Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Änderungsbedarf in gemSpec_Kon

Bei der Schlüsselerzeugung für die gSMC-K soll u. a. mit technischen Maßnahmen die Vertraulichkeit der relevanten Schlüssel sichergestellt werden:

⌦ **TIP1-A_7225 Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung**

Der Hersteller des Konnektors, der Schlüssel für die gSMC-K erzeugt, MUSS diese Schlüssel ~~in einem HSM~~ mittels eines Hardwaresicherheitsmoduls erzeugen, welches

a) über einen Zugriffsschutz verfügt, sodass nur Berechtigte ~~den~~ Schlüssel darauf nutzen können,

b) in einem zutrittsgeschützten Bereich aufbewahrt wird und

c) mindestens nach FIPS 140-2 Level 3 oder [COS-G2] (CC-zertifizierte Chipkarte der TI) zertifiziert ist.

Wird für die Schlüsselerzeugung eine Schlüsselableitung verwendet, so MUSS die Schlüsselableitung die fachlichen Anforderungen aus GS-A_5386 erfüllen.

Es ist zulässig, dass asymmetrische Schlüssel bei der Personalisierung auf der gSMC-K selbst erzeugt werden und symmetrische Schlüssel mittels einer Schlüsselableitung erzeugt werden, bei dem sich der Ableitungsschlüssel (Masterkey) innerhalb eines nach (c) zulässigen Hardwaresicherheitsmoduls befindet.

Der Hersteller des Konnektors MUSS die Schlüsselerzeugung und die Schlüsselverwaltung in einem Konzept darstellen, das die technischen und organisatorischen Maßnahmen beschreibt, die den Schutzbedarf der verarbeiteten Informationsobjekte befriedigen. Der Hersteller des Konnektors MUSS dieses Konzept der gematik zur Verfügung stellen. ⌫

… [Literaturverzeichnis] …

[COS-G2]	Common Criteria Protection Profile, Card Operating System Generation 2, (PP COS G2), BSI-CC-PP-0082-V2

© gematik – öffentlich_Entwurf