SRQ - Specification Related Question

SRQ-ID: 1218

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

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	CMAC bei Personalisierung der eGK
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSpec_Krypt]
Version	1.3.0
Bezug (Kap., Abschnitt, Tab., Abb.)	6.9

Stichwort: CMAC bei Personalisierung der eGK

Frage:

In SRQ 0906 zum Dokument [gemPersKrypt] existiert ein Verweis auf [gemSpec_Krypt#6.9]. In der im Basis-Rollout gültigen Dokumentenversion 1.3.0 von [gemSpec_Krypt] existiert dieses Kapitel nicht. Wie soll das betroffene Kapitel aussehen?

Betrifft (wird von PQA ausgefüllt):

Gültig ab	09.07.2012	Verbindlichkeit	normativ
Zulassungsrelevanz	Der SRQ hat keine Auswirkungen auf die Zulassungen.		
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:

Es werden folgende Ergänzungen in [gemSpec_Krypt] aufgenommen.

6.9 Message Authentication Code (MAC) im Rahmen der Personalisierung der eGK

Für die Personalisierung der eGK müssen Daten übermittelt und integritätsgeschützt werden. Für die Absicherung der Integrität ist in diesem Kontext der AES-256 CMAC nach [SP800-38B] (vgl. [BSI-TR-03116#3.2.2, 4.4.2]) zu verwenden.

Die Länge des CMAC muss 128 Bit betragen.

Nach [SP800-38B,S.13] sollen nicht mehr als 2^{48} Nachrichtenblöcke (2^{22} GByte) mit demselben Schlüssel verarbeitet werden. Nach [SP800-38B, S. 14] ist ein CMAC anfällig für Replay-Attacken, was bei der Anwendung des CMACs zu berücksichtigen ist.

Tabelle : Algorithmen für die Berechnung eines MACs

Algorithmen Typ	Algorithmus	Schlüssellänge	2008	2009	2010	2011	2012	2013
Berechnung eines MAC für die Absicherung der Datenintegrität	CMAC basierend auf AES	AES 256	M	M	M	M	M	M

Tabelle : Betroffene Systeme – Message Authentication Code (MAC) im Rahmen der Personalisierung der eGK

System	Einsatz
Systeme zur Personalisierung der eGK	Systeme, zwischen denen Daten zur Personalisierung der eGK Übermittelt werden, müssen für den Integritätsschutz den zuvor angegebenen Algorithmus verwenden

A4 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[SP800-38B]	NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition