

SRQ-ID: 0841

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

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Verschlüsselung von Antwortdaten
zu Dokument / Datei	eGK-Spezifikation Teil 1
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	(N226) (N337) (N338)

Stichwort: Verschlüsselung von Antwortdaten

Frage:

Es ist in N226, N337 und N338 nicht genau formuliert, wann Antwortdaten zu verschlüsseln sind und wie dies vom COS zu ermitteln ist. Wie lautet die präzise Anforderung?

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	<input type="checkbox"/> erfasst <input type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input type="checkbox"/> freigegeben <input checked="" type="checkbox"/> eingearbeitet in Folgeversion		

(wird von der bearbeitenden AG ausgefüllt):

Antwort:

Dies ist bereits implizit an anderen Stellen festgelegt. Mit den folgenden Ergänzungen findet sich dies nun auch explizit im Dokument (Nummerierung nach neuer Noatation):

N022600

d. *SessionkeyContext.flagRspEnc* MUSS genau dann auf True gesetzt werden, wenn die Zugriffsbedingung das Element *SmRspEnc* enthält.

N033700

Falls das optionale Datenfeld Data vorhanden ist und verschlüsselt übertragen wird
(*flagRspEnc* ist True, siehe (N029900)d.7 und (N022600)d) und Kenc ein 3DES

Schlüssel ist, gilt:

N033800

Falls das optionale Datenfeld Data vorhanden ist und verschlüsselt übertragen wird
(*flagRspEnc* ist True, siehe (N029900)d.7 und (N022600)d) und Kenc ein AES

Schlüssel ist, gilt:

.