SRQ - Specification Related Question

SRQ-ID: 0873

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

Themenkreis	Dezentrale Komponenten
Schlagwort	Sicherung SICCT TLS Verbindung
zu Dokument / Datei	gemSpec_KT
Version	2.6.0
Bezug (Kap., Abschnitt, Tab., Abb.)	4.11

Stichwort: Sicherung SICCT TLS Verbindung

Frage:

Wie sind die CA-Zertifikate zu handhaben und wie soll sich das Kartenterminal verhalten, wenn die Prüfung des Konnektorzertifikates fehl schlägt?

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 CA-Zertifikate müssen vertraulich gehandhabt (Einbringung, Speicherung) werden. Ein Filtern nach TSP-K Zertifikaten ist durch den Extension Eintrag möglich. Bei fehlgeschlagener Prüfung der Konnektorzertifikates, muss der Verbindungsaufbau abgebrochen werden. Die Änderungen sind in Kapitel 4.11 der Spezifikation festgeschrieben

Die Dienste bzw. CA-Zertifikate in der TCL sind über die TSL-Extension zuordenbar: Im Extension-Eintrag wird zu jedem CA-Zertifikat angegeben, welche Typen von Zertifikaten er ausstellen darf (siehe [gemVerw_Zert_TI#10.3]). Ein Filtern nach TSP-Ks ist damit einfach möglich. Beim Einbringen dieser CA-Zertifikate in das Kartenterminal und ihrer anschließenden Speicherung innerhalb des Kartenterminals MUSS deren Authentizität gewährleistet werden und sie MÜSSEN ausreichend gegen Veränderungen geschützt, gespeichert werden. Nehmen neue CAs ihren Betrieb für das Generieren von Komponentenzertifikaten für Konnektoren auf, MÜSSEN die zugehörigen CA-Zertifikate

auf vertrauenswürdige Weise in ein eHealth-Kartenterminal eingebracht werden können. Dies KANN zum Beispiel über einen Update der Firmware des Kartenterminals erfolgen (siehe auch [gemPKI_KT#7.1.1]).

Zur Feststellung, ob das ansteuernde System ein betriebszugelassener Konnektor[3] ist, MUSS das Kartenterminal im Zuge des TLS-Verbindungsaufbaus das vom Konnektor präsentierte Zertifikat gemäß [gemPKI_KT#7.1.2] prüfen. Die Prüfung erfolgt immer einstufig,
d. h. das präsentierte Zertifikat lässt sich direkt anhand eines am Kartenterminal hinterlegten CA-Zertifikates prüfen. Schlägt die Prüfung des Zertifikates fehl, MUSS das Kartenterminal den TLS-Verbindungsaufbau abbrechen.

[3] Für eine automatische Prüfung der Betriebszulassung eines Konnektors durch andere IT-Systeme steht ein X.509-Zertifikat zusammen mit den damit verbundenen geheimen und öffentlichen Schlüsseln im Rahmen der Identitäten des Konnektors zur Verfügung. Es ist dabei durch organisatorische Prozesse im Rahmen der Baureihenzulassung sichergestellt, dass nur betriebszugelassene Geräte mit solchen Zertifikaten ausgestattet werden.