

Änderung in gemSpec_Krypt

Folgender Abschnitt wird neu aufgenommen:

2.5 Einmalpasswörter

Bei verschiedenen Registrierungs- oder Anmeldeprozessen werden Einmalpasswörter (insbesondere bei KIM) verwendet. Für diese Einmalpasswörter gilt folgende Vorgabe:

A_22686 - Einmalpasswörter (One-Time-Passwords, OTP), Mindestentropie

Alle Produkttypen, die Einmalpasswörter (One-Time-Passwords, OTP) erzeugen, MÜSSEN sicherstellen, dass diese Einmalpasswörter eine Mindestentropie von 120 Bit besitzen. D. h. sie werden zufällig erzeugt und sind mit praktischer Sicherheit - Wahrscheinlichkeit gleich $1 - 2^{(-120)}$ - nicht erratbar. [\leq]