

Elektronische Gesundheitskarte und Telematikinfrastruktur

Errata 5 zum Konnektor PTV1 (VSDM) und PTV2 (QES) Online-Produktivbetrieb (Stufe 1)

Version: 1.0.0
Stand: 04.02.2020
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: [gemErrata_5_Kon_PTV1_PTV2]

Betroffene Produkttypen

gemProdT_Kon_PTV1 gemProdT_Kon_PTV1.10.3-1
gemProdT_Kon_PTV2 gemProdT_Kon_PTV2.12.1-1

ID	Dokument	Quelle	Beschreibung der Änderung	Anpassung 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_PTV1 gemProdT_Kon_PTV2

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 Zulassungsverfahren 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

Identifizier	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