
C_12223_Anlage

ECC-only HBA

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Liste der Änderungen.....	3
2.1 Änderung 1.....	3
2.2 Änderung 2.....	3

1 Änderungsbeschreibung

Das Team Smartcard beschäftigt sich mit dem Themenkomplex RSA2ECC Migration. Auslöser sind Festlegungen in [gemSpec_Krypt] wonach Kryptografie auf Basis von RSA mit einer Schlüssellänge von 2048 bit nur bis 31.12.2025 einsetzbar ist, siehe [gemSpec_Krypt#5]. Insbesondere für den QES-Schlüssel des HBA regelt die BNetzA den Einsatzzeitraum von Kryptographie. Nach aktuellem Stand (8. April 2025) ist ein Einsatz von RSA-2048 bit Schlüsseln für QES nur bis zum 31.12.2025 zulässig.

Spätestens dann, wenn die derzeit in der HBA-Objektsystemspezifikation definierten RSA-Schlüssel mit einer Länge von 2048 Bit nicht mehr einsetzbar sind, ist es möglich derartige Schlüssel und Zertifikate nicht mehr auf Karten aufzubringen.

Dieser Änderungseintrag bezieht sich auf die Dokumentenversion 5.2.0 von [gemSpec_HBA_ObjSys_G2.1] (siehe https://gemspec.gematik.de/docs/gemSpec/gemSpec_HBA_ObjSys_G2_1/gemSpec_HBA_ObjSys_G2_1_V5.2.0/), die im Produkttypsteckbrief "gemProdT_HBA_ObjSys_G2_1_PTV_4.8.0-0" verwendet wird (siehe https://gemspec.gematik.de/docs/gemProdT/gemProdT_HBA_ObjSys_G2_1/gemProdT_HBA_ObjSys_G2_1_PTV_4.8.0-0_V1.0.1/). Der Änderungseintrag bezieht sich auf die Nicht-Personalisierung von Containern für RSA-Schlüssel und RSA-Zertifikate. Diese Änderung betrifft ausschließlich die Personalisierung eines initialisierten Objektsystems.

2 Liste der Änderungen

2.1 Änderung 1

In [gemSpec_HBA_ObjSys_G2.1] in der Dokumentenversion 5.2.0 werden folgende Anforderungen ersatzlos gestrichen:

1. Card-G2-A_3307-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048
2. Card-G2-A_3308-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048
3. A_15221-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048
4. Card-G2-A_3305 - PrK.HP.AUT.R2048 K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN /
5. Card-G2-A_3306 - PrK.HP.ENC.R2048 K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN /
6. A_15225 - DF.ESIGN / PrK.HP.SIG.R2048 K_Personalisierung: Personalisierte Attribute von MF /
7. Card-G2-A_3301-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048
8. Card-G2-A_3298 - PrK.HP.QES.R2048 K_Personalisierung: Personalisierte Attribute von MF / DF.QES /

2.2 Änderung 2

In [gemSpec_HBA_ObjSys_G2.1] in der Dokumentenversion 5.2.0 wird Kapitel 4.9 mit folgendem Inhalt neu aufgenommen:

4.9 Wegfall der Personalisierung von RSA-Objekten

Gemäß [gemSpec_Krypt#G2-A_4357-*) sind RSA-Schlüssel mit einer Modulslänge von 2048 bit nur zeitlich begrenzt einsetzbar. Anschließend ist es aus Sicht dieses Dokumentes weiterhin zulässig, die in diesem Dokument spezifizierten RSA-Schlüssel und RSA-Zertifikatscontainer wie bisher mit Schlüsselmaterial und Zertifikaten zu befüllen. Allerdings ist das mit Aufwand und Kosten verbunden, dem kein Nutzen innerhalb der TI gegenübersteht. Deshalb werden Anforderungen zur Personalisierung so geändert, dass RSA-Artefakte nach der Personalisierung "leer" sind, das heißt im Rahmen der Personalisierung nicht befüllt werden.

In späteren Dokumentenversionen werden die RSA-Artefakte nicht mehr enthalten sein.

Im Vergleich zur vorherigen Dokumentenversion wurden die Personalisierungsvorschriften für RSA-Artefakte entfernt. Hier folgen nun Festlegungen, wie mit den weiterhin vorhandenen RSA-Artefakten im Rahmen der Personalisierung zu verfahren ist:

A_27619 -K_Personalisierung: RSA-Schlüssel

Bei der Personalisierung MÜSSEN die im folgenden genannten RSA-Schlüsselobjekte (falls vorhanden und erforderlich), so behandelt werden, dass bei regelkonformer Nutzung des RSA-Schlüsselobjekts statt des Statuswortes '9000' = NoError ein Wert aus der Menge {'6400', '6982'} zurückgemeldet wird:

1. MF / DF.ESIGN / PrK.HP.AUT.R2048
2. MF / DF.ESIGN / PrK.HP.ENC.R2048
3. MF / DF.ESIGN / PrK.HP.SIG.R2048
4. MF / DF.QES / PrK.HP.QES.R2048.

[<=,HBA_G2.1_Pers,funkt. Eignung: Personalisierungsvalidierung]

A_27620 -K_Personalisierung: RSA-Zertifikatscontainer

Bei der Personalisierung MÜSSEN die im folgenden genannten RSA-Zertifikatscontainer (falls vorhanden und erforderlich), so behandelt werden, dass *positionLogicalEndOfFile* = 1 ist und das erste Oktett in *body* den Wert '00' hat:

1. MF / DF.ESIGN / EF.C.HP.AUT.R2048
2. MF / DF.ESIGN / EF.C.HP.ENC.R2048
3. MF / DF.ESIGN / EF.C.HP.SIG.R2048
4. MF / DF.QES / EF.C.HP.QES.R2048.

[<=,HBA_G2.1_Pers,funkt. Eignung: Personalisierungsvalidierung]

Hinweis: Um Fehlersituationen im Feld zu vermeiden, wird im Rahmen von Interoperabilitätstests nachgewiesen, dass die übrigen TI-Komponenten die geänderten Karten unterstützen. Ein verbindlicher Zeitplan für den Rollout der betroffenen TI-Komponenten wird zeitnah festgelegt.