SRQ - Specification Related Question

SRQ-ID: 1217

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	Gültigkeitsdauer X.509 Zertifikate
zu Dokument / Datei (evtl. ersetzt SRQ)	gemTSL_SP_CP
Version	1.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	8.3.2

Stichwort: Gültigkeitsdauer X.509 Zertifikate

Frage:

Das Dokument „Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUTH/OSIG-Zertifikaten“ sieht eine Zertifikatslaufzeit für X.509-Endnutzerzertifikate der eGK und SMC-B von max. 5 Jahren vor.

Um eine möglichst hohe Wirtschaftlichkeit der Gesundheitskarten im Feld zu erzielen, sollten diese möglichst lange im Feld verbleiben können, bevor sie ausgetauscht werden müssen.

Des Weiteren wird für die Produktion, Personalisierung und den Versand der Gesundheitskarten zusätzlich zur definierten Gültigkeit von 60 Monaten ein Puffer benötigt, um eine 5 Jahre gültige Karte ausgeben zu können. Dies gilt analog auch für die SMC-B.

Ist es daher zulässig, die Zertifikatslaufzeit dieser Karten in der Telematikinfrastruktur zu erhöhen?

Betrifft :

Gültig ab	01.01.2012	Verbindlichkeit	normativ
Zulassungsrelevanz	SRQ ist gültig für Zulassungsanträge ab dem 01.01.2012 sowie Zulassungsanträge, deren Testobjekte nach dem 01.01.2012 bei der gematik eingereicht werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:	Von dieser SRQ ist das Zulassungsverfahren Validierung der Personalisierungsdaten eGK betroffen.		
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Eine Anpassung der Gültigkeitsdauer der Zertifikate wird unter Berücksichtigung der Anforderungen an die Vorgaben zur Sicherheit der Telematikinfrastruktur ermöglicht, indem die Spezifikation (Kapitel 8.3.2) wie folgt ergänzt wird:

8.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Der TSP MUSS Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren definieren. Die Gültigkeitsperioden orientieren sich am aktuellen Stand der Technik und Kryptologie.

Die vom TSP und den TSP-Services ausgestellten Zertifikate haben folgende Gültigkeitszeiträume:

- Zertifikat für TSP mit Root-Funktion maximal zehn (10) Jahre,
- Zertifikate für TSPs maximal acht (8) Jahre,
- alle anderen Zertifikate maximal fünf (5) Jahre, wobei eine Erweiterung der Gültigkeitsdauer der End-Entity-Zertifikate bis zum Ende des Monats, in welchem die fünf Jahre enden, zulässig ist.

Die Nutzungsdauer von privaten Schlüsseln entspricht grundsätzlich der Gültigkeitsdauer der darauf basierenden Zertifikate. Eine Verwendung von vorhandenen Schlüsselpaaren im Rahmen einer Re-Zertifizierung ist zulässig, wenn die empfohlenen Algorithmen und Schlüssellängen dies erlauben (siehe Abschnitt 8.1.5).

Weitere Vorgaben gemäß [gemSiKo#F.3.1].