SRQ - Specification Related Question

SRQ-ID: 0949

Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Kodierung Transportschutz für PIN.QES
zu Dokument / Datei	[gemSpec_eGK_P2]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Kapitel 7.7

Stichwort: Kodierung Transportschutz für PIN.QES

Frage:

(N993200) verweist auf [gemSpec_eGK_P1] Tabelle 9 „Transportschutzkodierung“. Die Referenzierung bezieht sich dabei auf die neueste Version, also auf [gemSpec_eGK_P1] in der Version 2.2.2. Dieser Verweis ist erstens nicht mehr richtig und zweitens enthält die Tabelle 10 in [gemSpec_eGK_P1] "Transportschutzkodierung" im Gegensatz zu vorhergehenden Versionen nicht mehr die Spalte "Kodierung". Wie ist das in (N993200) definierte Wertfeld zu kodieren?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☐ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Diese SRQ ist zulassungsrelevant für alle Zulassungen, die auf dem Dokument [gemSpec_eGK_P2] basieren und nach dem 05.12.2008 bescheinigt werden.

Hierbei handelt es sich um eine Inkonsistenz zwischen den Dokumenten [gemSpec_eGK_P1] und [gemSpec_eGK_P2], die durch eine Überarbeitung des Teils 1 entstanden ist.

Die in [gemSpec_eGK_P2] (N993.200) spezifizierte Kodierung des Wertfeldes ergibt sich mittels [gemSpec_eGK_P1] Tabelle 10 in Verbindung mit [gemSpec_eGK_P1] Tabelle 107, wobei dort die vier niederwertigsten Bit des Trailers zu verwenden sind. Dadurch wird die ursprüngliche Aussage des Textes wieder hergestellt.

Allerdings ist festzuhalten, dass der Inhalt dieses Wertfeldes statisch ist und damit ähnlich problematisch, wie seinerzeit die Verwendung von EF.StatusPin, da es nach Aufheben des Transportschutzes zwangsläufig zu Inkonsistenzen zwischen dem in (N993.200) definierten Wert und den Eigenschaften von PIN.QES kommt. Zumindest alternativ sollte es deshalb möglich sein, den Status des Transportschutzes mittels "GET PIN STATUS" abzufragen.

Insgesamt führt dies zu folgenden Änderungen am Dokument

Änderung 1:

Der Text von (N993200) ist durch folgenden zu ersetzen:

(N32) K_Personalisierung

Das vierte Datenobjekt des Wertfeldes MUSS ein Tag = ´C4´ besitzen. Das Wertfeld dieses Datenobjektes MUSS aus einem Oktett bestehen und enthält Informationen zum Wert der Transport–PIN (siehe Kapitel 7.5). Das Wertfeld wird gemäß [gemSpec_eGK_P1] Tabelle 9 „Transportschutzkodierung“ in Verbindung mit [gemSpec_eGK_P1] Tabelle 106 „GET PIN STATUS Antwort APDU im Erfolgsfall“ kodiert und MUSS folgendes Oktett enthalten I2OS(Trailer mod 16, 1). Falls dabei der Wert „Transport–PIN_Zufallszahl“ angezeigt wird, so SOLL der Wert der Datei EF.BVD (siehe Kapitel 7.7.2) entnommen werden.

Änderung 2:

In Tabelle 51 für EF.ASD soll im Zustand "Operational state (activated)" das Auslesen von Information möglich sein. Deshalb ist in der Tabelle der Block mit den Zugriffsregeln durch folgenden zu ersetzen:

Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	

Änderung 3:

Der Status des Transportschutzes für PIN.QES soll auch vor Abschluss des Nachladevorgangs also noch im logisch deaktivierten Zustand von PIN.QES möglich sein. Deshalb wird das komplette Kapitel 7.7.6 durch folgendes ersetzt:

7.7.6 / MF / DF.QES / PIN.QES

Dieses Benutzergeheimnis wird zur Freischaltung der Signaturfunktionalität mit dem Schlüssel PrK.CH.QES (siehe Kapitel 7.7.7) benötigt.

Tabelle 57: Attribute / MF / DF.QES / PIN.QES

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	siehe Hinweis 74:
startRetryCounter	3	
retryCounter	3	
transportStatus	…	wird personalisiert
flagEnabled	True	
startSsec	1	alle SE
PUK	…	wird personalisiert
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=0	ALWAYS	siehe Hinweis 75:
GET PIN STATUS	ALWAYS	
RESET RC., P1=1	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD	nicht Gegenstand dieser Spezifikation	siehe Hinweis 76:
GET PIN STATUS	ALWAYS	
alle	NEVER	

Hinweis 73: Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Passwortobjekt arbeiten, sind:
CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER, VERIFY

Hinweis 74: Gemäß [gemSpec_eGK_P1] kontrolliert das Betriebssystem der eGK lediglich die Mindestlänge. Die Maximallänge der PIN.QES beträgt acht Stellen. Die Einhaltung der Bedingung für die Maximallänge wird nicht von der eGK kontrolliert.

Hinweis 75: Die oben angegebene Zugriffsart für das Kommando CHANGE REFERENCE DATA gilt nur für den Fall, dass kein Transportschutz für dieses Passwortobjekt besteht. Je nach verwendetem Transportschutzverfahren KANN zur Aufhebung des Transportschutzes auch eine andere CHANGE REFERENCE DATA Variante verwendet werden.

Hinweis 76: Ob, und falls ja, unter welchen Voraussetzungen im Zustand "Operational state (deactivated)" das Kommando CHANGE REFERENCE DATA möglich ist, wird in diesem Dokument nicht festgelegt. Die Festlegung erfolgt im Rahmen des Bestätigungsverfahrens.