SRQ - Specification Related Question

SRQ-ID: 0869

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

Themenkreis	Dezentrale Komponenten
Schlagwort	Kartenterminalidentität SM-KT, Ausprägung OID Zertifikate
zu Dokument / Datei	gemSpec_KT
Version	2.6.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3.7.1

Stichwort: Kartenterminalidentität SM-KT, Ausprägung OID Zertifikate

Frage:

Welches Format haben die Zertifikate auf dem SM-KT und wo sind die zugehörigen OIDs definiert?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	2.6.2	voraussichtl. Zeitpunkt	19.09.08
Anmerkungen:			
Status	☒ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort: Die Zertifikate sind im DER Format auf dem SM-KT gespeichert. Die OIDs sind in einem eigenen Dokment der gematik festgelegt. Daraus ergeben sich folgende Änderungen an der Spezifikation:

3.7.1 Anforderungen an die Kartenterminalidentität

Aufgabe der gematik ist (u. a.) die Sicherstellung der Interoperabilität und Kompatibilität technischer Komponenten für die Nutzung der Telematikinfrastruktur. Darüber hinaus hat die gematik sicherzustellen, dass nur zugelassene Komponenten in der Telematikinfrastruktur eingesetzt werden. ~~Festlegungen zu den zu diesen Identitäten gehörenden Zertifikaten und der verwendeten PKI sind in [gemPKI_KT] beschrieben.~~

3.7.1.1 Ausführung

Die SMKT-Identitäten werden durch asymmetrische Schlüssel und X.509-Zertifikate umgesetzt. Genauere kryptographische Festlegungen werden in [gemSpec_Krypt] getroffen. Festlegungen zu den zu diesen Identitäten gehörenden Zertifikaten und der verwendeten PKI sind in [gemPKI_KT] beschrieben. Die zugehörigen Object Identifier (OID) sind im Dokument [gemSpec_OID] festgelegt. Das Zertifikat wir im DER Format auf der Karte gespeichert.

[…]

Es MUSS sichergestellt sein, dass das Shared Secret nicht im Klartext zur Anzeige gebracht wird.

[gemSpec_OID]	gematik: Einführung der Gesundheitskarte - Spezifikation: Festlegung von OIDs