
C_12232_Anlage

ECC-only gSMC-K

Inhaltsverzeichnis

| | |
|-------------------------------------|----------|
| 1 Änderungsbeschreibung..... | 2 |
| 2 Liste der Änderungen..... | 3 |
| 2.1 Änderung 1..... | 3 |
| 2.2 Änderung 2..... | 4 |
| 2.3 Änderung 3..... | 5 |

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].

Spätestens dann, wenn die derzeit in der gSMC-K-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 3.14.0 von [gemSpec_gSMC-K_ObjSys] (siehe https://gemspec.gematik.de/docs/gemSpec/gemSpec_gSMC-K_ObjSys/gemSpec_gSMC-K_ObjSys_V3.14.0/), die im Produkttypsteckbrief "gemProdT_gSMC-K_ObjSys_PTV_4.6.0-0" verwendet wird (siehe https://gemspec.gematik.de/docs/gemProdT/gemProdT_gSMC-K_ObjSys/gemProdT_gSMC-K_ObjSys_PTV_4.6.0-0_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_gSmC-K_ObjSys] in der Dokumentenversion 3.14.0 werden folgende Anforderungen ersatzlos gestrichen:

1. Card-G2-A_3580 - K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten
2. Card-G2-A_3401 - K_Personalisierung: Personalisierte Attribute von MF / PrK.GP.R2048
3. Card-G2-A_3400 - K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.AUT.R2048
4. Card-G2-A_3338 - K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.ENC.R2048
5. Card-G2-A_3376 - K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.TLS.R2048
6. Card-G2-A_3382 - K_Personalisierung: Personalisierte Attribute von MF / PrK.SDS.R2048
7. Card-G2-A_3402 - K_Personalisierung: Personalisierte Attribute von MF / PuK.GP.R2048
8. Card-G2-A_3450 - K_Personalisierung: Personalisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048
9. Card-G2-A_3406 - K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048
10. Card-G2-A_3407 - K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048
11. Card-G2-A_3410 - K_Personalisierung: Personalisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048
12. Card-G2-A_3416 - K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.CFS.R2048
13. Card-G2-A_3411 - K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048
14. Card-G2-A_3417 - K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PuK.CFS.R2048
15. Card-G2-A_3423 - K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048
16. Card-G2-A_3424 - K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048
17. Card-G2-A_3431 - K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048
18. Card-G2-A_3434 - K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048

2.2 Änderung 2

In [gemSpec_gSMC-K_ObjSys] in der Dokumentenversion 3.14.0 wird Kapitel 4.10 mit folgendem Inhalt neu aufgenommen:

4.10 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. Danach ist es 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_27633 -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 / PrK.GP.R2048
2. MF / PrK.KONN.AUT.R2048
3. MF / PrK.KONN.ENC.R2048
4. MF / PrK.KONN.TLS.R2048
5. MF / PrK.SDS.R2048
6. MF / DF.AK / PrK.AK.AUT.R2048
7. MF / DF.AK / PrK.AK.CA_PS.R2048
8. MF / DF.NK / PrK.CFS.R2048
9. MF / DF.NK / PrK.NK.VPN.R2048
10. MF / DF.SAK / PrK.SAK.AUT.R2048
11. MF / DF.SAK / PrK.SAK.CA_xTV.R2048
12. MF / DF.SAK / PrK.SAK.SIG.R2048.

[<=,gSMC-K_G2_Pers,funkt. Eignung: Personalisierungsvalidierung]

A_27634 -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 / EF.PuK.RCA.CS.R2048 für Testkarten
2. MF / DF.AK / EF.C.AK.AUT.R2048

3. MF / DF.NK / EF.C.NK.VPN.R2048
4. MF / DF.SAK / EF.C.SAK.AUT.R2048.

【<=,gSMC-K_G2_Pers,funkt. Eignung: Personalisierungsvalidierung】

2.3 Änderung 3

In Kapitel 5.4.3, Absatz 2 wird der Passus "C.AK.AUT.R2048" wie folgt ersatzlos gestrichen:

Bei Wechsel des Schlüsselmaterials zu einem späteren Zeitpunkt, können durch ein Kartenadministrationssystem (CMS oder CUpS) in dieser Datei wahlweise auch die Zertifikate C.AK.AUT.R3072, ~~C.AK.AUT.R2048~~ oder C.AK.AUT.E384 gespeichert werden.

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 Ein verbindlicher Zeitplan für den Rollout der betroffenen TI-Komponenten wird zeitnah festgelegt.