmodulen	
GS-A_2244	PIN/PUK-Speicherung: Verschlüsselung unterschiedlicher PINs mit unterschiedlichen Schlüsseln	gemSpec_PINPUK_TI
GS-A_2246	PIN/PUK-Speicherung: Verschlüsselung gleicher PINs führt zu unterschiedlichen verschlüsselten Werten	gemSpec_PINPUK_TI
GS-A_2247	PIN/PUK-Speicherung: Wiederholte Verschlüsselung der PIN führt zu unterschiedlichen Werten	gemSpec_PINPUK_TI
GS-A_2248	PIN/PUK-Speicherung: unterschiedliche Schlüssel für unterschiedliche Zwecke	gemSpec_PINPUK_TI
GS-A_2249	PIN/PUK-Speicherung: Dokumentation der Zwecke	gemSpec_PINPUK_TI
GS-A_2250	PIN/PUK-Speicherung: Entschlüsselung nur durch berechtigten Empfänger	gemSpec_PINPUK_TI
GS-A_2253	PIN/PUK-Transport: Sicherer PIN-Transport beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2254	PIN/PUK-Transport: Schutz außerhalb geschützter Hardware beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2255	PIN/PUK-Transport: Verteilung beschränken	gemSpec_PINPUK_TI
GS-A_2256	PIN/PUK-Transport: einmalige PIN-Erstellung beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2260	PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls	gemSpec_PINPUK_TI
GS-A_2261	PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls - kein Klartext	gemSpec_PINPUK_TI
GS-A_2264	PIN/PUK-Transport: elektronische PIN-Verteilung	gemSpec_PINPUK_TI
GS-A_2266	PIN/PUK-Transport: Verschlüsselung gleicher PINs muss zu unterschiedlichen Werten führen	gemSpec_PINPUK_TI
GS-A_2270	PIN/PUK-Transport: Unterschiedliche verschlüsselte Werte auch bei gleichen PINs	gemSpec_PINPUK_TI
GS-A_2271	PIN/PUK-Transport: kein Rückschluss auf vorher benutzte Schlüssel	gemSpec_PINPUK_TI
GS-A_2274	PIN/PUK-Transport: Löschung der PIN nach Transport	gemSpec_PINPUK_TI
GS-A_2276	PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip bei der Zuordnung einer PIN/PUK zu einer Karte	gemSpec_PINPUK_TI
GS-A_2277	PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip beim Rücksetzen des Fehlbedienungs Zählers	gemSpec_PINPUK_TI
GS-A_2284	PIN/PUK-Änderung: Änderungen durch Kartenpersonalisierer im Vier-Augen-Prinzip	gemSpec_PINPUK_TI
GS-A_2285	PIN/PUK-Änderung: Prozess bei Kompromittierung beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_5085	PIN/PUK-Änderung: Prozess bei Kompromittierungsmeldung durch Karteninhaber	gemSpec_PINPUK_TI
GS-A_2287	PIN/PUK-Löschung: Nachweis der Löschung nicht mehr gebrauchter PIN beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2252	PIN/PUK-Löschung: Löschung von PIN/PUK nach Ablauf der	gemSpec_PINPUK_TI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Speicherdauer	
GS-A_2291	PIN/PUK-Löschung: Löschen von nicht mehr benötigten Klartext-PIN	gemSpec_PINPUK_TI
GS-A_2292	PIN/PUK-Löschung: Außerbetriebnahme der PIN und Karte	gemSpec_PINPUK_TI
GS-A_2295	Schutz der Schlüssel für PIN/PUK gemäß Hierarchiestufe 4	gemSpec_PINPUK_TI
GS-A_3760	Gutachten zur Einhaltung der Sicherheitsanforderungen für Dienstbetreiber	gemSpec_SiBetrUmg
GS-A_4980	Umsetzung der Norm ISO/IEC 27001	gemSpec_SiBetrUmg
GS-A_4981	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_SiBetrUmg
GS-A_4982	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_SiBetrUmg
GS-A_4983	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_SiBetrUmg
GS-A_4984	Befolgen von herstellerepezifischen Vorgaben	gemSpec_SiBetrUmg
GS-A_3737	Spezifisches Sicherheitskonzept: Mindestumfang des spezifischen Sicherheitskonzeptes..	gemSpec_SiBetrUmg
GS-A_3747	Technische_Komponenten: Dokumentation der technischen Komponenten und der geforderten Sicherheitsfunktionalität.	gemSpec_SiBetrUmg
GS-A_3753	Notfallkonzept: Der Dienstanbieter muss ein Notfallkonzept erstellen	gemSpec_SiBetrUmg
GS-A_3772	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_SiBetrUmg
GS-A_3756	Umsetzung_Maßnahmen_spezifisches_Siko: Umsetzung und Prüfbarkeit von Maßnahmen	gemSpec_SiBetrUmg
GS-A_2087	Information für Betroffene über Produkte durch Anbieter und Betreiber	gemSpec_Sich_DS
GS-A_2213	Wahrnehmung der Betroffenenrechte beim Anbieter	gemSpec_Sich_DS
GS-A_2076	Datenschutzmanagement nach BSI für Betreiber	gemSpec_Sich_DS
GS-A_2174	Inhalte des Sicherheitsgutachtens aus Sicht des Datenschutzes	gemSpec_Sich_DS
GS-A_2177	Anbieter müssen Pflichten der Auftragsdatenverarbeitung erfüllen	gemSpec_Sich_DS
GS-A_2012	Verantwortung der Anbieter und Betreiber für Einhaltung der Anforderungen Datenschutz und Informationssicherheit	gemSpec_Sich_DS
GS-A_2021	Anwendung der einheitlichen Methoden der Informationssicherheit durch Betreiber und Anbieter	gemSpec_Sich_DS
GS-A_2046	Umsetzung der Anforderungen aus [gemSpec_SiBetrUmg] durch Anbieter von zentralen Produkten	gemSpec_Sich_DS
GS-A_4944	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_Sich_DS
GS-A_4945	Produktentwicklung: Qualitätssicherung	gemSpec_Sich_DS
GS-A_4946	Produktentwicklung: sichere Programmierung	gemSpec_Sich_DS
GS-A_4947	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_Sich_DS
GS-A_2047	Gestaltung der Umgebung von zentralen Produkten durch Betreiber für Schutzbedarf "mittel"	gemSpec_Sich_DS
GS-A_2309	ISM der Beteiligten: Rollen und Verantwortlichkeiten	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2326	ISM der Beteiligten: Etablierung	gemSpec_Sich_DS
GS-A_2328	ISM der Beteiligten: Pflege und Fortschreibung der Sicherheitskonzepte	gemSpec_Sich_DS
GS-A_2329	ISM der Beteiligten: Umsetzung der Sicherheitskonzepte	gemSpec_Sich_DS
GS-A_2330	ISM der Beteiligten: Schwachstellen-Management	gemSpec_Sich_DS
GS-A_2331	ISM der Beteiligten: Sicherheitsvorfalls-Management	gemSpec_Sich_DS
GS-A_2332	ISM der Beteiligten: Notfallmanagement	gemSpec_Sich_DS
GS-A_2345	ISM der Beteiligten: Reviews und Trendanalysen	gemSpec_Sich_DS
GS-A_2347	ISM der Beteiligten: Grundlagen neuer Planungsphasen	gemSpec_Sich_DS
GS-A_2361	ISM der Beteiligten: Vorfallsmanagement	gemSpec_Sich_DS
GS-A_2363	ISM der Beteiligten: Meldung schwerwiegender Sicherheitsvorfälle	gemSpec_Sich_DS
GS-A_2366	ISM der Beteiligten: Notfallbewältigung	gemSpec_Sich_DS
GS-A_5387	Beachten von Vorgaben bei der Kartenpersonalisierung	gemSpec_Sich_DS
Card-G2-A_3589	Schlüsselspeicherung	gemSpec_SMC-B_ObjSys

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_4233	Zertifikatsuspendierung für Kartenzertifikate	gemRL_TSL_SP_CP
TIP1-A_2581	Evaluierung von HSMs	gemSpec_CVC_TSP
GS-A_4479	kDSM: Meldung von Kontaktinformationen zum Datenschutzmanagement	gemSpec_DSM
GS-A_4523	Bereitstellung Kommunikationsschnittstelle für Informationssicherheit	gemSpec_ISM
GS-A_4524	Meldung von Kontaktinformationen zum Informationssicherheitsmanagement	gemSpec_ISM
GS-A_4528	Meldung von lokalen Sicherheitsvorfällen	gemSpec_ISM
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_4958	Neue Telematik-ID bei Folgekarten	gemSpec_PKI
GS-A_4712	Definition und Eindeutigkeit der Telematik-ID	gemSpec_PKI
GS-A_4961	Verwendung zugewiesener Berufs- und Rollenattribute	gemSpec_PKI
GS-A_4962	Verhalten bei Kartenverlust und Änderung persönlicher Daten	gemSpec_PKI
GS-A_4963	Deaktivierung von Chipkarten nach Gültigkeitsende	gemSpec_PKI
GS-A_4971	Zuordnung von SMC-B zur Institution	gemSpec_PKI
GS-A_4972	Bezug des CV-Zertifikat	gemSpec_PKI
GS-A_4973	Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-Sub-CA	gemSpec_PKI
GS-A_3784	Nachweis durch ISO27001 Zertifikat	gemSpec_SiBetrUmg
GS-A_2356	ISM der Beteiligten: Nutzung des Incident-Management-Prozesses	gemSpec_Sich_DS
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
Card-G2-A_3589	Schlüsselspeicherung	gemSpec_SMC-B_ObjSys

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)
	Es liegen keine Anforderungen vor	

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 beschrieben. Die Spezifikationen des COS und des Objektsystems der SMC-B 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]
- Falls die SMC-B administriert werden soll, müssen bei der Personalisierung
 - entweder symmetrische Schlüssel für die Authentisierung mit einem CMS / CUPs gemäß [gemSpec_SMC-B_ObjSys#2]
 - oder asymmetrische Schlüssel für die Authentisierung mit einem CMS / CUPs [gemSpec_SMC-B_ObjSys#2]

in die entsprechenden Objekte der Karte eingebracht werden.

- Für die Personalisierung der CV-Zertifikate und privaten Schlüssel sind die unterschiedlichen Vorgaben für SMC-Bs der Leistungserbringer-Institutionen (nicht gekennzeichnet) und SMC-Bs in der Ausprägung_ORG (als „Ausprägung_ORG“ gekennzeichnet) zu berücksichtigen, die in den Anforderungen Card-G2-A_3346, Card-G2-A_3348, Card-G2-A_3349, Card-G2-A_3353 und Card-G2-A_3355 festgelegt sind.
- 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_2176, Card-G2-A_2180 und Card-G2-A_2184 gibt es für den Produkttyp SMC-B sechs verschiedene Möglichkeiten, die AUTR-Schlüssel einer SMC-B

Produkttypversion: 4.4.0-2

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).

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

A2 – Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion.....	6
Tabelle 2: Mitgeltende Dokumente.....	6
Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"	7
Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"	9
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"...	11
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"	15
Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	16

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
[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