SRQ - Specification Related Question

SRQ-ID: 0874

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

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

Stichwort: EHEALTH TERMINAL AUTHENTICATE - STRUCTURES

Frage:

Welche Korrekturen gibt es an den Strukturen die im Rahmen des Kommandos EHEALTH TERMINAL AUTHENTICATE verwendet bzw. spezifiziert werden?

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: Es ergeben sich die folgenden Korrekturen an den Strukturen die im Rahmen des Kommandos EHEALTH TERMINAL AUTHENTICATE:

4.7.2.5.1 Response Structure

EHEALTH TERMINAL AUTHENTICATE	Kodierung R-APDU		
	[Body:]	Trailer	
	[Requested Data / Information]	Status Byte 1	Status Byte 2

	Requested data	in case of success and P2=01 : Signature of Shared Secret created with Certificate of SM-KT	SW1	SW2
	Requested data	in case of success and P2=02: SHA-256 hash value		
	Requested data	in case of success and P2=03: Challenge		
	Empty	in case of error		

4.7.2.6 Status-Codes SW1-SW2

SW1SW2	P2	Specification	Meaning
6400	'01' CREATE	Execution Error	Nor or incomplete input in time
	'04' ADD	Execution Error	Hashvalue not found
6401	'01' CREATE	Execution Error	Process aborted by pressing of CANCEL key
~~6402~~	~~'04' ADD~~	~~Execution Error~~	~~Presented Public key already known~~
6900	'01' CREATE	Command not allowed	No unused pairing block available or shared secret already stored
	'02' VALIDATE	Command not allowed	Presented Public Key unknown
	'04' ADD	Command not allowed	CT is not in the state "EHEALTH EXPECT CHALLENGE RESPONSE"
6A80	'01' CREATE	Incorrect Parameters	Length of SS DO is not 16 bytes or No Displaymessage given.
	'02' VALIDATE	Incorrect Parameters	Length of SSC DO is smaller than 16 bytes
	'04' ADD	Incorrect Parameters	Length of SSR DO is unequal 32 bytes

Shared Secret Response Data Object (SSR DO)			
TAG	'D6'	One byte tag according ISO 7816-6: Application Label	
		Tag coding according ASN.1 BER see SICCT 5.5.10.3	
		BER-Coding : private, primitive, Tag-Number = 22 ('16')	
LEN	LEN coding see SICCT 5.5.10.3		
	'20'	one byte coding LEN=32	

	all other values	reject with error
VALUE	Shared Secret Response	
	SHA-256 Hashvalue	