SRQ - Specification Related Question

SRQ-ID: 0946

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

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Geänderte PIN Initialisierung
zu Dokument / Datei	[gemSpec_eGK_P2]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Kapitel 6.2.7, Kapitel 6.2.8

Stichwort: Geänderte PIN Initialisierung

Frage:

Welche Auswirkungen hat das neue PIN-Initialisierungskonzept auf PIN.CH und PIN.home?

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.

Durch das neue Konzept zur PIN Initialisierung ist es nicht mehr möglich PIN.CH außerhalb der Telematikinfrastruktur zu verändern, oder PIN.home transportgeschützt ins Feld zu bringen.

Deshalb sind die Kapitel 6.2.7 und 6.2.8 komplett durch den hier gezeigten Inhalt zu ersetzen:

6.2.7 / MF / PIN.CH

Dieses Passwortobjekt wird zur Freischaltung von Schlüsseln und Inhalten der eGK verwendet. Dieses Passwortobjekt wird nur innerhalb der TI verwendet.

Tabelle 13: Attribute / MF / PIN.CH

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	siehe Hinweis 18:
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword, Leer–PIN_1, Leer–PIN_2, Transport–PIN_0000}	siehe Hinweis 19:
flagEnabled	True	
startSsec	unendlich	alle SE
PUK	…	siehe (N991.800)
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=1	C.1.2.3.4.8.9	siehe Hinweis 20:
	herstellerspezifisch	siehe (N991.810)
CHANGE RD, P1=0	C.1.2.3.4.8.9	siehe Hinweis 21:
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	C.1.2.3.4.8.9	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis 17: Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Passwortobjekt arbeiten, sind: CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER, VERIFY

Hinweis 18: Gemäß [gemSpec_eGK_P1] kontrolliert das Betriebssystem der eGK lediglich die Mindestlänge. Die Maximallänge von PIN.CH und PIN.home beträgt acht Stellen. Die Einhaltung der Bedingung für die Maximallänge wird nicht vom COS der eGK kontrolliert.

Hinweis 19: Die Anforderung an die Ausgabeprozesse für PIN.home und PIN.CH sind im Dokument [gemCMS_PINPUK] festgelegt.

Hinweis 20: Diese Tabellenzeile gilt für den Fall, dass transportStatus gleich Leer–PIN_1 ist.

Hinweis 21: Diese Tabellenzeile gilt für den Fall, dass transportStatus ungleich Leer–PIN_1 ist.

(N991.800) K_Personalisierung

Bei der Personalisierung MUSS eine PUK mit acht Ziffern gewählt werden.

(N991.810) K_Personalisierung

Wenn als Transportschutz Leer–PIN_1 verwendet wird, dann DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Diese Anforderung ist herstellerspezifisch umzusetzen.

6.2.8 / MF / PIN.home

Dieses Passwortobjekt wird zur Freischaltung von Schlüsseln und Inhalten der eGK der TI verwendet. Dieses Passwortobjekt wird nur außerhalb der TI verwendet.

Tabelle 14: Attribute / MF / PIN.home

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´02´ = 2	
secret	…	wird personalisiert
minimumLength	6	siehe Hinweis 18:
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword}	siehe Hinweis 19:
flagEnabled	True	
startSsec	unendlich	alle SE
PUK	…	siehe (N991.900)
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis 22: Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Passwortobjekt arbeiten, sind:
CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER, VERIFY

(N991.900) K_Personalisierung
Bei der Personalisierung MUSS eine PUK mit acht Ziffern gewählt werden.