SRQ - Specification Related Question

SRQ-ID: 0950

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

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Verwendung Security Environment
zu Dokument / Datei	[gemSpec_eGK_P2]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Kapitel 6, Kapitel 7

Stichwort: Verwendung Security Environment

Frage:

Welche Security Environaments muss eine eGK unterstützen?

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.

Derzeit wird nur für PrK.eGK.AUT_CVC ein unterschiedliches Verhalten in Abhängigkeit vom aktiven Security Environment gefordert. Dies hat historische Gründe. Da sich die Wahl des Security Environments auf kein anderes Objekt innerhalb der eGK auswirkt, ist die Unterscheidung der Security Environments für PrK.eGK.AUT_CVC obsolet. Deshalb wird die Konfiguration der eGK so geändert, dass (die folgende Darstellung ist informativ, normative Festlegungen folgen weiter unten)

a) PrK.eGK.CVC_AUT im Security Environment SE#1 eine Authentisierung sowohl mit, als auch ohne Aushandlung von Sessionkeys vorzunehmen in der Lage ist.

b) das Verhalten der eGK nur im Security Environment SE#1 normativ festgelegt wird. Das Verhalten in anderen Security Environments ist damit nicht mehr zulassungsrelevant.

Das neue Security Environment Konzept wirkt sich wie folgt normativ auf das Dokument aus:

Änderung 1:

Der Text von (N2) ist durch folgenden zu ersetzen:

(N2) K_Personalisierung

Dieses Dokument legt das Verhalten aller Objekte im Security Environment SE#1 normativ fest. Das Verhalten in Security Environments mit einer anderen Nummer als SE#1 wird durch dieses Dokument nicht festgelegt.
.Hinweis: Die auf dem Protection Profile zur eGK basierende Evaluierung gewährleistet, dass eine mögliche Nutzung in von SE#1 abweichenden Security Environments die hier spezifizierte Sicherheit nicht untergräbt.

a. Alle Angaben zu Objekten (Ordnern, Dateien, Passworten und Schlüsseln) in diesem Objekt beziehen sich ausschließlich auf das Security Environment SE#1. Im SE#1 MÜSSEN alle Objekte die in diesem Dokument festgelegten Eigenschaften aufweisen.

b. Die Nutzung von Objekten außerhalb von SE#1 KANN möglich sein. Falls die Nutzung möglich ist, dann sind die Objekteigenschaften außerhalb von SE#1 herstellerspezifisch.

c. Die Nutzung von Objekten außerhalb von SE#1 KANN durch das COS unterbunden werden.

Änderung 2:

In allen Tabellen ist der Passus

Zugriffsregel für logischen LCS „Operational state (activated)", alle SE

durch folgenden zu ersetzen

Zugriffsregel für logischen LCS „Operational state (activated)"

Änderung 3:

In Tabelle 12 für PIN.CH und in Tabelle 13 für PIN.home ist der Passus

startSsec	unendlich	alle SE

durch folgenden zu ersetzen

startSsec	unendlich	

Änderung 4:

In Tabelle 14 ist für PrK.eGK.AUT_CVC der Passus

algorithmIdentifier	Werte gemäß [gemSpec_eGK_P1] rsaRoleAuthentication falls SE#1 rsaSessionkey4SM falls SE#2	

durch folgenden zu ersetzen

algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {rsaRoleAuthentication, rsaSessionkey4SM}	

Änderung 5:

In Tabelle 40 ist für PrK.CH.AUT der Passus

algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}	für SE#1, SE#2

durch folgenden zu ersetzen

algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}	

Änderung 6:

In Tabelle 48 für PIN.QES ist der Passus

startSsec	1	alle SE

durch folgenden zu ersetzen

startSsec	1	

Änderung 7:

In Tabelle 60 ist für SK.Admin der Passus

algorithmIdentifier	desSessionkey4SM, siehe [gemSpec_eGK_P1]	für alle SE

durch folgenden zu ersetzen

algorithmIdentifier	desSessionkey4SM, siehe [gemSpec_eGK_P1]	