

Einführung der Gesundheitskarte

Produkttypsteckbrief

Prüfvorschrift

gSMC-K

Produkttypversion: 4.2.0-1

Produkttypstatus: freigegeben

Version: 1.0.0
Revision: \main\rel_opb1\8
Stand: 06.02.2017
Status: freigegeben
Klassifizierung: öffentlich
Referenz: [gemProdT_gSMC-K_PTV4.2.0-1]

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.

Produkttyp-version	Beschreibung der Änderung	Referenz
2.0.0	Initiale Version G2-Karten für Vergabeverfahren	[gemProdT_gSMC-K_PTV2.0.0]
2.0.1	Anpassung Produkttypversion auf Stand ORS1 vom 22.04.13	[gemProdT_gSMC-K_PTV2.0.1]
2.0.2	Anpassung an G2 Iteration 1	[gemProdT_gSMC-K_PTV2.0.2]
4.0.0	Anpassung an G2 Iteration 2	[gemProdT_gSMC-K_PTV4.0.0]
4.0.1	Anpassung an G2 Iteration 2b	[gemProdT_gSMC-K_PTV4.0.1]
4.1.0	Anpassung an G2 Iteration 3	[gemProdT_gSMC-K_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4, 4a, 4b	[gemProdT_gSMC-K_PTV4.2.0]
4.2.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_gSMC-K_PTV4.2.0-1]

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	06.02.17		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	10
3.2 Anforderungen zur sicherheitstechnischen Eignung	12
3.2.1 CC-Evaluierung	12
3.2.2 Sicherheitsgutachten	12
3.2.3 Herstellererklärung sicherheitstechnische Eignung.....	15
3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	16
4 Produkttypspezifische Merkmale	18
4.1 Angaben zu EF.Version2.....	18
4.2 Optionale Ausprägungen	18
4.3 Variationen	18
4.3.1 Festlegung des Attributwertes „transportStatus“ der gSMC-K PINs	18
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 gSMC-K in der Produkttypversion 4.2.0-1 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 gSMC-K-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

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich Anforderungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

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 gesond-

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.

erten 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 den Produkttyp 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 normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemKPT_Test	Testkonzept	1.9.0
gemRL_TSL_SP_CP	Certificate Policy	1.7.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.8.0
gemSpec_DSM	Spezifikation koordinierendes DSM	1.3.1
gemSpec_gSMC-K_ObjSys	Spezifikation der gSMC-K Objektsystem	3.10.0
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	2.7.0
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)	1.11.0
gemSpec_SiBetrUmg	Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung	1.4.0
gemSpec_Sich_DS	Spezifikation Sicherheits-/Datenschutzanforderungen	1.4.1
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	2.10.0

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 normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps 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 Produkttyps 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)
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_3336	K_Initialisierung und K_Personalisierung: Vorgaben für die Option_Erweiterung_herstellerspezifische_Schlüssel_01	gemSpec_gSMC-K_ObjSys
Card-G2-A_2538	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_gSMC-K_ObjSys
Card-G2-A_2665	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_gSMC-K_ObjSys
Card-G2-A_3201	K_Personalisierung und K_Initialisierung: Zuordnung zu transportStatus für die Passwortobjekte der gSMC-K	gemSpec_gSMC-K_ObjSys
Card-G2-A_2994	K_Personalisierung: Absicherung der Kartenadministration	gemSpec_gSMC-K_ObjSys
Card-G2-A_2541	K_Personalisierung: zusätzliche Ordner	gemSpec_gSMC-K_ObjSys
Card-G2-A_2542	K_Personalisierung: zusätzliche Objekte	gemSpec_gSMC-K_ObjSys
Card-G2-A_2544	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_gSMC-K_ObjSys
Card-G2-A_2545	K_Personalisierung: Wert des Attributes iccsn8	gemSpec_gSMC-K_ObjSys
Card-G2-A_3514	K_Personalisierung: personalisierter Wert von pointInTime	gemSpec_gSMC-K_ObjSys
Card-G2-A_2547	K_Personalisierung und K_Initialisierung: ATR-Kodierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_2548	K_Personalisierung und K_Initialisierung: TC1 Byte im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2997	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_3041	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_gSMC-K_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3394	K_Personalisierung: Personalisierte Attribute von MF / EF.EnvironmentSettings	gemSpec_gSMC-K_ObjSys
Card-G2-A_2567	K_Personalisierung: Personalisiertes Attribut von EF.GDO	gemSpec_gSMC-K_ObjSys
Card-G2-A_3393	K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SAK.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3580	K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3581	K_Personalisierung: Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3328	K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3329	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3331	K_externe Welt: Festlegung von CHR für EF.C.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2570	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3333	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3400	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3338	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3376	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3380	K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3382	K_Personalisierung: Personalisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3401	K_Personalisierung: Personalisierte Attribute von MF / PrK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3402	K_Personalisierung: Personalisierte Attribute von MF / PuK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3262	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3404	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3405	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3447	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3449	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_gSMC-K_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3450	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3406	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3407	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3410	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3411	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3416	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3417	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PuK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3423	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3424	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2638	K_Personalisierung: CHR von C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3429	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3430	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2640	K_Personalisierung: CHR von C.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3431	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3434	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3582	K_Personalisierung: Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3583	K_Personalisierung: Personalisierte Attribute von MF / EF.C.TSL.CA_1 für Testkarten	gemSpec_gSMC-K_ObjSys
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3497	K_Personalisierung: Vollständige Befüllung von EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TIP
Card-G2-A_3507	K_Personalisierung Versionierung Inhalte von EF.EnvironmentSettings	gemSpec_Karten_Fach_TIP
Card-G2-A_3509	K_Personalisierung Inhalt von EF.EnvironmentSettings	gemSpec_Karten_Fach_TIP
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_4707	Kennzeichen für Technische Rolle für Komponenten und Dienste	gemSpec_PKI
GS-A_4606	Identischer ICCSN in allen Zertifikaten einer gSMC-K	gemSpec_PKI
GS-A_4974	CV-Ausstattung von Smartcards der TI	gemSpec_PKI
GS-A_4622	Zugriffsprofil einer gSMC-K	gemSpec_PKI
GS-A_5335	Zugriffsprofil einer gSMC-K für Administrationszwecke	gemSpec_PKI
Card-G2-A_2016	Formfaktor gSMC-K	gemSpec_SMC_OPT
Card-G2-A_2017	Layout Vorderseite gSMC-K	gemSpec_SMC_OPT
Card-G2-A_2018	Layout Vorderseite gSMC-K, Kartenummer	gemSpec_SMC_OPT
Card-G2-A_2019	Layout Vorderseite gSMC-K, Profilnummern	gemSpec_SMC_OPT
Card-G2-A_2020	Layout Vorderseite gSMC-K, ID-000-Bereich	gemSpec_SMC_OPT
Card-G2-A_2021	Schriftgröße ID-000 gSMC-K	gemSpec_SMC_OPT

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps 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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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
TIP1-A_6526	Produkttypen: Bereitstellung	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
Card-G2-A_3261	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_3396	K_Personalisierung: Personalisierte Attribute von MF / PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3397	K_Personalisierung: Personalisierte Attribute von MF / PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3398	K_Personalisierung: Personalisierte Attribute von MF / PIN.Pers	gemSpec_gSMC-K_ObjSys
Card-G2-A_3399	K_Personalisierung: Personalisierte Attribute von MF / PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3403	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3438	K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_3439	K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA	gemSpec_gSMC-K_ObjSys
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4605	Verwendung registrierter Daten für gSMC-K-Zertifikatsbeantragung	gemSpec_PKI

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

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

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
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	gemSpec_CVC_TSP
TIP1-A_2584	Schlüsselpaare und CV-Zertifikate	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
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys
GS-A_4529	Meldung von schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
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, Version 1.1	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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 Sicherheitsmodulen	gemSpec_PINPUK_TI
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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 Fehlbedienungszählers	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 Speicherdauer	gemSpec_PINPUK_TI
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	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Betreiber	
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
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

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
GS-A_4479	kDSM: Meldung von Kontaktinformationen zum Datenschutzmanagement	gemSpec_DSM
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys
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_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_4963	Deaktivierung von Chipkarten nach Gültigkeitsende	gemSpec_PKI
GS-A_4965	Suspendierung von X.509-Zertifikaten (außer für eGK)	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

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 gSMC-K wird im Dokument [gemSpec_Karten_Fach_TIP] festgelegt.

4.2 Optionale Ausprägungen

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

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec_gSMC-K_ObjSys#4.3.2]
- Bereitstellung asymmetrischer Schlüssel für die Authentisierung mit einem CMS / CUPs gemäß [gemSpec_gSMC-K_ObjSys#2]
- Bereitstellung symmetrischer Schlüssel für die Authentisierung mit einem CMS / CUPs gemäß [gemSpec_gSMC-K_ObjSys#2]
- Bereitstellung zusätzlicher herstellerspezifischer Schlüssel gemäß der Option_Erweiterung_herstellerspezifische_Schlüssel_01 [gemSpec_gSMC-K_ObjSys#2]

Die gSMC-K kann gemäß [gemSpec_gSMC-K_ObjSys#2] als Testkarte ausgestaltet werden.

4.3 Variationen

4.3.1 Festlegung des Attributwertes „transportStatus“ der gSMC-K PINs

Gemäß Card-G2-A_2569, Card-G2-A_2571, Card-G2-A_2573, Card-G2-A_2575 Card, G2-A_2658 und Card-G2-A_2660 gibt es für den Produkttyp gSMC-K zwei verschiedene Möglichkeiten, den Wert für das Attribut „transportStatus“ der PINs einer gSMC-K festzulegen: „Leer-PIN“ oder „Transport-PIN“. Der Wert "Transport-PIN" kann bei der Personalisierung in "regularPassword" mit der Zuordnung eines konkreten PIN-Wertes geändert werden. Alle PINs einer gSMC-K müssen dabei bei einer Karte gemäß Card-G2-A_3201 mit demselben Wert für „transportStatus“ belegt werden.

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"	10
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ...	12
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"	16
Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	17

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