

SRQ-ID: 1009

Betrifft:

Themenkreis	Dezentrale Komponenten
Schlagwort	Verschlüsselung
zu Dokument / Datei	gemLast_MobKT
Version	1.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	4.3.2.2, 6.3.2.11

Stichwort: Verschlüsselung

Frage:

Welche Karte soll zur Verschlüsselung von zwischengespeicherten Daten verwendet werden?

Betrifft:

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
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 type="checkbox"/> eingearbeitet in Folgeversion		

Antwort:

Die Wahl der Karte mit der die Daten verschlüsselt werden bleibt dem Hersteller überlassen. Es ergeben sich die folgenden Änderungen:

4.3.2.2 Ausbaustufe 2

Die Verschlüsselung MUSS mittels einer berechtigten Karte, ~~welche auch zum Freischalten der eGK verwendet wurde~~, erfolgen

6.3.2.11 Kryptodienst

Der Mini-AK MUSS dem mobilen Kartenterminal einen Ver- und Entschlüsselungsdienst bereitstellen. Hierbei MUSS der Mini-AK die Daten mit der berechtigten Karte

verschlüsseln, ~~die zur Freischaltung der eGK verwendet wurde~~ und es MUSS der öffentliche ENC-Key verwendet werden [A_02048].

A1 – Ausgangsanforderungen

Afo-ID	Klasse	Beschreibung	Kapitel
A_02048	F	Der Mini-AK MUSS die Daten mit der berechtigten Karte verschlüsseln und es MUSS der öffentliche ENC-Key zur Verschlüsselung verwendet werden	6.3.2.11