

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief
Prüfvorschrift
gSMC-KT
**Zulassungsobjekt gSMC-KT-
Objektsystem**

Produkttyp Version: 4.3.0-3
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 19424
Stand: 14.05.2018
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_gSMC-KT_ObjSys_PTV_4.3.0-3

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-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_ObjSys_PTV2.0.2] |
| 4.0.0 | Anpassung an G2 Iteration 2 | [gemProdT_gSMC-KT_ObjSys_PTV4.0.0] |
| 4.0.1 | Anpassung an G2 Iteration 2b | [gemProdT_gSMC-KT_ObjSys_PTV4.0.1] |
| 4.1.0 | Anpassung an G2 Iteration 3 | [gemProdT_gSMC-KT_ObjSys_PTV4.1.0] |
| 4.2.0 | Anpassung an G2 Iteration 4 | [gemProdT_gSMC-KT_ObjSys_PTV4.2.0] |
| 4.3.0 | Einarbeitung der Errata R1.4.1 bis R1.4.6 | [gemProdT_gSMC-KT_ObjSys_PTV4.3.0] |
| 4.3.0-1 | Anpassung auf Releasestand 1.6.3 | [gemProdT_gSMC-KT_ObjSys_PTV4.3.0-1] |
| 4.3.0-2 | Anpassung auf Releasestand 1.6.4 | [gemProdT_gSMC-KT_ObjSys_PTV4.3.0-2] |
| 4.3.0-3 | Anpassung auf Releasestand 2.1.2 | [gemProdT_gSMC-KT_ObjSys_PTV4.3.0-3] |

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 |

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 | Herstellereklärung funktionale Eignung | 12 |
| 3.2 | Anforderungen zur sicherheitstechnischen Eignung | 13 |
| 3.2.1 | Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie | 13 |
| 3.2.2 | CC-Evaluierung | 16 |
| 3.2.3 | Herstellereklärung sicherheitstechnische Eignung..... | 16 |
| 3.3 | Anforderungen zur elektrischen, mechanischen und physikalischen Eignung..... | 17 |
| 4 | Produkttypspezifische Merkmale | 18 |
| 4.1 | Angaben zu EF.Version2..... | 18 |
| 4.2 | Optionale Ausprägungen | 18 |
| 5 | Anhang A – Verzeichnisse | 19 |
| 5.1 | Abkürzungen..... | 19 |
| 5.2 | Tabellenverzeichnis..... | 19 |
| 5.3 | Referenzierte Dokumente..... | 19 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an die Herstellung des Zulassungsobjektes gSMC-KT-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-KT-Objektsystem richtet sich an gSMC-KT-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-KT-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-KT-Objektsystem normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

| Dokumenten Kürzel | Bezeichnung des Dokumentes | Version |
|------------------------------|--|---------|
| gemSpec_OM | Übergreifende Spezifikation Operations und Maintenance | 1.89.0 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.910.0 |
| gemSpec_DS_Hersteller | Spezifikation Datenschutz- und Sicherheitsanforderungen an Hersteller | 1.0.0 |
| gemSpec_gSMC-KT_ObjSys_G2_1 | Spezifikation der gSMC-KT Objektsystem | 4.2.0 |
| gemSpec_PKI | Übergreifende Spezifikation Spezifikation PKI | 2.2.0 |
| gemSpec_Karten_Fach_TIP_G2_1 | Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1 | 3.0.0 |
| gemKPT_Test | Testkonzept der TI | 42.40.0 |
| gemSpec_SMC_OPT | Gemeinsame optische Merkmale der SMC | 3.5.0 |
| gemSpec_Karten_Fach_TIP | Befüllvorschriften für die Plattformanteile der Karten der TI | 2.6.0 |
| gemSpec_gSMC-KT_ObjSys | Spezifikation der gSMC-KT Objektsystem | 3.9.0 |
| gemSpec_Sich_DS | Spezifikation Sicherheits-/Datenschutzanforderungen | 1.4.1 |

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-Prüftool | 1.0 |

Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für das Zulassungsobjekt gSMC-KT-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-KT-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_250 1 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_348 5 | K_Initialisierung: Datenobjekte in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_252 3 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_247 5 | K_Initialisierung: Anzahl logischer Kanäle | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_252 9 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_348 1 | Ausschluss für die Kodierung von Produktidentifikatoren | gemSpec_Karten_Fach_TIP |
| Card-G2-A_247 0 | K_Initialisierung: Verwendung von SE | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_252 6 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_251 8 | K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_348 9 | K_Initialisierung: DO_PI_CHIP in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_348 4 | K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2 | gemSpec_Karten_Fach_TIP |
| Card-G2-A_248 7 | Initialisierung: Initialisierte von MF | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_302 | K_Initialisierung: Initialisierte Attribute von MF / | gemSpec_gSMC- |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------------|---|-----------------------------|
| 8 | PuK.RCA.ADMINCMS.CS.E256 | KT_ObjSys |
| Card-G2-A_347 3 | K_gSMC-KT: Option_PACE_PCD | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_350 4 | K_Initialisierung: Initiale Belegung von EF.KeyInfo für die gSMC-KT | gemSpec_Karten_Fach_ TIP |
| Card-G2-A_287 7 | K_gSMC-KT: Vorhandensein einer USB-Schnittstelle | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_347 9 | Kodierung von Versionskennungen | gemSpec_Karten_Fach_ TIP |
| Card-G2-A_350 1 | K_Initialisierung: Kodierung der Kryptosysteme in EF.KeyInfo | gemSpec_Karten_Fach_ TIP |
| Card-G2-A_349 3 | K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung | gemSpec_Karten_Fach_ TIP |
| Card-G2-A_346 9 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E256 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC- KT_ObjSys |
| GS-A_5026 | Versionierung von Karten durch die Produktidentifikation | gemSpec_OM |
| Card-G2-A_284 9 | K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“ | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_252 4 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.XXXX (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_251 1 | K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256 | gemSpec_gSMC- KT_ObjSys |
| GS-A_5140 | Inhalt der Selbstauskunft von Karten | gemSpec_OM |
| Card-G2-A_248 3 | K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_349 9 | K_Initialisierung: Speicherstruktur für EF.KeyInfo | gemSpec_Karten_Fach_ TIP |
| Card-G2-A_319 4 | K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_346 8 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT2.R2048 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_250 9 | K_Initialisierung: Initialisierte Attribute von MF / EF.Version2 | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_346 1 | K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128 | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_326 9 | K_Initialisierung: Wert von pointInTime | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_287 6 | K_gSMC-KT: Kryptobox | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_247 2 | K_Initialisierung: Ordnerattribute | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_251 2 | K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_302 7 | K_Personalisierung und K_Initialisierung: Historical Bytes im ATR | gemSpec_gSMC- KT_ObjSys |
| Card-G2-A_348 | Kodierung von Produktidentifikatoren | gemSpec_Karten_Fach_ |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|---|-------------------------|
| 0 | | TIP |
| Card-G2-A_3019 | Vorgaben für die Option_lange_Lebensdauer_im_Feld | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3453 | K_Initialisierung: Attribute von MF / EF.KeyInfo | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2522 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2497 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2504 | K_Initialisierung: Initialisierte Attribute von MF / EF.DIR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3486 | K_Initialisierung: DO_BufferSize in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3026 | K_gSMC-KT: USB-Schnittstelle | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3196 | K_Initialisierung: Inhalt persistentPublicKeyList | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3273 | K_Initialisierung: Wert des Attributes root | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2488 | K_Initialisierung: Initialisierte Attribute von MF / EF.ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3488 | K_Initialisierung: DO_PT_COS in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2496 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2481 | K_Personalisierung und K_Initialisierung: ATR-Kodierung | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3490 | K_Initialisierung: DO_PI_COS in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3463 | K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2474 | K_Initialisierung: Zugriffsregeln für besondere Kommandos | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3487 | K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2514 | K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3483 | K_Initialisierung: Inhalt body von EF.Version2 | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3274 | K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2506 | K_Initialisierung: Initialisierte Attribute von MF / EF.GDO | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3491 | K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2519 | K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256 | gemSpec_gSMC-KT_ObjSys |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------------|---|-------------------------|
| Card-G2-A_347 1 | K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_252 7 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.XXXX (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_253 1 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_250 3 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| GS-A_4559 | Versionierung der Karten der TI | gemSpec_OM |
| GS-A_5054 | Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen | gemSpec_OM |
| GS-A_3695 | Grundlegender Aufbau Versionsnummern | gemSpec_OM |
| Card-G2-A_350 5 | K_Initialisierung: Kennungen von EF.KeyInfo für die gSMC-KT | gemSpec_Karten_Fach_TIP |
| Card-G2-A_248 2 | K_Personalisierung und K_Initialisierung: TC1-Byte in ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_253 0 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R3072 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| GS-A_3700 | Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation | gemSpec_OM |

3.1.2 Herstellererklärung funktionale Eignung

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

Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------------|---|------------------------|
| GS-A_3696 | Zeitpunkt der Erzeugung neuer Versionsnummern | gemSpec_OM |
| Card-G2-A_327 6 | K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung | gemSpec_gSMC-KT_ObjSys |
| TIP1-A_6538 | Durchführung von Produkttests | gemKPT_Test |
| TIP1-A_6772 | Partnerprodukte bei Interoperabilitätstests | gemKPT_Test |
| TIP1-A_6526 | Produkttypen: Bereitstellung | gemKPT_Test |
| GS-A_5039 | Änderung der Produktversion bei Änderungen der Produkttypversion | gemSpec_OM |
| GS-A_2162 | Kryptographisches Material in Entwicklungs- und Testumgebungen | gemKPT_Test |
| GS-A_3697 | Anlass der Erhöhung von Versionsnummern | gemSpec_OM |
| TIP1-A_6533 | Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter | gemKPT_Test |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-------------|---|-------------------|
| TIP1-A_6518 | Eigenverantwortlicher Test: TDI | gemKPT_Test |
| GS-A_5038 | Festlegungen zur Vergabe einer Produktversion | gemSpec_OM |
| TIP1-A_6539 | Durchführung von Produktübergreifenden Tests | gemKPT_Test |
| TIP1-A_6517 | Eigenverantwortlicher Test: TBV | gemKPT_Test |
| TIP1-A_6524 | Testdokumentation gemäß Vorlagen | gemKPT_Test |
| TIP1-A_6537 | Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter | gemKPT_Test |
| TIP1-A_6519 | Eigenverantwortlicher Test: Hersteller und Anbieter | gemKPT_Test |
| GS-A_4542 | Spezifikationsgrundlage für Produkte | gemSpec_OM |
| TIP1-A_6532 | Zulassung eines neuen Produkts: Aufgaben der TDI | gemKPT_Test |
| TIP1-A_4191 | Keine Echtdaten in RU und TU | gemKPT_Test |
| TIP1-A_6523 | Zulassungstest: Hersteller und Anbieter | gemKPT_Test |
| TIP1-A_6536 | Zulassung eines geänderten Produkts: Aufgaben der TDI | gemKPT_Test |
| TIP1-A_6516 | Eigenverantwortlicher Test: Test & Transitionmanager | gemKPT_Test |
| TIP1-A_6525 | Produkttypen: Testziele | 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_6535 | Zulassung eines geänderten Produkts: Aufgaben des TBV | gemKPT_Test |

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_2501 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3485 | K_Initialisierung: Datenobjekte in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2523 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2475 | K_Initialisierung: Anzahl logischer Kanäle | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2529 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048 | gemSpec_gSMC-KT_ObjSys |
| GS-A_3696 | Zeitpunkt der Erzeugung neuer Versionsnummern | gemSpec_OM |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------------|---|-------------------------|
| Card-G2-A_348 1 | Ausschluss für die Kodierung von Produktidentifikatoren | gemSpec_Karten_Fach_TIP |
| Card-G2-A_327 6 | K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_247 0 | K_Initialisierung: Verwendung von SE | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_252 6 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_251 8 | K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_348 9 | K_Initialisierung: DO_PI_CHIP in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_348 4 | K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2 | gemSpec_Karten_Fach_TIP |
| Card-G2-A_248 7 | Initialisierung: Initialisierte von MF | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_302 8 | K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_347 3 | K_gSMC-KT: Option_PACE_PCD | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_350 4 | K_Initialisierung: Initiale Belegung von EF.KeyInfo für die gSMC-KT | gemSpec_Karten_Fach_TIP |
| Card-G2-A_347 9 | Kodierung von Versionskennungen | gemSpec_Karten_Fach_TIP |
| Card-G2-A_350 1 | K_Initialisierung: Kodierung der Kryptosysteme in EF.KeyInfo | gemSpec_Karten_Fach_TIP |
| Card-G2-A_349 3 | K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung | gemSpec_Karten_Fach_TIP |
| Card-G2-A_246 9 | K_Initialisierung: Änderung von Zugriffsregeln | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_346 9 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E256 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| GS-A_5026 | Versionierung von Karten durch die Produktidentifikation | gemSpec_OM |
| Card-G2-A_319 7 | K_Initialisierung: Größe persistentPublicKeyList | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_319 5 | K_Initialisierung: Eigenschaften der Objekte in anderen SEs | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_284 9 | K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“ | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_252 4 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.XXXX (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_251 1 | K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256 | gemSpec_gSMC-KT_ObjSys |
| GS-A_5140 | Inhalt der Selbstauskunft von Karten | gemSpec_OM |
| Card-G2-A_247 3 | K_Initialisierung: SFID nicht vorhanden | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_248 | K_Personalisierung und K_Initialisierung: Vorgaben für | gemSpec_gSMC- |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|---|-------------------------|
| 3 | Historical Bytes | KT_ObjSys |
| Card-G2-A_3499 | K_Initialisierung: Speicherstruktur für EF.KeyInfo | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3194 | K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3468 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT2.R2048 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2509 | K_Initialisierung: Initialisierte Attribute von MF / EF.Version2 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3461 | K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3269 | K_Initialisierung: Wert von pointInTime | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2472 | K_Initialisierung: Ordnerattribute | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2476 | K_Terminal: Ausschluss kontaktlose Schnittstelle | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2512 | K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3027 | K_Personalisierung und K_Initialisierung: Historical Bytes im ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3480 | Kodierung von Produktidentifikatoren | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3019 | Vorgaben für die Option_lange_Lebensdauer_im_Feld | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3453 | K_Initialisierung: Attribute von MF / EF.KeyInfo | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2522 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2497 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2504 | K_Initialisierung: Initialisierte Attribute von MF / EF.DIR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3486 | K_Initialisierung: DO_BufferSize in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3196 | K_Initialisierung: Inhalt persistentPublicKeyList | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3273 | K_Initialisierung: Wert des Attributes root | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2488 | K_Initialisierung: Initialisierte Attribute von MF / EF.ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3488 | K_Initialisierung: DO_PT_COS in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2496 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2481 | K_Personalisierung und K_Initialisierung: ATR-Kodierung | gemSpec_gSMC-KT_ObjSys |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|---|-------------------------|
| Card-G2-A_3490 | K_Initialisierung: DO_PI_COS in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3463 | K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2474 | K_Initialisierung: Zugriffsregeln für besondere Kommandos | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3487 | K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2514 | K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3483 | K_Initialisierung: Inhalt body von EF.Version2 | gemSpec_Karten_Fach_TIP |
| Card-G2-A_3274 | K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2506 | K_Initialisierung: Initialisierte Attribute von MF / EF.GDO | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3491 | K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2519 | K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256 | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_3471 | K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2527 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.XXXX (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2531 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2503 | K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| GS-A_4559 | Versionierung der Karten der TI | gemSpec_OM |
| GS-A_3695 | Grundlegender Aufbau Versionsnummern | gemSpec_OM |
| Card-G2-A_3505 | K_Initialisierung: Kennungen von EF.KeyInfo für die gSMC-KT | gemSpec_Karten_Fach_TIP |
| Card-G2-A_2482 | K_Personalisierung und K_Initialisierung: TC1-Byte in ATR | gemSpec_gSMC-KT_ObjSys |
| Card-G2-A_2530 | K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R3072 (Option_lange_Lebensdauer_im_Feld) | gemSpec_gSMC-KT_ObjSys |
| GS-A_3700 | Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation | gemSpec_OM |

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_4945-01 | Produktentwicklung: Qualitätssicherung | gemSpec_DS_Hersteller |
| GS-A_4946-01 | Produktentwicklung: sichere Programmierung | gemSpec_DS_Hersteller |
| GS-A_4380 | Card-to-Server (C2S) Authentisierung und Trusted Channel G2 | gemSpec_Krypt |
| GS-A_4947-01 | Produktentwicklung: Schutz der Vertraulichkeit und Integrität | gemSpec_DS_Hersteller |
| GS-A_4381 | Schlüssellängen Algorithmus AES | gemSpec_Krypt |
| GS-A_4366 | CV-CA-Zertifikate G2 | gemSpec_Krypt |
| GS-A_2525-01 | Hersteller: Schließen von Schwachstellen | 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_4365 | CV-Zertifikate G2 | gemSpec_Krypt |
| GS-A_4944-01 | Produktentwicklung: Behebung von Sicherheitsmängeln | gemSpec_DS_Hersteller |
| GS-A_5021 | Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung | gemSpec_Krypt |
| GS-A_4367 | Zufallszahlengenerator | gemSpec_Krypt |
| GS-A_2330-02 | Hersteller: Schwachstellen-Management | gemSpec_DS_Hersteller |
| GS-A_4368 | Schlüsselerzeugung | gemSpec_Krypt |
| GS-A_2524-01 | Produktunterstützung: Nutzung des Problem-Management-Prozesses | gemSpec_DS_Hersteller |
| 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_351 3 | Bemäßung der Kontakte der (g)SMC | gemSpec_SMC_OPT |
| Card-G2-A_347 8 | Elektrophysikalische Eigenschaften des Kartenkörpers der (g)SMC | gemSpec_SMC_OPT |

4 Produkttypspezifische Merkmale

4.1 Angaben zu EF.Version2

Die detaillierte Versionskennzeichnung der gSMC-KT wird im Dokument [gemSpec_Karten_Fach_TIP] festgelegt.

4.2 Optionale Ausprägungen

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

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec_gSMC-KT_ObjSys#4.3.2]
- Vorbereitung der gSMC-KT-Objektsystem für längere Laufzeit im Feld gemäß [gemSpec_gSMC-KT_ObjSys#2]
- 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.

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" | 12 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie"..... | 13 |
| Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" | 17 |
| Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung | 17 |

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 |