SRQ - Specification Related Question

SRQ-ID: 1205

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	maximale Gültigkeitsdauer von schon erzeugten CVC-Root-CA-Zertifikaten und CVC-Sub-CA-Zertifikaten und die mit ihnen verbundenen Schlüssel
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anhang F - Kryptographiekonzept TI

Stichwort: maximale Gültigkeitsdauer von schon erzeugten CVC-Root-CA-Zertifikaten und CVC-Sub-CA-Zertifikaten und die mit ihnen verbundenen Schlüssel

Frage:

Welche Entscheidung bezüglich der maximalen Gültigkeitsdauer von CVC-Root-CA-Zertifikaten und CVC-Sub-CA-Zertifikaten und der mit ihnen verbundenen Schlüssel wurde durch die Gesellschafterversammlung der gematik getroffen? (Hinweis: BMG-Stellungnahme ist hier schon eingeflossen.)

Betrifft:

Gültig ab	03.08.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	keine Zulassungsrelevanz		
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:

Im Anhang F des Sicherheitskonzepts wird ein Kapitel F3.5 „Weitere Festlegungen für kryptographische Schlüssel“ wie folgt hinzugefügt.

F3.5 Weitere Festlegungen für kryptographische Schlüssel

Es wird festgelegt, dass die maximale Gültigkeitsdauer des aktuell verwendeten Signatur-Schlüsselpaars der CVC-Root-CA mit der Bezeichnung „DEGZW/C.RSA.CS.R2048 S256“, welches am 23.07.2008 erzeugt wurde, einmalig bis zum 1.1.2018 ausgedehnt wird. Damit ist das Schlüsselpaar vom Zeitpunkt seiner Erzeugung bis maximal inkl. des 31.12.2017 gültig.

Dies soll analog auch für das mit diesem Schlüsselpaar verbundene aktuelle CVC-Root-CA-Zertifikat gelten.

Für die mit Hilfe dieses Signatur-Schlüsselpaars ausgestellten CVC-Sub-CA-Zertifikate und die mit ihnen verbundenen Schlüssel soll die maximale Gültigkeit ebenfalls analog erweitert werden. Nach dem Schalenmodell sind die CVC-Sub-CA-Zertifikate höchstens solange gültig, wie das aktuell verwendete CVC-Root-CA-Zertifikat.