SRQ - Specification Related Question

SRQ-ID: 1109

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	3TDES statt 3DES
zu Dokument / Datei (evtl. ersetzt SRQ)	gemSpec_Krypt
Version	1.3.0
Bezug (Kap., Abschnitt, Tab., Abb.)	6.3.2

Stichwort: 3TDES statt 3DES

Frage:

In gemSpec_Krypt wird im Kapitel 6.3.2 im Zusammenhang mit der Card-to-Server Authentisierung der Algorithmus 3DES im CBC Mode referenziert. Der Bezeichner 3DES wird weder in der Technischen Richtlinie 03116 noch in anderen Standards verwendet. Welcher Algorithmus ist hier gemeint?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz			
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	1.4.0	voraussichtl. Zeitpunkt	10.07.2008
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Die korrekte Bezeichnung für den zu verwendenden Algorithmus ist 3TDES im CBC Mode. Dies bedeutet Triple-DES mit drei 56-Bit-Schlüsseln im CBC Mode.