SRQ - Specification Related Question

SRQ-ID: 0880

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

Themenkreis	Dezentrale Komponenten
Schlagwort	Zufallszahlengenerator
zu Dokument / Datei	gemSpec_KT
Version	2.6.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3.6.9

Stichwort: Zufallszahlengenerator

Frage:

Welche Anforderungen werden an die Qualität und Güte des Zufallszahlengenerators und der von ihm erzeugten Zufallszahlen gestellt?

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 Anforderung an Qualität und Güte sind in Kapitel 3.6.9 der Spezifikation aufgenommen worden.

3.6.9 Zufallszahlen und Schlüssel

Ein Zufallsgenerator erzeugt Zufallszahlen und Schlüssel im Rahmen bestimmter Kryptoverfahren wie z. B. TLS. Das Kartenterminal MUSS das Erstellen von Zufallszahlen und Einmalschlüsseln unterstützen. Die Länge der angeforderten Zufallszahlen bzw. Einmalschlüssel und die Qualität des Generators ist vom jeweiligen Einsatzzweck abhängig. Die Güte und der ordnungsgemäße Betrieb des Zufallsgenerators sind geeignet sicherzustellen. Genaueres regelt das Kryptographiekonzept [gemSpec_Krypt#5.2]. Das Kartenterminal kann einen Hardware- oder Softwaregenerator verwenden. Als Quelle für Zufallszahlen KANN der Zufallszahlengenerator des SM-KT

(siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**) verwendet werden, welcher die oben genannten Anforderungen an Qualität und die Güte der Zufallszahlen erfüllt.

Da das SM-KT erst in das Kartenterminal eingebracht werden muss, steht der Zufallszahlengenerator des SM-KT nicht immer zur Verfügung. Zur Erzeugung von Zufallszahlen ohne vorhandenes SM-KT MUSS das KT daher mindestens einen rein in Software umsetzbaren Zufallszahlengenerator zur Verfügung stellen. Abweichend von den Festlegungen in [gemSpec_Krypt#5.2] KANN dieser Zufallszahlengenerator eine geringere Qualität, und die von ihm erzeugten Zufallszahlen eine geringere Güte aufweisen.

Ist kein SM-KT im Kartenterminal vorhanden KANN der Zufallszahlengenerator des Kartenterminals zum Aufbau von nicht SICCT-spezifischen TLS-Verbindungen verwendet werden, selbst wenn er die Anforderungen an Qualität und Güte aus [gemSpec_Krypt#5.2] nicht erfüllt. Es MUSS jedoch sichergestellt sein, dass ein Zufallszahlengenerator geringerer Güte ausschließlich zum Aufbau von nicht SICCT-spezifischen TLS Verbindungen und nur unter der Bedingung, dass keine SM-KT im Kartenterminal gesteckt ist, eingesetzt wird.

Es liegt in der Verantwortung der Hersteller im Rahmen der Sicherheitsevaluierung nachzuweisen, dass durch den Einsatz des Zufallszahlengenerators des Kartenterminals kein Schaden entstehen kann.