SRQ - Specification Related Question

SRQ-ID: 0870

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

Themenkreis	Dezentrale Komponenten
Schlagwort	EHEALTH TERMINAL AUTHENTICATE Funktionsweise
zu Dokument / Datei	gemSpec_KT
Version	2.6.0
Bezug (Kap., Abschnitt, Tab., Abb.)	4.7.2

Stichwort: EHEALTH TERMINAL AUTHENTICATE Funktionsweise

Frage:

Welche Korrekturen gibt es an der Funktionsweise des Kommandos EHEALTH TERMINAL AUTHENTICATE?

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		

Es ergeben sich die folgenden Korrekturen an den EHEALTH Kommandos:

4.7.2.1 Funktion

Das Kommando hat drei Ausprägungen wobei für alle Ausprägungen gilt, dass das Kartenterminal sicherstellen MUSS, dass die gespeicherten Shared Secrets und die gespeicherten öffentlichen Schlüssel für Konnektoren eindeutig sind.

[…]

Wird das Kommando mit P2=’01’ (CREATE) ausgeführt, läuft die Verarbeitung des Kommandos im Kartenterminal in 8 Schritten ab.

(1) Das Kartenterminal prüft, ob noch ein freier Pairingblock vorhanden ist. Ist dies nicht der Fall so bricht das Kartenterminal den Befehl mit einer entsprechenden Fehlermeldung ab (SW1SW2=6900).

(2) Das Kartenterminal prüft, ob ein Displaytext enthalten ist. Fehlt der Displaytext so bricht das Kommando mit Fehler ab (SW1SW2=6A80).

(3) Das Kartenterminal prüft, ob der im Shared Secret DO übergebene Byte String genau 16 Byte lang ist. (Shared Secret). Ist dies nicht der Fall bricht das Kartenterminal mit Fehler ab (SW1SW2=6A80). Das Shared Secret ist eine vom Konnektor generierte Zufallszahl.

(4) Hat es bereits ein identisches Shared Secret gespeichert, bricht das Kartenterminal mit Fehler ab (SW1SW2=6900).

(5) Das Terminal zeigt den Displaytext an und wartet darauf, dass auf dem PIN Pad die Bestätigungs-Taste gedrückt wird. Durch Druck der Abbrechen-Taste wird der Befehl abgebrochen. Wird nicht binnen einer herstellerspezifischen Zeitspanne die maximal 10 Minuten betragen darf, die Bestätigungs-Taste gedrückt, MUSS der Befehl abgebrochen werden. Bei Abbruch löscht das Kartenterminal das Shared Secret wieder aus seinem Speicher und schickt eine Fehlermeldung zurück. Bei Abbruch durch Tastendruck MUSS mit Fehlercode SW1SW2=6401 geantwortet werden. Bei Abbruch durch Timeout MUSS mit Fehlercode SW1SW2=6400 geantwortet werden.

(6) Hat das Kartenterminal den öffentlichen Schlüssel des beim Verbindungsaufbau präsentierten Konnektorzertifikats bereits gespeichert, MUSS es diesen aus dem korrespondierenden Pairingblock löschen. Der Pairingblock bleibt jedenfalls erhalten, selbst wenn keine öffentlichen Schlüssel in ihm gespeichert sind. Das Kartenterminal speichert den im Shared Secret DO übergebenen Byte-String zusammen mit dem während des TLS-Aufbaus erhaltenen öffentlichen Schlüssel des Konnektorzertifikats in einem unbenutzten Pairingblock ab.

(7) Für das erhaltene Shared Secret wird mittels der SM-KT unter Verwendung des Zertifikats für die SMKT-Identität eine Signatur erstellt. Hierfür generiert das Kartenterminal den SHA-256-Hashwert des Shared Secrets. Dieser Hashwert wird durch die SM-KT mittels EMSA-PKCS1-v1_5 gemäß [PKCS#1] Kapitel 9.2 mit einer Moduluslänge von 2048 Bit signiert. Diese Verfahren stehen auf der SM-KT zur Verfügung.

(8) Die in Schritt (6) berechnete Signatur wird in der Response APDU zurückgeschickt.

[…]

Für P2=’04’ (ADD Phase 2) ist der Ablauf wie folgt:

(1) Das Kartenterminal prüft ob es sich im Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“ befindet. Ist dies nicht der Fall bricht das Kartenterminal mit einem Fehler ab (SW1SW2=6900).

(2) Das Kartenterminal verlässt den Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“

(3) Das Kartenterminal prüft, ob der im Shared Secret Response DO übergebene Byte-String genau 32 Byte lang ist. Ist dies nicht der Fall bricht das Kartenterminal mit Fehler ab (SW1SW2=6A80)

(4) Für jeden genutzten Pairingblock berechnet das Kartenterminal aus der in Phase 1 generierten Zufallszahl und dem Shared Secret des jeweiligen Pairingblocks die SHA-256 Hashwerte (vgl. Ablauf bei P2='02') und löscht anschließend die generierte Zufallszahl.

(5) Das Kartenterminal vergleicht alle generieren Hashwerte mit der im Shared Secret Response DO enthaltenen Antwort des Konnektors.

(6) Stimmt genau einer der Hashwerte überein, selektiert das Kartenterminal den Pairingblock, der das erfolgreich geprüfte Shared Secret enthält, um dort den öffentlichen Schlüssel des beim TLS-Verbindungsaufbaus erhaltenen Konnektorzertifikats einzutragen. Sonst bricht das Kartenterminal mit Fehler ab (SW1SW2=6400). Ist der neue öffentliche Schlüssel bereits in einem anderen Pairingblock als dem selektierten enthalten, MUSS das Kartenterminal diesen, vor dem Eintragen des neuen Schlüssels, aus dem entsprechenden Pairingblock löschen. Die Regeln für das Eintragen des neuen öffentlichen Schlüssels sind dabei wie folgt:

(7) Ist der neue öffentliche Schlüssel bereits im selektierten Pairingblock enthalten, trägt das Kartenterminal den Schlüssel nicht ein und antwortet mit einem Command successful (SW1SW2=9000).

(8) Ist der neue öffentliche Schlüssel noch nicht im selektierten Pairingblock enthalten und ist noch mindestens ein Speicherslot für öffentliche Schlüssel im Pairingblock frei, wird der neue öffentliche Schlüssel hinzugefügt und das Kartenterminal antwortet mit einem Command successful (SW1SW2=9000).

(9) Ist der neue öffentliche Schlüssel noch nicht im selektierten Pairingblock enthalten und ist kein Speicherslot für öffentliche Schlüssel im Pairingblock mehr frei, wird der älteste öffentliche Schlüssel, jener dessen Pairingvorgang am längsten zurück liegt, mit dem neuen öffentlichen Schlüssel überschrieben und das Kartenterminal antwortet mit einem Command successful (SW1SW2=9000).