SRQ - Specification Related Question

SRQ-ID: 1065

Betrifft:

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	SM Padding Case 1 APDU
zu Dokument / Datei	gemSpec_eGK_P1
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	(N328)

Stichwort: SM Padding Case 1 APDU

Frage:

Im Falle einer Case 1 APDU wird gemäß (N328) vor der eigentlichen MAC Berechnung zweimal gepadded. Ist das gewollt?

Betrifft:

Gültig ab Release	0.5.2	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:

Nein, das doppelte Padden im Falle einer Case 1 APDU ist nicht konform zu ISO/IEC 7816-4 und nicht gewollt. Der komplette Text von (N328) ist zu ersetzen durch:

(N328) K_externeWelt {K_eGK}
Es gilt: tmpData = ProtectedData || LeDO
Falls Kmac ein

a. 3TDES Schlüssel ist, gilt:

1. MACin = I2OS(SSCmac, 8)

2. Falls OctetLength(tmpData)

i. gleich null ist, dann gilt:
MACin = MACin || head

ii. ungleich null ist, dann gilt:
MACin = MACin || PaddingIso(head, 8) || tmpData

3. MAC = CALCULATE_Retail_MAC(Kmac, MACin)

b. AES Schlüssel ist, gilt:

1. MACin = I2OS(SSCmac, 16)

2. Falls OctetLength(tmpData)

i. gleich null ist, dann gilt:
MACin = MACin || head

ii. ungleich null ist, dann gilt:
MACin = MACin || PaddingIso(head, 16) || tmpData

3. MAC = CALCULATE_CMAC(Kmac, MACin)