SRQ - Specification Related Question

SRQ-ID:

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

Themenkreis	Dezentrale Komponenten
Schlagwort	
zu Dokument / Datei	
Version	
Bezug (Kap., Abschnitt, Tab., Abb.)	

Stichwort:

Frage:

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release		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: Die Anforderungen an die administrative LAN-Schnittstelle und deren Sicherung wurden überarbeitet, ein alternatives Sperren ist zulässig. Die Änderungen sind in der Spezifikation folgendermaßen festgeschrieben. Die Änderungen sind in der Spezifikation folgendermaßen festgeschrieben:

3.6.6.1 Sicherung der administrativen TLS-Verbindung

Das Kartenterminal MUSS für die administrative TLS-Verbindung die in [gemSpec_Krypt#6.4.4] angeführten (stärkeren) Algorithmen unterstützen. Sofern eine SM-KT vorhanden ist, MUSS für den TLS Aufbau das Schlüsselmaterial der SM-KT verwendet werden (ID.SMKT.AUT). Falls keine SM-KT vorhanden ist, KANN das Kartenterminal Schlüsselmaterial sowie ein zugehöriges Zertifikat zur Verfügung stellen (z. B. in der Firmware). Falls das Kartenterminal das für den TLS-Verbindungsaufbau

notwendige kryptographische Material nicht zur Verfügung stellt, MÜSSEN eventuell vorhandene Netzwerk-basierte Managementschnittstellen deaktiviert sein wenn keine SM-KT vorhanden ist. Die Netzwerk-basierte Managementschnittstelle MUSS ebenfalls deaktiviert sein, wenn das Kartenterminal über keinen für den Verbindungsaufbau notwendigen Zufallszahlengenerator verfügt (siehe Kapitel 3.6.9).

3.6.9 Zufallszahlen und Schlüssel

Zur Erzeugung von Zufallszahlen ohne vorhandenes SM-KT KANN das KT daher mindestens einen rein in Software umsetzbaren Zufallszahlengenerator zur Verfügung stellen.