

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 Telematikinfrastuktur 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]

2.4.1 Prüfung auf angreifbare (schwache) Schlüssel

Im Folgerelease wird es hier Anforderungen für die verpflichtenden Schlüsseltests auf angreifbare (schwache) Schlüssel im Kontext der EE-Zertifikatserstellung geben.

A_17294 - TSP-X.509: Prüfung auf angreifbare (schwache) Schlüssel

Ein TSP-X.509 nonQES MUSS vor einer 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

- (1) der Test auf die "Debian-OpenSSL-PRNG-Schwachstelle", und
- (2) der Test auf die Anfälligkeit gegen den ROCA-Angriff sein.

Der TSP MUSS den Mindestumfang der Prüfung bei Bekanntwerden neuer Angriffsmöglichkeiten gemäß [gemSpec_DS_Anbieter#GS-A_5560] erweitern. <=

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_17294 auch für TI-TSPs. Die gematik stellt auf Anfrage eine Beispielimplementierung für die Tests des Mindestumfangs bereit.

2. Auswirkung auf Produkttypsteckbriefe

In folgenden Produkttypsteckbriefen

- gemProdT_gematik-Root-CA
- 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_17294 im Kapitel 3.1.2, 3.2.2 und 3.2.3 als *neu* markiert.

Weiterhin wird in den o. g. Steckbriefen die Zuweisung von GS-A_5518 analog zu A_17294 angepasst.