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_Krypt

⌦ **GS-A_4383 IPsec-Kontext – Verschlüsselte Kommunikation**

Alle Produkttypen, die mittels IPsec-Daten schützen, MÜSSEN dies ausschließlich auf Grundlage der in GS-A_4382 als zulässig aufgeführten Verfahren und Vorgaben tun. ~~Weiter gilt:~~

- ~~Bei den symmetrische Verschlüsselungsalgorithmen MÜSSEN die in Tabelle Tab_KRYPT_013 aufgeführten Verfahren unterstützt werden. Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.3.1, Tabelle 7] verwendet werden.~~
- ~~Für den Integritätsschutz MUSS HMAC mittels SHA-1 unterstützt werden. Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.3.1, Tabelle 8] verwendet werden.~~
- ~~Rekeying: Die IPsec-SA-Lifetime darf maximal 3600 Sekunden betragen. Der Initiator soll nach Möglichkeit vor Ablauf der Lifetime das Rekeying anstoßen. Ansonsten muss der Responder bei Ablauf der Lifetime das Rekeying von sich aus sicherstellen.~~ ⌫

© gematik – öffentlich_Entwurf