1 Änderung in gemSpec_CM_KOMLE

KOM-LE-A_2010 wird durch KOM-LE-A_2010-01 ersetzt:

KOM-LE-A_2010-01 - Extrahieren von MTA-Adresse, Portnummer und Kartenaufrufkontext
Das Clientmodul MUSS den Benutzernamen, ~~die MTA-Adresse, die zugehörige Portnummer und~~ den Kartenaufrufkontext und, wenn vorhanden, die MTA-Adresse und die zugehörige Portnummer aus dem vom Clientsystem erhaltenen SMTP-Benutzernamen entsprechend Abbildung Abb_MTA_Nutzer_Name extrahieren.**[**<=, Basis-Consumer, KOM-LE CM, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA**]**

In Kapitel 3.3.4.1.1 Wird in der Beschreibung unter KOM-LE-A_2190 der folgende Freitext entfernt:

~~Da der Versand einer Nachricht an mehrere Empfänger erfolgen kann und das Clientmodul nicht erkennt, ob alle Empfänger ECC beherrschen, muss das Signieren einer Nachricht immer mit dem RSA-Schlüssel der SM-B erfolgen.~~

In Kapitel 3.3.4.1.1 Wird in der Beschreibung unter KOM-LE-A_2191 der folgende Freitext entfernt:

Zum Verschlüsseln der Nachricht bezieht das Clientmodul die erforderlichen Zertifikate aus dem Verzeichnisdienst der TI. ~~Vor der Verwendung der Zertifikate für die Verschlüsselung muss das Clientmodul prüfen, ob der verwendete Konnektor die ECC-Kryptographie unterstützt. Ist dies nicht der Fall, dürfen im Verzeichnisdienst gefundene ECC-Zertifikate nicht für die Verschlüsselung benutzt werden. Unterstützt der Konnektor ECC, sind sowohl die RSA- als auch die ECC-Zertifikate für die Verschlüsselung zu verwenden. Durch diese Herangehensweise wird sichergestellt, dass auch Empfänger, die noch kein ECC beherrschen, die Nachricht entschlüsseln können. Dieses Prinzip gilt solange, bis alle TI-Beteiligten ECC beherrschen und somit die RSA-Zertifikate gesperrt sind.~~ Wenn im Verzeichnisdienst der TI für den Empfänger nur ein RSA-Zertifikat gefunden wird, dann wird mit RSA verschlüsselt. Wenn ein ECC- bzw. RSA- und ECC-Zertifikat gefunden wird, dann wird nur mit dem ECC-Zertifikat verschlüsselt.

KOM-LE-A_2022 wird durch KOM-LE-A_2022-01 ersetzt:

- Bezüglich der Herausnahme der RSA-2048 Zertifikate aus der TI-TSL verlässt sich das KOMLE-Clientmodul auf den Verzeichnisdienst, dass dort auch für jeden KIM-Teilnehmer die RSA-Zertifikate entsprechend entfernt werden. Für zusätzliche Robustheit wird hier auch das Verhalten des KOMLE-Clientmodul angepasst, sodass präferiert und falls beim Sender/Empfänger vorhanden nur noch mit ECC verschlüsselt wird. Nur für den Fall, dass bei einem Teilnehmer laut VZD kein ECC Material verfügbar sein sollte, wird mit RSA Verschlüsselt. Weiterhin wird durch diese Änderung auch die Performance bei der Ver- bzw. Entschlüsselung verbessert, da bis zu 50% weniger zu verschlüsselndes Material anfällt.
- Hinweis: Der Fall dass Konnektoren bei Sendern/Empfängern nicht ECC-fähig sein könnten muss nicht mehr betrachtet werden, da ab Mitte 2024 alle Konnektorhersteller ECC-fähige Versionen zugelassen und im Feld verfügbar haben werden.

KOM-LE-A_2022-01 - Verschlüsseln der Nachricht mit den Verschlüsselungszertifikaten C.HCI.ENC bzw. C.HP.ENC
Das Clientmodul MUSS vom Clientsystem erhaltene E-Mail-Nachrichten sowohl für jeden in den RCPT-Kommandos angegebenen Empfänger als auch für den Sender aus dem `from` bzw. `sender` Header-Element der Nachricht mit ~~allen dem Sender bzw. Empfängern zugeordneten~~ Verschlüsselungszertifikaten (C.HCI.ENC für eine Institution oder C.HP.ENC für einen Leistungserbringer) verschlüsseln. Falls dem Sender bzw. Empfänger sowohl ein ECC- als auch RSA-Zertifikat zugeordnet ist, MUSS für die Verschlüsselung ausschließlich das ECC-Zertifikat verwendet werden.
[<=, Basis-Consumer, KIM-iCM, KOM-LE CM, funkt. Eignung: Test Produkt/FA**]**

3.8.1. Erstellung der digitalen Signatur einer Nachricht mit einer SM-B

…

5. Die Signatur der KOM-LE-Nachricht erfolgt unter Verwendung der `SignDocument` Operation des Konnektors~~. Dabei werden die~~ mit den Parametern `Context` (dem Sender entsprechender Aufrufkontext), und `CardHandle` (Handle der ausgewählten SM-B)~~,~~ ~~`KeyReference` (C.OSIG_RSA) verwendet~~. Die Verwendung weiterer Parameter muss unter Berücksichtigung der Anforderungen aus [gemSMIME_KOMLE] erfolgen.

3.8.4 Entschlüsselung einer Nachricht mit einer SM-B bzw. einem HBA

…

3. Die IDs der Verschlüsselungszertifikate (Ermittlung über die Operation `ReadCardCertificate` des Konnektors) der über `GetCards` ermittelten HBAs und SM-Bs werden mit den Zertifikats-IDs aus dem `recipient-emails` Attribut des CMS-Objektes, die zur E-Mail-Adresse des Empfängers gehören, verglichen. Bei der Ermittlung der Zertifikate über die Operation ReadCardCertificate ist ggf. sowohl das RSA-ENC-Zertifikat als auch ECC-ENC-Zertifikat der Karten zu berücksichtigen.