FaQ-ID: 0051

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

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Erläuterung SRQ 0887 (Nachladen QES)
zu Dokument / Datei	[gemSpec_eGK_P2]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	7.2, 7.3.2

Stichwort: Erläuterung SRQ 0887 (Nachladen QES)

Frage:

In SRQ 0887 ist nicht ersichtlich, welche Vorgaben für den Nachladeprozess gelten, da lediglich auf die Inhalte des Dokuments [gemSpec_eGK_P2] in der Nachfolgeversion 2.2.1 verwiesen wird. Wie sollen die betroffenen Kapitel in der im Basis-Rollout gültigen Dokumentenversion 2.2.0 aussehen?

Betrifft (wird vom PB ausgefüllt):

gültig ab (Datum)	22.11.2011	Verbindlichkeit	informativ
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:

Es ist korrekt, dass allein aus dem Basisdokument [gemSpec_eGK_P2] in der Version 2.2.0 und SRQ 0887 nicht ersichtlich ist, welche Vorgaben für den QES-Nachladeprozess im Basis-Rollout gelten.

SRQ 0887 verweist lediglich auf die Inhalte des Dokuments [gemSpec_eGK_P2] in der Version 2.2.1. Diese Dokumentenversion ist dem abgekündigten Release 2.3.4

zugeordnet. Bis zur Abkündigung des Releases 2.3.4 war der Verweis in SRQ 0887 hinreichend.

Die betroffenen Kapitel aus der Version 2.2.1 sind nachfolgend aufgeführt:

7.2 Optionen für unvollständige QES-Anwendung

Die Unterkapitel 7.2 bis einschließlich 7.9 befinden sich derzeit in der Abstimmung mit der T7 Gruppe. Deshalb ist es möglich, dass sich deren Inhalt ändert.[1]

Dieses Unterkapitel behandelt die verschiedenen Optionen, zwischen denen es einem ZDA möglich ist zu wählen, wenn die eGK im Auslieferungszustand keine nutzbare QES-Anwendung enthält.

Zunächst ist festzuhalten, dass die QES-Anwendung im hier behandelten Fall erst nutzbar ist, wenn gewisse Schritte erfolgreich ausgeführt wurden. Weil diese Schritte sicherheitsrelevant sind, ist technisch zu verhindern, dass sie von Unberechtigten ausführbar sind. Mit anderen Worten: Nur ein ZDA ist in der Lage, die notwendigen Schritte auszuführen. Deshalb sind in den Prozess folgende ZDAs eingebunden:

- ZDA–VP: ZDA, der die Vorpersonalisierung durchführt, dies kann auch ein von einem ZDA beauftragter Dritter gemäß § 4 Abs. 5 SigG sein.
- ZDA–NL: ZDA gemäß § 2 Nr. 8 SigG, der die Komplettierung der QES-Anwendung durchführt.

In Kapitel 7.3 werden die Optionen zum Aufbau eines geschützten Kommunikationskanals beschrieben. Dieser geschützte Kanal stellt sicher, dass nur Berechtigte die antizipierten Schritte ausführen. Als Optionen stehen dem ZDA–VP zur Verfügung:

- „TC.sym.DF“ gemäß Kapitel 7.3.1,
- ~~„TC.asym.PrkMF.PukMF“ gemäß Kapitel 7.3.2.1,~~
- ~~„TC.asym.PrkMF.PukDF“ gemäß Kapitel 7.3.2.2~~ ~~und~~
- „TC.asym.PrkDF.PukDF“ gemäß Kapitel 7.3.2.3[2].

~~Die Option, dass der private Schlüssel DF-spezifisch ist und der öffentliche Schlüssel einer Root-CA des MFs zugeordnet ist, wird hier lediglich der Vollständigkeit halber erwähnt und nicht weiter betrachtet.~~

Des Weiteren hat der ZDA–VP die Wahl, ob das Schlüsselmaterial des Signaturschlüssels bei der Auslieferung vorhanden ist oder nicht. Dies wird in Kapitel 7.4 behandelt. Als Optionen stehen dem ZDA–VP zur Verfügung:

- „qesKeyNotAvailable“ gemäß Kapitel 7.4.1,

[1] Dieser Hinweis ist inzwischen nicht mehr erforderlich.

[2] Hinweis: Der Aufbau eines Trusted Channels mittels asymmetrischer Schlüssel wird in Kapitel 7.3.2 beschrieben. Die untergeordnete Kapitelstruktur entfällt durch die in Kapitel 7.3.2 vorgenommenen Streichungen.

- „qesPukReadable“ gemäß Kapitel 7.4.2.1 und
- „qesPukCertificate“ gemäß Kapitel 7.4.2.2.

Falls ein Brief an den Karteninhaber der eGK zu versenden ist, der Daten zur Benutzerverifikation enthält (PIN / PUK Brief), so werden in den Kapiteln 7.5 und 7.6 Verfahren beschrieben, wie der ZDA–NL in den Besitz dieser Werte gelangt. Als Optionen stehen dem ZDA–VP die in [gemSpec_eGK_P1] Kapitel 9.2.5 definierten Verfahren zur Verfügung.

Falls dabei ein Verfahren aus der Menge {

- „Transport–PIN_Zufallszahl“ (siehe Kapitel 7.5.1),
- „Transport–PIN_abgeleitet“ (siehe Kapitel 7.5.2)

} eingesetzt wird, dann beschreiben die zuvor referenzierten Kapitel, wie der ZDA–NL Kenntnis vom Wert der Transport–PIN erhält.

Aus dem technischen Blickwinkel der eGK ist es einem ZDA–VP möglich aus jedem der Unterkapitel 7.3, 7.4, 7.5 und 7.6 eine Option auszuwählen, wobei die jeweilige Auswahl in einem Unterkapitel völlig unabhängig von der Wahl in anderen Unterkapiteln ist. Es ist nicht Gegenstand dieses Dokumentes festzulegen, ob alle theoretisch möglichen Kombinationsmöglichkeiten auch in der Praxis genutzt werden.

…

7.3.2 Trusted Channel mittels asymmetrischer Schlüssel

~~Je nach Speicherort des verwendeten Schlüsselmaterials wird hier zwischen verschiedenen Verfahren unterschieden.~~

(N992100) K_NachladenQES[3]

Die gegenseitige Authentisierung und die Aushandlung von Sessionkeys MUSS gemäß [gemSpec_eGK_P1] Kapitel 16.4.2 „RSA Schlüssel“ erfolgen. Als *algorithmIdentifier* wird dabei stets rsaSessionkey4SM verwendet.

7.3.2.1 ~~Privater Schlüssel global, öffentlicher Schlüssel global~~

7.3.2.2 ~~Privater Schlüssel global, öffentlicher Schlüssel DF–spezifisch~~

7.3.2.3 ~~Privater Schlüssel DF–spezifisch, öffentlicher Schlüssel DF–spezifisch~~

In der Variante TC.asym.PrkDF.PukDF basiert die gegenseitige Authentisierung auf einem

- privaten Schlüsselobjekt PrK.eGK.ZDA_AUT (siehe Tabelle 59)[4] zusammen mit dem ihm zugeordneten CV-Zertifikat in Kapitel 7.7.5 und

[3] Hinweis: In der Dokumentenversion 2.2.0 wird dieser Punkt als (N21) bezeichnet.

[4] Hinweis: In der Dokumentenversion 2.2.0 wird an dieser Stelle Tabelle 58 referenziert.

- öffentlichen Schlüsselobjekt PuK.RCA–ZDA.CS (siehe Tabelle 60)[5], welches für den Import von Zertifikatsketten (siehe [gemSpec_eGK_P1] Kapitel 15.8.6) verwendet wird.

[5] Hinweis: In der Dokumentenversion 2.2.0 wird an dieser Stelle Tabelle 59 referenziert.