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

1. Änderung in [gemSpec_Krypt]

2.4 Schlüsselerzeugung und Schlüsselbestätigung

… am Ende des Abschnitts wird hinzugefügt: …

A_14653 - TSP.X509: Prüfung auf angreifbare (schwache) Schlüssel

Alle TSPs, die X.509-Zertifikate erzeugen, MÜSSEN vor der Zertifikatserzeugung den durch das Zertifikat zu bestätigenden öffentlichen Schlüssel auf dessen kryptographische Angreifbarkeit hin prüfen. Falls die Prüfung des öffentlichen Schlüssels das Ergebnis „angreifbar“ liefert, so MUSS der TSP die Zertifikatserstellung für diesen Schlüssel ablehnen. Mindestumfang der Prüfung MÜSSEN der Test (1) auf den Debian PRNG-Bug und (2) den ROCA-Angriff sein. Der TSP MUSS den Mindestumfang der Prüfung auf Anweisung der gematik (bspw. bei Bekanntwerden neuer Angriffsmöglichkeiten) erweitern. Die gematik informiert alle zugelassenen TSPs schriftlich über eine notwendige Anpassung. <=

TSPs, die im Internet TLS-Zertifikate ausgeben – bspw. für die Verwendung von HTTPS, müssen aufgrund der Baseline Requirement des CA/Browser Forums (https://cabforum.org/baseline-requirements-documents/) vor der Zertifikatserzeugung kryptographische Prüfungen des zu bestätigenden öffentlichen Schlüssels durchführen. Analog gilt dies mit A_14653 auch für TI-TSPs. Die gematik stellt auf Anfrage eine Referenzimplementierung für die Tests des Mindestumfangs bereit.

2. Auswirkung auf Produkttypsteckbriefe

In folgenden Produkttypsteckbriefen

- gemProdT_X509_TSP_nonQES_eGK
- gemProdT_X509_TSP_nonQES_HBA
- gemProdT_X509_TSP_nonQES_Komp
- gemProdT_X509_TSP_nonQES_SMC-B

wird die Anforderung A_14653 im Kapitel 3.1.2, 3.2.2 und 3.2.3 als *neu* markiert.