Elektronische Gesundheitskarte und Telematikinfrastruktur

Errata 5 zum Konnektor PTV 3 (eMP/AMTS, NFDM)

Version:	1.0.0
Stand:	04.02.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_5_Kon_PTV3]

betroffener Produkttyp	**neue Produkttypversion:**
gemProdT_Kon_PTV3	PTV3.6.0-1

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente*
C_7124	gemSpec_Kon		**Nur Konnektoren mit dual-personalisierten gSMC-K** Ab dem 01.07.2020 dürfen nur Konnektoren mit dual-personalisierten Karten (gSMC-K) ausgeliefert werden.	Siehe C_7124_Anlage	gemSpec_Kon gemProdT_Kon_PTV3
C_7123	gemProdT_Kon_PTV3		**Herstellererklärung zur Herausgabe der gSMC-K** Der Konnektorhersteller ist verantwortlich für die Herausgabe der gSMC-K. Die Anforderungen zur Personalisierung der gSMC-K werden im Konnektor-Produkttypsteckbrief abgebildet und dort dem Prüfverfahren "Herstellererklärung funktionale Eignung" zugeordnet. Dazu wird eine eigene Tabelle für die Anforderungen an die gSMC-K-Herausgabe im Abschnitt "Herstellererklärung funktionale Eignung" eingefügt.	Siehe C_7123_Anlage	gemProdT_Kon_PTV3

Änderungen in [gemProdT_Kon_PTV3, gemProdT_Kon_PTV4]

3.1.2 Herstellererklärung funktionale Eignung

[Neue Tabelle am Ende von Kapitel 3.1.2:]

Tabelle 7: Anforderungen zur funktionalen Eignung "Herstellererklärung" zur Herausgabe der gSMC-K

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2575	Zugelassenes Zugriffsprofil im CV-Rollen-Zertifikat	gemSpec_CVC_TSP
TIP1-A_2578	Korrekte ICCSN der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2589	Personalisierung des CVC-CA-Zertifikats	gemSpec_CVC_TSP
Card-G2-A_3734	K_Personalisierung: Personalisierte Attribute von MF/DF.AK/EF.C.AK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3735	K_Personalisierung: Personalisierte Attribute von MF/DF.AK/PrK.AK.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3738	K_Personalisierung: Personalisierte Attribute von MF/DF.AK/PrK.AK.CA_PS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3740	K_Personalisierung: Personalisierte Attribute von MF/DF.NK/EF.C.NK.VPN2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3741	K_Personalisierung: Personalisierte Attribute von MF/DF.NK/PrK.NK.VPN.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3744	K_Personalisierung: Personalisierte Attribute von MF/DF.SAK/EF.C.SAK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3745	K_Personalisierung: Personalisierte Attribute von MF/DF.SAK/PrK.SAK.AUT.E256	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_2538	K_Initialsierung: Anzahl logischer Kanäle	gemSpec_gSMC-K_ObjSys
Card-G2-A_2665	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_gSMC-K_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_3261	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_2994	K_Personalisierung: Absicherung der Kartenadministration	gemSpec_gSMC-K_ObjSys
Card-G2-A_2541	K_Personalisierung: zusätzliche Ordner	gemSpec_gSMC-K_ObjSys
Card-G2-A_2542	K_Personalisierung: zusätzliche Objekte	gemSpec_gSMC-K_ObjSys
Card-G2-A_2544	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_gSMC-K_ObjSys
Card-G2-A_2545	K_Personalisierung: Wert des Attributes iccsn8	gemSpec_gSMC-K_ObjSys
Card-G2-A_3514	K_Personalisierung: personalisierter Wert von pointInTime	gemSpec_gSMC-K_ObjSys
Card-G2-A_2547	K_Personalisierung und K_Initialisierung: ATR-Kodierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_2548	K_Personalisierung und K_Initialisierung: TC1 Byte im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2997	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_3041	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_gSMC-K_ObjSys
Card-G2-A_3394	K_Personalisierung: Personalisierte Attribute von MF / EF.EnvironmentSettings	gemSpec_gSMC-K_ObjSys
Card-G2-A_2567	K_Personalisierung: Personalisiertes Attribut von EF.GDO	gemSpec_gSMC-K_ObjSys
Card-G2-A_3393	K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SAK.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3580	K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten	gemSpec_gSMC-K_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3581	K_Personalisierung: Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3328	K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3329	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3331	K_externe Welt: Festlegung von CHR für EF.C.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2570	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3396	K_Personalisierung: Personalisierte Attribute von MF / PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3397	K_Personalisierung: Personalisierte Attribute von MF / PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3398	K_Personalisierung: Personalisierte Attribute von MF / PIN.Pers	gemSpec_gSMC-K_ObjSys
Card-G2-A_3399	K_Personalisierung: Personalisierte Attribute von MF / PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3333	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3400	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3338	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3376	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3380	K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3382	K_Personalisierung: Personalisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3401	K_Personalisierung: Personalisierte Attribute von MF / PrK.GP.R2048	gemSpec_gSMC-K_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3402	K_Personalisierung: Personalisierte Attribute von MF / PuK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3262	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3403	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3404	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3405	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3447	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3449	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3450	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3406	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3407	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3410	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3411	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3416	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3417	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PuK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3423	K_Personalisierung: Personalisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3424	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_2638	K_Personalisierung: CHR von C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3429	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3430	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2640	K_Personalisierung: CHR von C.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3431	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3434	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3582	K_Personalisierung: Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3583	K_Personalisierung: Personalisierte Attribute von MF / EF.C.TSL.CA_1 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3438	K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_3439	K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA	gemSpec_gSMC-K_ObjSys
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3495	K_Personalisierung: DO_PI_Personalisierung in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP
Card-G2-A_3496	K_Initialisierung: Weitere Datenobjekte in DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3497	K_Personalisierung: Vollständige Befüllung von EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TIP
Card-G2-A_3507	K_Personalisierung Versionierung Inhalte von EF.EnvironmentSettings	gemSpec_Karten_Fach_TIP
Card-G2-A_3509	K_Personalisierung Inhalt von EF.EnvironmentSettings	gemSpec_Karten_Fach_TIP
GS-A_4707	Kennzeichen für Technische Rolle für Komponenten und Dienste	gemSpec_PKI
GS-A_4605	Verwendung registrierter Daten für gSMC-K-Zertifikatsbeantragung	gemSpec_PKI
GS-A_4606	Identischer ICCSN in allen Zertifikaten einer gSMC-K	gemSpec_PKI
GS-A_4974	CV-Ausstattung von Smartcards der TI	gemSpec_PKI
GS-A_4622	Zugriffsprofil einer gSMC-K	gemSpec_PKI
GS-A_5335	Zugriffsprofil einer gSMC-K für Administrationszwecke	gemSpec_PKI
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
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_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	gemSpec_OM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4560	Versionierung von Datenstrukturen der Karten der TI	gemSpec_OM
Card-G2-A_3850	K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung	gemSpec_gSMC-K_ObjSys
GS-A_5020	Einbringung des Komponentenzertifikats durch den Kartenherausgeber	gemRL_TSL_SP_CP

Marktwirksame Kennzeichnung von Konnektoren mit ECC-Vorbereitung

Um abzusichern, dass mit der Umstellung der Telematikinfrastruktur auf den ECC-Algorithmus in vier Jahren alle Konnektoren, die ab Mitte 2020 installiert werden, per Softwareupdate umgestellt werden können, wird die Vorbereitung von ECC-Zertifikaten auf der gSMC-K in der Spezifikation neu geregelt.

Dazu wird eine Verpflichtung aufgenommen, ab Mitte 2020 nur ECC-personalisierte gSMC-K auszuliefern.

Mit dem Konnektor PTV4 wird die ECC-Personalisierung der gSMC-K im Administratorinterface sichtbar.

Durch die Anforderung zur Unterstützung von beiden Personalisierungsvarianten wird eine Abbildung in einem Zulassungverfahren ermöglicht.

Änderungen in [gemSpec_Kon]

3.1 Konnektoridentität und gSMC-K

[…]

TIP1-A_4506 - Initiale Identitäten der gSMC-K
In Abhängigkeit vom kryptographischen Verfahren MUSS der Konnektor folgende Objekte der gSMC-K als Quelle seiner Identitäten verwenden:

Tabelle: TAB_KON_856: Identitäten des Konnektors auf der gSMC-K

Identifier	Verzeichnis	Objekt der gSMC-K in Abhängigkeit vom kryptographischen Verfahren	
		RSA	ECC
ID.NK.VPN	MF/DF.NK	EF.C.NK.VPN.R2048	EF.C.NK.VPN2.XXXX
ID.AK.AUT	MF/DF.AK	EF.C.AK.AUT.R2048	EF.C.AK.AUT2.XXXX
ID.SAK.AUT	MF/DF.SAK	EF.C.SAK.AUT.R2048	EF.C.SAK.AUT2.XXXX
C.SAK.AUTD_CVC	MF/DF.SAK	-	EF.C.SAK.AUTD_CVC.E256

<=

3.1.1 Organisatorische Anforderungen und Sperrprozesse

[…]

[Neue Anforderungen einfügen nach TIP1-A_5696:]

A_18928 – Ausstattung mit dual-personalisierten gSMC-K-X.509-Zertifikaten

Der Hersteller des Konnektors MUSS die Konnektoren mit einer gSMC-K mit personalisierten RSA- und ECC-Zertifikaten gemäß TAB_KON_856 ausstatten.

<=

Die Afo A_18928 wird dem Konnektor PTV1, PTV2, PTV3 und PTV4 zugewiesen und dort jeweils dem Prüfverfahren „funkt. Eignung: Herstellererklärung“ zugeordnet.

Änderungen in [gemProdT_Kon_PTV1, gemProdT_Kon_PTV2, gemProdT_Kon_PTV3]

[Neues Kapitel:]

4.4 Zeitliche Gültigkeit von Anforderungen

Die Anforderungen in Tabelle Tab_gSMC-K_Kon_HW_Version gelten spätestens ab dem 01.07.2020 für Konnektoren, die noch nicht beim Leistungserbringer in Betrieb genommen sind.

Tabelle 1: Tab_gSMC-K_Kon_HW_Version

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_18928	Ausstattung mit dual-personalisierten gSMC-K-X.509-Zertifikaten	gemSpec_Kon