SRQ - Specification Related Question

SRQ-ID: 1067

Betrifft:

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Initialisierung CBC Entschlüsselung
zu Dokument / Datei	gemSpec_eGK_P1
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	(N41)b

Stichwort: Initialisierung Entschlüsselung

Frage:

Bei der Entschlüsselung im CBC Mode wird als Initialisierung P_0 verwendet, korrekt wäre aber C_0, oder?

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:

Die Beobachtung ist korrekt. In (N41)b ist die Bezeichnung P_0 zu ersetzen durch die Bezeichnung C_0. Damit lautet der komplette Text von (N41)b wie folgt:

b. Schritt 2: C_0 = I2OS(T_1, 8)