SRQ - Specification Related Question

SRQ-ID: 1123

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	Level (Prüftiefe) für Zertifizierung nach FIPS 140-2
zu Dokument / Datei (evtl. ersetzt SRQ)	gemTSL_SP_CP, SRQ_0913
Version	1.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Kapitel 7, 8.2.1

Stichwort: Level (Prüftiefe) für Zertifizierung nach FIPS 140-2

Frage:

Wird der Level (Prüftiefe) der Zertifizierung nach FIPS 140-2 im vorliegenden Dokument gefordert?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	Die SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:	Dieser SRQ enthält Maßnahmen, die sich aus dem Sicherheitsgutachten ergeben haben.		
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Bisher nicht. Die Formulierungen im Kapitel 7 und 8.2.1, Absatz 3 werden deshalb wie folgt angepasst.

Kapitel 7, Absatz 3:

Folgende zusätzliche Anforderungen bzw. Konkretisierungen MÜSSEN für die Sicherheit des gematik-TSL-Service Provider und allen beteiligten TSPs umgesetzt werden:

- Als HSM MUSS ein Modul eingesetzt werden, das erfolgreich evaluiert wurde. Als Evaluierungsschemata kommen Common Criteria, ITSEC oder FIPS 140-2 in Frage. Die

entsprechende Prüftiefe der Zertifizierung eines HSM wird im Kapitel 8.2.1 festgelegt. ~~MUSS dabei mindestens Common Criteria EAL 4 entsprechen.~~

Kapitel 8.2.1:

Die verwendeten kryptographischen Module SOLLEN anerkannte Standards verwenden.

~~Werden HSM-Module im Rahmen der Zertifizierung eingesetzt, MUSS das Modul einem der folgend genannten oder einem äquivalenten Standard genügen:~~

- ~~FIPS 140-2 Level 3~~
- ~~CC EAL4 oder ITSEC E3 der Stärke „hoch“~~

Werden HSMs im Rahmen der Zertifizierung eingesetzt, MUSS das Modul dem Evaluierungsschema Common Criteria, ITSEC, FIPS 140-2 oder einem äquivalenten Standard genügen. Die Prüftiefe MUSS mindestens

- FIPS 140-2 Level 3,
- Common Criteria EAL 4 oder
- ITSEC E3 der Stärke „hoch“

entsprechen.