

## Einführung der Gesundheitskarte

# Produkttypsteckbrief

*Prüfvorschrift*

## gSMC-KT

**Produkttypversion:** 4.2.0

**Produkttypstatus:** freigegeben

Version: 1.1.0  
Revision: \main\rel\_ors1\3  
Stand: 07.08.2015  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenz: [gemProdT\_gSMC-KT\_PTV4.2.0]

---

## Historie Produkttypversion und Produkttypsteckbrief

---

### Historie Produkttypversion

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

Produkttypversion	Beschreibung der Änderung	Referenz
2.0.0	Initiale Version G2-Karten für Vergabeverfahren	[gemProdT_gSMC-KT_PTV2.0.0]
2.0.1	Anpassung Produkttypversion auf Stand ORS1 vom 22.04.13	[gemProdT_gSMC-KT_PTV2.0.1]
2.0.2	Anpassung an G2 Iteration 1 und 2a	[gemProdT_gSMC-KT_PTV2.0.2]
4.0.1	Anpassung an G2 Iteration 2b	[gemProdT_gSMC-KT_PTV4.0.1]
4.1.0	Anpassung an G2 Iteration 3	[gemProdT_gSMC-KT_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4, 4a, 4b	[gemProdT_gSMC-KT_PTV4.2.0]

### Historie Produkttypsteckbrief

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

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	24.07.15		freigegeben	gematik
		2	Aktualisierung	
1.1.0	07.08.15		freigegeben	

---

## Inhaltsverzeichnis

---

Historie Produkttypversion und Produkttypsteckbrief .....	2
Inhaltsverzeichnis .....	3
<b>1 Einführung.....</b>	<b>4</b>
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
<b>2 Dokumente .....</b>	<b>6</b>
<b>3 Blattanforderungen.....</b>	<b>7</b>
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 .....	10
3.2.1 CC-Evaluierung .....	10
3.2.2 Sicherheitsgutachten .....	10
3.2.3 Sicherheitsbestätigung .....	12
3.2.4 Herstellerklärung sicherheitstechnische Eignung.....	12
3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	13
3.4 Anforderungen zur betrieblichen Eignung .....	13
3.4.1 Prozessprüfung betriebliche Eignung .....	13
3.4.2 Herstellererklärung betriebliche Eignung .....	14
<b>4 Umsetzungsanforderungen .....</b>	<b>15</b>
<b>5 Produkttypspezifische Merkmale .....</b>	<b>16</b>
5.1 Angaben zu EF.Version2.....	16
5.2 Optionale Ausprägungen .....	16
<b>Anhang A - Verzeichnisse .....</b>	<b>17</b>
A1 - Abkürzungen.....	17
A2 – Tabellenverzeichnis.....	17
A3 - Referenzierte Dokumente.....	17

---

## 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-KT in der Produkttypversion 4.2.0 oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen<sup>1</sup> 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-KT-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-

---

<sup>1</sup> 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 wider, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der Anforderung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

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

## 2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

**Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion**

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemKPT_Test_ORs1	gematik: Testkonzept Online-Rollout (Stufe 1)	1.6.0
gemRL_TSL_SP_CP	gematik: Certificate Policy, Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	1.3.0
gemSpec_CVC_TSP	gematik: Spezifikation Trust Service Provider CVC	1.5.0
gemSpec_DSM	gematik: Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur	1.2.0
gemSpec_gSMC-KT_ObjSys	gematik: Spezifikation gSMC-KT Objektsystem	3.8.0
gemSpec_ISM	gematik: Koordinierendes Informationssicherheitsmanagement der TI	1.2.0
gemSpec_Karten_Fach_TIP	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI	2.4.1
gemSpec_Krypt	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.4.0
gemSpec_OM	gematik: Spezifikation Operations und Maintenance (Fehlermanagement, Versionierung, Monitoring)	1.6.0
gemSpec_PKI	gematik: Spezifikation PKI	1.7.0
gemSpec_SiBetrUmg	gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI	1.3.0
gemSpec_Sich_DS	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen	1.2.0
gemSpec_SMC_OPT	gematik: Gemeinsame optische Merkmale der SMC	3.3.0

**Tabelle 2: Mitgeltende Dokumente**

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemSpec_OID	gematik: Spezifikation Festlegung von OIDs	2.8.0

### 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_2588	Personalisierung des öffentlichen Root-Schlüssels	gemSpec_CVC_TSP
TIP1-A_2589	Personalisierung des CVC-CA-Zertifikats	gemSpec_CVC_TSP
Card-G2-A_3019	Vorgaben für die Option_lange_Lebensdauer_im_Feld	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3515	K_Personalisierung: personalisierter Wert von pointInTime	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2849	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3276	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2477	K_Personalisierung: weitere Applikationen	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2478	K_Personalisierung: Zusätzliche Objekte	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3274	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2479	K_Personalisierung: Wert des Attributes iccsn8	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2481	K_Personalisierung und K_Initialisierung: ATR-Kodierung	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2482	K_Personalisierung und K_Initialisierung: TC1-Byte in ATR	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3027	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2483	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2507	K_Personalisierung: Personalisiertes Attribut von EF.GDO	gemSpec_gSMC-KT_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3455	K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.E256	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2500	K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUTD_RPS_CVC.E256	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3456	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256	gemSpec_gSMC-KT_ObjSys
Card-G2-A_2502	K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUTD_RPS_CVC.E384	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3457	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3275	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3459	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3460	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3462	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3464	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3465	K_Personalisierung: Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3466	K_Personalisierung: Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048	gemSpec_gSMC-KT_ObjSys
Card-G2-A_3467	K_Personalisierung: Personalisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048	gemSpec_gSMC-KT_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_Personalisierung: 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
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TIP
GS-A_4379	Card-to-Card-Authentisierung G2	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



Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_4974	CV-Ausstattung von Smartcards der TI	gemSpec_PKI
GS-A_5126	Zugriffsprofil einer gSMC-KT	gemSpec_PKI
Card-G2-A_2022	Formfaktor (g)SMC-KT	gemSpec_SMC_OPT
Card-G2-A_2023	Layout Vorderseite gSMC-KT	gemSpec_SMC_OPT
Card-G2-A_2024	Layout Vorderseite gSMC-KT, Kartennummer	gemSpec_SMC_OPT
Card-G2-A_2025	Layout Vorderseite gSMC-KT, Profilnummer	gemSpec_SMC_OPT
Card-G2-A_3209	Layout Vorderseite gSMC-KT, Hashwert von C.SMKT.AUT.R2048, Bedruckung	gemSpec_SMC_OPT
Card-G2-A_3239	Layout Vorderseite gSMC-KT, Hashwert von C.SMKT.AUT.R2048, Übermittlung	gemSpec_SMC_OPT
Card-G2-A_2026	Layout Vorderseite gSMC-KT, ID-000-Bereich	gemSpec_SMC_OPT
Card-G2-A_2027	Schriftgröße ID-000 gSMC-KT	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)
Card-G2-A_3458	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_gSMC-KT_ObjSys
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
GS-A_4964	Bezug von X.509-Zertifikaten aus der zentralen PKI der TI	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 in einem HSM	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
TIP1-A_2667	Sicherstellung der Eignung der CVC-CA durch den Kartenherausgeber	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_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_4529	Meldung von schwerwiegenden Sicherheitsvorfällen und -	gemSpec_ISM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	notfällen	
GS-A_4384	TLS-Verbindungen	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_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 herstelllerspezifischen Vorgaben	gemSpec_SiBetrUmg
GS-A_3784	Nachweis durch ISO27001 Zertifikat	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 (1)	gemSpec_SiBetrUmg
GS-A_3772	Notfallkonzept: Der Dienstanbieter MUSS ein Notfallkonzept erstellen (2)	gemSpec_SiBetrUmg
GS-A_3756	Umsetzung_Maßnahmen_spezifisches_Siko: Umsetzung und Prüfbarkeit von Maßnahmen.	gemSpec_SiBetrUmg
GS-A_3760	Gutachten zur Einhaltung der Sicherheitsanforderungen für Dienstbetreiber	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	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Betreiber für Schutzbedarf "mittel"	
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_2356	ISM der Beteiligten: Nutzung des Incident-Management-Prozesses	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

### 3.2.3 Sicherheitsbestätigung

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

### 3.2.4 Herstellerklärung sicherheitstechnische Eignung

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

**Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4233	Zertifikatsuspendierung für Kartenzertifikate	gemRL_TSL_SP_CP
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

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

### 3.4 Anforderungen zur betrieblichen Eignung

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

#### 3.4.1 Prozessprüfung betriebliche Eignung

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

**Tabelle 8: Anforderungen zur betrieblichen Eignung "Prozessprüfung"**

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

### 3.4.2 Herstellererklärung betriebliche Eignung

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

**Tabelle 9: Anforderungen zur betrieblichen Eignung "Herstellererklärung"**

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

---

## 4 Umsetzungsanforderungen

---

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

**Tabelle 10: Offene Umsetzungsanforderungen an den Produkttyp**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

---

## 5 Produkttypspezifische Merkmale

---

### 5.1 Angaben zu EF.Version2

Die detaillierte Versionskennzeichnung der gSMC-KT wird im Dokument [gemSpec\_Karten\_Fach\_TIP] festgelegt.

### 5.2 Optionale Ausprägungen

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

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec\_gSMC-KT\_ObjSys#4.3.2]
- Bereitstellung symmetrischer Schlüssel für die Authentisierung mit einem CMS / CUPs gemäß [gemSpec\_gSMC-KT\_ObjSys#2]
- Bereitstellung asymmetrischer Schlüssel für die Authentisierung mit einem CMS / CUPs gemäß [gemSpec\_gSMC-KT\_ObjSys#2]
- Bei Nutzung der Option\_lange\_Lebensdauer\_im\_Feld gemäß [gemSpec\_gSMC-KT\_ObjSys#2] muss ein asymmetrischer Schlüssel für die Authentisierung mit einem CMS / CUPs in das Objekt gemäß [gemSpec\_gSMC-KT\_ObjSys#5.4.14.1] eingebracht werden.
- Nutzung der Option PACE\_PCD gemäß [gemSpec\_gSMC-KT\_ObjSys#2]

Die gSMC-KT kann gemäß [gemSpec\_gSMC-KT\_ObjSys#2] als Testkarte ausgestaltet 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" .....	9
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"...	10
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" .....	12
Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	13
Tabelle 8: Anforderungen zur betrieblichen Eignung "Prozessprüfung" .....	14
Tabelle 9: Anforderungen zur betrieblichen Eignung "Herstellererklärung" .....	14
Tabelle 10: Offene Umsetzungsanforderungen an den Produkttyp .....	15

### 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) <a href="https://www.bsi.bund.de/Schutzprofile">https://www.bsi.bund.de/Schutzprofile</a>
[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)

[Quelle]	Herausgeber: Titel, Version
	<a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile</a>
[SigG01]	Bundesgesetzblatt I (2001), S.876: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)