SRQ - Specification Related Question

SRQ-ID: 0944

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

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Verwendung Authentisierungsschlüssel CH.AUT und CH.AUTN
zu Dokument / Datei	[gemSpec_eGK_P2]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Tabelle 40, Tabelle 41

Stichwort: Verwendung der Schlüssel CH.AUT und CH.AUTN

Frage:

In [gemSpec_eGK_P2] sind für die AUT und AUTN Schlüssel folgende Algorithmen angegeben:

- PrK.CH.AUT: {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}

- PrK.CH.AUTN: rsaClientAuthentication

Da PrK.CH.AUTN auch für XML-Signaturen verwendet werden soll, müssten die gleichen Algorithmen wie bei PrK.CH.AUT zugelassen sein, oder?

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.

Wie in der Fragestellung beschrieben, wird in [gemSpec_eGK_P2] Version 2.2.0 Kapitel 6.4.7 der Schlüssel PrK.CH.AUTN fälschlicherweise nicht so konfiguriert, wie vorgesehen. Auch PrK.CH.AUTN soll im Rahmen von Nachrichtensignaturen und fortgeschrittenen Signaturen eingesetzt werden. Daraus ergeben sich für [gemSpec_eGK_P2] Version 2.2.0 folgende Änderungen:

Ersetze für PrK.CH.AUTN in Tabelle 41 die Menge der zugelassenen algorithmIdentifier durch folgende: {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}