

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

gSMC-K

Zulassungsobjekt gSMC-K- Objektsystem

Produkttyp Version: 4.3.1-3
Produkttyp Status: freigegeben

Version: 1.1.0
Revision: 57146
Stand: 26.10.2018
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_gSMC-K_ObjSys_PTV_4.3.1-3

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_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_ObjSys_PTV2.0.2]
4.0.0	Anpassung an G2 Iteration 2	[gemProdT_gSMC-K_ObjSys_PTV4.0.0]
4.0.1	Anpassung an G2 Iteration 2b	[gemProdT_gSMC-K_ObjSys_PTV4.0.1]
4.1.0	Anpassung an G2 Iteration 3	[gemProdT_gSMC-K_ObjSys_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4	[gemProdT_gSMC-K_ObjSys_PTV4.2.0]
4.3.1	Einarbeitung der Errata R1.4.1 bis R1.4.6	[gemProdT_gSMC-K_ObjSys_PTV4.3.1]
4.3.1-1	Anpassung auf Releasestand 1.6.3	[gemProdT_gSMC-K_ObjSys_PTV4.3.1-1]
4.3.1-2	Anpassung auf Releasestand 1.6.4	[gemProdT_gSMC-K_ObjSys_PTV4.3.1-2]
4.3.1-3	Anpassung auf Releasestand 2.1.2	[gemProdT_gSMC-K_ObjSys_PTV4.3.1-3]

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	14.05.18		freigegeben	gematik
1.1.0	26.10.18		freigegeben	gematik

Inhaltsverzeichnis

1	Einführung.....	5
1.1	Zielsetzung und Einordnung des Dokumentes	5
1.2	Zielgruppe	5
1.3	Geltungsbereich	5
1.4	Abgrenzung des Dokumentes	6
1.5	Methodik.....	6
2	Dokumente	7
3	Blattanforderungen	9
3.1	Anforderungen zur funktionalen Eignung	9
3.1.1	Produkttest/Produktübergreifender Test	9
3.1.2	Herstellererklärung funktionale Eignung	16
3.2	Anforderungen zur sicherheitstechnischen Eignung	18
3.2.1	Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie 18	
3.2.2	CC-Evaluierung	26
3.2.3	Herstellererklärung sicherheitstechnische Eignung.....	26
3.3	Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	27
4	Produkttypspezifische Merkmale	28
4.1	Angaben zu EF.Version2.....	28
4.2	Optionale Ausprägungen	28
4.3	Variationen	28
4.3.1	Festlegung des Wertes für das Attribut „transportStatus“ der PINs der gSMC-K 28	
5	Anhang A – Verzeichnisse	29
5.1	Abkürzungen.....	29
5.2	Tabellenverzeichnis.....	29
5.3	Referenzierte Dokumente.....	29

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an die Herstellung des Zulassungsobjektes gSMC-K-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 Zulassungsobjekt gSMC-K-Objektsystem richtet sich an gSMC-K-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

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 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 gSMC-K-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 gSMC-K-Objektsystem normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumenten Kürzel	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_gSMC-K_ObjSys	Spezifikation der gSMC-K Objektsystem	3.11.1
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

Tabelle 2: Mitgeltende Dokumente

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemSpec_TLK_COS_G2	gematik: Spezifikation der Testlaborkarte COS / Objektsysteme	1.6.0
gemSpec_OID	gematik: Spezifikation Festlegung von OIDs	2.12.0
TR-03143	BSI: eHealth G2-COS Konsistenz-Prüf tool	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 gSMC-K-Objektsystem normativen Anforderungen, die für die Herstellung des Zulassungsobjektes 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 Zulassungsobjektes gSMC-K-Objektsystem verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3483	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP

Card-G2-A_3499	K_Initialisierung: Speicherstruktur für EF.KeyInfo	gemSpec_Karten_Fach_TIP
Card-G2-A_3501	K_Initialisierung: Kodierung der Kryptosysteme in EF.KeyInfo	gemSpec_Karten_Fach_TIP
Card-G2-A_3502	K_Initialisierung: Initiale Belegung von EF.KeyInfo für die gSMC-K	gemSpec_Karten_Fach_TIP
Card-G2-A_3503	K_Initialisierung: Kennungen von EF.KeyInfo für die gSMC-K	gemSpec_Karten_Fach_TIP
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
Card-G2-A_2533	K_Initialisierung: Verwendung von SE#1	gemSpec_gSMC-K_ObjSys
Card-G2-A_2535	K_Initialisierung: Ordnerattribute	gemSpec_gSMC-K_ObjSys
Card-G2-A_2537	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_gSMC-K_ObjSys
Card-G2-A_2538	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_gSMC-K_ObjSys
Card-G2-A_2540	K_Initialisierung: Normative Anforderungen	gemSpec_gSMC-K_ObjSys
Card-G2-A_2543	K_Initialisierung: Wert des Attributes root	gemSpec_gSMC-K_ObjSys
Card-G2-A_2544	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_gSMC-K_ObjSys
Card-G2-A_2546	K_Initialisierung: Inhalt persistentPublicKeyList	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_2553	K_Initialisierung: Initialisierte Attribute von MF	gemSpec_gSMC-K_ObjSys
Card-G2-A_2554	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2561	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2562	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E384	gemSpec_gSMC-K_ObjSys

Card-G2-A_2563	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2565	K_Initialisierung: Initialisierte Attribute von MF / EF.EnvironmentSettings	gemSpec_gSMC-K_ObjSys
Card-G2-A_2566	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_gSMC-K_ObjSys
Card-G2-A_2568	K_Initialisierung: Initialisierte Attribute von MF / EF.Version2	gemSpec_gSMC-K_ObjSys
Card-G2-A_2569	K_Initialisierung: Initialisierte Attribute von MF / PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2571	K_Initialisierung: Initialisierte Attribute von MF / PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2573	K_Initialisierung: Initialisierte Attribute von MF / PIN.Pers	gemSpec_gSMC-K_ObjSys
Card-G2-A_2575	K_Initialisierung: Initialisierte Attribute von MF / PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2577	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2578	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2579	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2580	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2581	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2582	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2583	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2585	K_Initialisierung: Initialisierte Attribute von MF / PuK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2588	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_2589	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2592	K_Initialisierung: Initialisierte Attribute von MF / DF.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2595	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2599	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2600	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048	gemSpec_gSMC-K_ObjSys

Card-G2-A_2601	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2602	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2605	K_Initialisierung: Initialisierte Attribute von MF / DF.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2606	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ActKey	gemSpec_gSMC-K_ObjSys
Card-G2-A_2607	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CardInfo	gemSpec_gSMC-K_ObjSys
Card-G2-A_2608	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey	gemSpec_gSMC-K_ObjSys
Card-G2-A_2609	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ConfigUser	gemSpec_gSMC-K_ObjSys
Card-G2-A_2612	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2617	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2623	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2626	K_Initialisierung: Vorhandensein von DF.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2627	K_Initialisierung: Konfiguration von DF.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2628	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2631	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK/EF.C.SAK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_2635	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2639	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2641	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2643	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2644	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2645	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2646	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R3072	gemSpec_gSMC-K_ObjSys

Card-G2-A_2647	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2648	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2649	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2650	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2653	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker	gemSpec_gSMC-K_ObjSys
Card-G2-A_2654	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2655	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_1	gemSpec_gSMC-K_ObjSys
Card-G2-A_2656	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_2	gemSpec_gSMC-K_ObjSys
Card-G2-A_2658	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2660	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2663	K_gSMC-K: Anlegen von EF.GeneralPurpose in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker	gemSpec_gSMC-K_ObjSys
Card-G2-A_2665	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_gSMC-K_ObjSys
Card-G2-A_2666	K_Initialisierung: Initialisierte Attribute von MF / EF.C.RCA.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2873	K_gSMC-K: Kryptobox	gemSpec_gSMC-K_ObjSys
Card-G2-A_2995	K_gSMC-K: USB-Schnittstelle	gemSpec_gSMC-K_ObjSys
Card-G2-A_2996	K_gSMC-K: Vorhandensein einer USB-Schnittstelle	gemSpec_gSMC-K_ObjSys
Card-G2-A_2997	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2998	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3041	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_gSMC-K_ObjSys
Card-G2-A_3192	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs	gemSpec_gSMC-K_ObjSys
Card-G2-A_3201	K_Personalisierung und K_Initialisierung: Zuordnung zu	gemSpec_gSMC-K_ObjSys

	transportStatus für die Passwortobjekte der gSMC-K	
Card-G2-A_3206	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3251	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_3252	K_Initialisierung: Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3254	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3256	K_Initialisierung: Initialisierte Attribute von MF/DF.AK/PrK.AK.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3258	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3259	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3260	K_Initialisierung: Initialisierte Attribute von MF/DF.NK/EF.C.NK.VPN2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3268	K_Initialisierung: Wert von pointInTime	gemSpec_gSMC-K_ObjSys
Card-G2-A_3280	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3330	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3332	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3334	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3336	K_Initialisierung und K_Personalisierung: Vorgaben für die Option_Erweiterung_herstellerspezifische_Schlüssel_01	gemSpec_gSMC-K_ObjSys
Card-G2-A_3337	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3339	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3345	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3372	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys

Card-G2-A_3377	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3378	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3379	K_Initialisierung: Initialisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3381	K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3383	K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3384	K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3392	K_Initialisierung: Attribute von MF / EF.KeyInfo	gemSpec_gSMC-K_ObjSys
Card-G2-A_3408	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3409	K_Initialisierung: Initialisierte Attribute von MF/DF.AK/PrK.AK.CA_PS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3412	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3413	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3414	K_Initialisierung: Initialisierte Attribute von MF/DF.NK/PrK.NK.VPN.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3415	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3418	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3419	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3420	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3421	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3422	K_Initialisierung: Initialisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys

Card-G2-A_3425	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3426	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3427	K_Initialisierung: Initialisierte Attribute von MF/DF.SAK/PrK.SAK.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3428	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3432	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3433	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3435	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3436	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3442	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3443	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3444	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3446	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3448	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3451	K_Initialisierung: Initialisierte Attribute von MF/DF.AK/EF.C.AK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3452	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3850	K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung	gemSpec_gSMC-K_ObjSys

3.1.2 Herstellererklärung funktionale Eignung

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

Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellereklärung"

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_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_2572	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2574	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.Pers	gemSpec_gSMC-K_ObjSys

Card-G2-A_2576	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2659	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.BNetzA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2661	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.TSL_CA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2662	K_Initialisierung: Zahl der Ordner in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker	gemSpec_gSMC-K_ObjSys
Card-G2-A_3261	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_gSMC-K_ObjSys

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie

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

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3483	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP

Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP
Card-G2-A_3499	K_Initialisierung: Speicherstruktur für EF.KeyInfo	gemSpec_Karten_Fach_TIP
Card-G2-A_3501	K_Initialisierung: Kodierung der Kryptosysteme in EF.KeyInfo	gemSpec_Karten_Fach_TIP
Card-G2-A_3502	K_Initialisierung: Initiale Belegung von EF.KeyInfo für die gSMC-K	gemSpec_Karten_Fach_TIP
Card-G2-A_3503	K_Initialisierung: Kennungen von EF.KeyInfo für die gSMC-K	gemSpec_Karten_Fach_TIP
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_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_2532	K_Initialisierung: Änderung von Zugriffsregeln	gemSpec_gSMC-K_ObjSys
Card-G2-A_2533	K_Initialisierung: Verwendung von SE#1	gemSpec_gSMC-K_ObjSys
Card-G2-A_2535	K_Initialisierung: Ordnerattribute	gemSpec_gSMC-K_ObjSys
Card-G2-A_2536	K_Initialisierung: Dateiattribute	gemSpec_gSMC-K_ObjSys
Card-G2-A_2537	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_gSMC-K_ObjSys
Card-G2-A_2538	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_gSMC-K_ObjSys
Card-G2-A_2540	K_Initialisierung: Normative Anforderungen	gemSpec_gSMC-K_ObjSys
Card-G2-A_2543	K_Initialisierung: Wert des Attributes root	gemSpec_gSMC-K_ObjSys
Card-G2-A_2544	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_gSMC-K_ObjSys
Card-G2-A_2546	K_Initialisierung: Inhalt persistentPublicKeyList	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	gemSpec_gSMC-K_ObjSys

	ATR	
Card-G2-A_2553	K_Initialisierung: Initialisierte Attribute von MF	gemSpec_gSMC-K_ObjSys
Card-G2-A_2554	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2561	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2562	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2563	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2565	K_Initialisierung: Initialisierte Attribute von MF / EF.EnvironmentSettings	gemSpec_gSMC-K_ObjSys
Card-G2-A_2566	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_gSMC-K_ObjSys
Card-G2-A_2568	K_Initialisierung: Initialisierte Attribute von MF / EF.Version2	gemSpec_gSMC-K_ObjSys
Card-G2-A_2569	K_Initialisierung: Initialisierte Attribute von MF / PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2571	K_Initialisierung: Initialisierte Attribute von MF / PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2572	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2573	K_Initialisierung: Initialisierte Attribute von MF / PIN.Pers	gemSpec_gSMC-K_ObjSys
Card-G2-A_2574	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.Pers	gemSpec_gSMC-K_ObjSys
Card-G2-A_2575	K_Initialisierung: Initialisierte Attribute von MF / PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2576	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2577	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2578	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2579	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2580	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2581	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2582	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2583	K_Initialisierung: Initialisierte Attribute von MF /	gemSpec_gSMC-K_ObjSys

	PuK.RCA.CS.E256	
Card-G2-A_2585	K_Initialisierung: Initialisierte Attribute von MF / PuK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2588	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_2589	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2592	K_Initialisierung: Initialisierte Attribute von MF / DF.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2595	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2599	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2600	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2601	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2602	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2605	K_Initialisierung: Initialisierte Attribute von MF / DF.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2606	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ActKey	gemSpec_gSMC-K_ObjSys
Card-G2-A_2607	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CardInfo	gemSpec_gSMC-K_ObjSys
Card-G2-A_2608	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey	gemSpec_gSMC-K_ObjSys
Card-G2-A_2609	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ConfigUser	gemSpec_gSMC-K_ObjSys
Card-G2-A_2612	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2617	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2623	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2626	K_Initialisierung: Vorhandensein von DF.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2627	K_Initialisierung: Konfiguration von DF.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2628	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2631	K_Initialisierung: Initialisierte Attribute von MF/	gemSpec_gSMC-K_ObjSys

	DF.SAK/EF.C.SAK.AUT2.XXXX	
Card-G2-A_2635	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2639	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2641	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2643	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2644	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2645	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2646	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2647	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2648	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_2649	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_2650	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2653	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker	gemSpec_gSMC-K_ObjSys
Card-G2-A_2654	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2655	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_1	gemSpec_gSMC-K_ObjSys
Card-G2-A_2656	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_2	gemSpec_gSMC-K_ObjSys
Card-G2-A_2658	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2659	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.BNetzA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2660	K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA	gemSpec_gSMC-K_ObjSys
Card-G2-A_2661	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.TSL_CA	gemSpec_gSMC-K_ObjSys

Card-G2-A_2662	K_Initialisierung: Zahl der Ordner in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker	gemSpec_gSMC-K_ObjSys
Card-G2-A_2663	K_gSMC-K: Anlegen von EF.GeneralPurpose in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker	gemSpec_gSMC-K_ObjSys
Card-G2-A_2665	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_gSMC-K_ObjSys
Card-G2-A_2666	K_Initialisierung: Initialisierte Attribute von MF / EF.C.RCA.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2997	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2998	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3040	K_Terminal: Ausschluss kontaktlose Schnittstelle	gemSpec_gSMC-K_ObjSys
Card-G2-A_3041	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_gSMC-K_ObjSys
Card-G2-A_3191	K_Initialisierung: Größe persistentPublicKeyList	gemSpec_gSMC-K_ObjSys
Card-G2-A_3192	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs	gemSpec_gSMC-K_ObjSys
Card-G2-A_3193	K_Initialisierung: Eigenschaften der Objekte in anderen SEs	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_3206	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3251	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_3252	K_Initialisierung: Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3254	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3256	K_Initialisierung: Initialisierte Attribute von MF/DF.AK/PrK.AK.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3258	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3259	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3260	K_Initialisierung: Initialisierte Attribute von MF/DF.NK/EF.C.NK.VPN2.XXXX	gemSpec_gSMC-K_ObjSys

Card-G2-A_3261	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_3268	K_Initialisierung: Wert von pointInTime	gemSpec_gSMC-K_ObjSys
Card-G2-A_3280	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3330	K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3332	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3334	K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3336	K_Initialisierung und K_Personalisierung: Vorgaben für die Option_Erweiterung_herstellerspezifische_Schlüssel_01	gemSpec_gSMC-K_ObjSys
Card-G2-A_3337	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3339	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3345	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3372	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3377	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3378	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3379	K_Initialisierung: Initialisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3381	K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3383	K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3384	K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R3072	gemSpec_gSMC-K_ObjSys

	(Option_Erweiterung_herstellerspezifische_Schlüssel_01)	
Card-G2-A_3392	K_Initialisierung: Attribute von MF / EF.KeyInfo	gemSpec_gSMC-K_ObjSys
Card-G2-A_3408	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3409	K_Initialisierung: Initialisierte Attribute von MF/DF.AK/PrK.AK.CA_PS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3412	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3413	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3414	K_Initialisierung: Initialisierte Attribute von MF/DF.NK/PrK.NK.VPN.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3415	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3418	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3419	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3420	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3421	K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3422	K_Initialisierung: Initialisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3425	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3426	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072	gemSpec_gSMC-K_ObjSys
Card-G2-A_3427	K_Initialisierung: Initialisierte Attribute von MF/DF.SAK/PrK.SAK.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3428	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3432	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3433	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3435	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048	gemSpec_gSMC-K_ObjSys

Card-G2-A_3436	K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3442	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3443	K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3444	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP2.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3446	K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3448	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3451	K_Initialisierung: Initialisierte Attribute von MF/DF.AK/EF.C.AK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3452	K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048	gemSpec_gSMC-K_ObjSys

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_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	Bemäßung der Kontakte der (g)SMC	gemSpec_SMC_OPT

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-Objektsystem beschrieben. Die Spezifikationen des COS und des Objektsystems der gSMC-K-Objektsystem lassen folgende Optionen zu:

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec_gSMC-K_ObjSys#4.3.2]
- Vorbereitung der gSMC-K zur Speicherung zusätzlicher herstellereinspezifischer Schlüssel durch Anlage der Schlüsselobjekte gemäß der Option_Erweiterung_herstellereinspezifische_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 Wertes für das Attribut „transportStatus“ der PINs der gSMC-K

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 das Objektsystem des Zulassungsobjektes gSMC-K zwei verschiedene Möglichkeiten, den Wert für das Attribut „transportStatus“ der PINs festzulegen: „Leer-PIN“ oder „Transport-PIN“. Alle PINs einer gSMC-K müssen dabei gemäß Card-G2-A_3201 mit demselben Wert für „transportStatus“ belegt werden.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion	7
Tabelle 2: Mitgeltende Dokumente.....	7
Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"	9
Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"	17
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie".....	18
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"	26
Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	27

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