SRQ - Specification Related Question

SRQ-ID: 0815

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

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Signaturinput
zu Dokument / Datei	eGK-Spezifikation Teil 1
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Diverse Kapitel (s.u.)

Stichwort: Längenbegrenzung Signaturinput

Frage:

Gemäß [gemSpec_eGK_P1] ist es heute zulässig, dass dieses Kommando den kompletten APDU Buffer belegt.

Wäre es aus Performancegründen nicht sinnvoll, die Länge der Kommandodaten auf einen Wert <= 255 zu begrenzen?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	2.2.1	voraussichtl. Zeitpunkt	19.09.08
Anmerkungen:			
Status	☐ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☒ eingearbeitet in Folgeversion		

(wird von der bearbeitenden AG ausgefüllt):

Antwort:

Mangels Use Case, der die Verarbeitung längerer Inputs fordert und zur Performancesteigerung wird der Input für Signaturoperationen in der Länge auf 64 Oktette begrenzt.

Dies wird in der eGK-Spezifikation Teil 1 an folgenden Stellen festgelegt:

IntAuth, rsaClientAuthentication: (N862)d, (N1193)

PSO CompDigSig, rsaClientAuthentication: (N873)a

PSO CompDigSig, signPSS: (N873)c, (N1225)

PSO CompDigSig, sign9796_2_DS2: Kapitel 15.8.1.2