

## 1 1.1 Einleitung

2 Das Team Smartcard beschäftigt sich mit dem Themenkomplex „RSA-Container aus der  
3 eGK-Objektsystemspezifikation entfernen“ auf Basis einer Anfrage aus der TUAG des  
4 GKV-Spitzenverbandes. Auslöser sind Festlegungen in [gemSpec\_Krypt]  
5 wonach Kryptografie auf Basis von RSA mit einer Schlüssellänge von 2048 Bit nur bis  
6 31.12.2025 einsetzbar ist, siehe [gemSpec\_Krypt#5].

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

10 Dieser Änderungseintrag bezieht sich auf die Dokumentenversion 4.6.0 von  
11 [gemSpec\_eGK\_ObjSys\_G2.1], die im Produkttypsteckbrief  
12 "gemProdT\_eGK\_ObjSys\_G2\_1\_PTV\_4.7.0-0" verwendet wird. Der Änderungseintrag  
13 bezieht sich auf die Entpersonalisierung von Containern für RSA-Schlüssel und RSA-  
14 Zertifikate. Diese Änderung betrifft ausschließlich die Personalisierung eines initialisierten  
15 Objektsystems.

16 *Hinweis 1: Die gematik betrachtet es als zulässig auch über das Ende des*  
17 *Einsatzzeitraumes von RSA 2048 bit Schlüsseln hinaus Karten des Typs eGK*  
18 *gemäß "gemProdT\_eGK\_ObjSys\_G2\_1\_PTV\_4.7.0-0" herauszugeben. Diese enthalten*  
19 *dann RSA-Schlüsselmateral und RSA-Zertifikate, die innerhalb der TI nicht mehr*  
20 *einsetzbar sind.*

21 *Hinweis 2: Die gematik betrachtet es als sinnvoll Karten des Typs eGK basierend auf*  
22 *diesem Änderungseintrag herauszugeben, sobald das Ende des Einsatzzeitraums von RSA*  
23 *2048 bit Schlüsseln erreicht ist.*

24

---

## 2 Liste der Änderungen

---

### 25 2.1 Änderung 1

26 In [gemSpec\_eGK\_ObjSys\_G2.1] in der Dokumentenversion 4.6.0 werden folgende  
27 Anforderungen ersatzlos gestrichen:

- 28 1. Card-G2-A\_3217-01 - K\_Personalisierung MF / DF.ESIGN / EF.C.CH.AUT.R2048
- 29 2. Card-G2-A\_3218 - K\_Personalisierung MF / DF.ESIGN / EF.C.CH.AUTN.R2048
- 30 3. Card-G2-A\_3219 - K\_Personalisierung MF / DF.ESIGN / EF.C.CH.ENC.R2048
- 31 4. Card-G2-A\_3220 - K\_Personalisierung MF / DF.ESIGN / EF.C.CH.ENC.V.R2048
- 32 5. Card-G2-A\_3221 - K\_Personalisierung MF / DF.ESIGN / PrK.CH.AUT.R2048
- 33 6. Card-G2-A\_3222 - K\_Personalisierung MF / DF.ESIGN / PrK.CH.AUTN.R2048
- 34 7. Card-G2-A\_3223 - K\_Personalisierung MF / DF.ESIGN / PrK.CH.ENC.R2048
- 35 8. Card-G2-A\_3224 - K\_Personalisierung MF / DF.ESIGN / PrK.CH.ENC.V.R2048
- 36 9. Card-G2-A\_3225 - K\_Personalisierung MF / DF.QES / EF.C.CH.QES.R2048
- 37 10. Card-G2-A\_3227 - K\_Personalisierung MF / DF.QES / PrK.CH.QES.R2048

38

## 39 2.2 Änderung 2

40 In [gemSpec\_eGK\_ObjSys\_G2.1] in der Dokumentenversion 4.6.0 wird Kapitel 4.6 mit  
41 folgendem Inhalt neu aufgenommen:

### 42 4.6 Wegfall der Personalisierung von RSA- 43 Objekten

44 Gemäß [gemSpec\_Krypt#G2-A\_4357-\*] sind RSA-Schlüssel mit einer Modulslänge von  
45 2048 bit nur zeitlich begrenzt einsetzbar. Danach ist es weiterhin zulässig, die in diesem  
46 Dokument spezifizierten RSA-Schlüssel und RSA-Zertifikatscontainer wie bisher mit  
47 Schlüsselmaterial und Zertifikaten zu befüllen. Allerdings ist das mit Aufwand und Kosten  
48 verbunden, dem kein Nutzen innerhalb der TI gegenübersteht. Deshalb werden  
49 Anforderungen zur Personalisierung so geändert, dass RSA-Artefakte nach der  
50 Personalisierung "leer" sind, das heißt im Rahmen der Personalisierung nicht befüllt  
51 werden.

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

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

#### 57 **A\_25235 - K\_Personalisierung: RSA-Schlüssel**

58 Bei der Personalisierung MÜSSEN die im folgenden genannten RSA-Schlüsselobjekte (falls  
59 vorhanden und erforderlich), so behandelt werden, dass bei regelkonformer Nutzung des  
60 RSA-Schlüsselobjekts statt des Statuswortes '9000' = NoError ein Wert aus der Menge  
61 {'6400', '6982'} zurückgemeldet wird:

- 62 1. MF / DF.ESIGN / PrK.CH.AUT.R2048
- 63 2. MF / DF.ESIGN / PrK.CH.AUTN.R2048
- 64 3. MF / DF.ESIGN / PrK.CH.ENC.R2048
- 65 4. MF / DF.ESIGN / PrK.CH.ENCV.R2048
- 66 5. MF / DF.QES / PrK.CH.QES.R2048

67 [**<=**]

#### 68 **A\_25236 - K\_Personalisierung: RSA-Zertifikatscontainer**

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

- 72 1. MF / DF.ESIGN / EF.C.CH.AUT.R2048
- 73 2. MF / DF.ESIGN / EF.C.CH.AUTN.R2048
- 74 3. MF / DF.ESIGN / EF.C.CH.ENC.R2048
- 75 4. MF / DF.ESIGN / EF.C.CH.ENCV.R2048
- 76 5. MF / DF.QES / EF.C.CH.QES.R2048

77 [**<=**]

78 *Hinweis: Um Fehlersituationen im Feld zu vermeiden, wird im Rahmen von*  
79 *Interoperabilitätstests nachgewiesen, dass die übrigen TI-Komponenten die geänderten*

80 *Karten unterstützen. Ein verbindlicher Zeitplan zum Rollout für die betroffenen TI-*  
81 *Komponenten wird zeitnah festgelegt.*

---

## 82 3 Kommentare zum Änderungseintrag

---

83 Während der Abstimmung zur Vorabveröffentlichung wurden die im Folgenden  
84 dargestellten Kommentare gestellt.

### 85 3.1 Ausgabebeginn ECC-only

86 Frage: Wie wird sichergestellt, dass ECC-only eGKs erst ins Feld gebracht werden, wenn  
87 die Konnektoren diese flächendeckend unterstützen?

88 Antwort: Diese Frage wird durch den (neuen) Hinweis am Ende des (neuen Kapitels) 4.6  
89 beantwortet.

### 90 3.2 Option\_RSA\_CVC

91 Frage: Sollte die Option\_RSA\_CVC entfallen (Card-G2-A\_3784)?

#### 92 **Card-G2-A\_3784 - K\_eGK: Unterstützung RSA CV-Zertifikate**

93 Für eine eGK KANN für das Objektsystem ein COS verwendet werden,

94 a) das die Option\_RSA\_CVC implementiert hat.

95 b) das die Option\_RSA\_CVC nicht implementiert hat.

96

97 [**<=**]

98 Antwort: Card-G2-A\_3784 erlaubt es einem Herausgeber von eGK zwischen  
99 verschiedenen COS-Varianten zu wählen. Es ist nicht beabsichtigt diese Wahlfreiheit  
100 einzuschränken. Deshalb entfällt Card-G2-A\_3784 nicht mit diesem Änderungseintrag,  
101 sondern erst später.

### 102 3.3 Option\_RSA\_KeyGeneration

103 Frage: Sollte die Option\_RSA\_KeyGeneration entfallen (Card-G2-A\_3846, Card-G2-  
104 A\_3847)?

#### 105 **Card-G2-A\_3846 - K\_eGK: Onboard-RSA-Schlüsselgenerierung**

106 Falls eine eGK die Option\_RSA\_KeyGeneration nutzen will, MUSS für das Objektsystem  
107 ein COS verwendet werden, das die Option\_RSA\_KeyGeneration implementiert hat. [**<=**]

#### 108 **Card-G2-A\_3847 - K\_eGK: Vorhandensein Onboard-RSA-Schlüsselgenerierung**

109 Falls eine eGK die Option\_RSA\_KeyGeneration nicht nutzen will, KANN für das  
110 Objektsystem ein COS verwendet werden,

111 1. das die Option\_RSA\_KeyGeneration implementiert hat.

112 2. das die Option\_RSA\_KeyGeneration nicht implementiert hat.

113 [**<=**]

114 Antwort: Card-G2-A\_3846 und Card-G2-A\_3847 erlauben es einem Herausgeber von  
115 eGK zwischen verschiedenen COS-Varianten zu wählen. Es ist nicht beabsichtigt diese  
116 Wahlfreiheit einzuschränken. Deshalb entfallen Card-G2-A\_3846 und Card-G2-A\_3847  
117 nicht mit diesem Änderungseintrag, sondern erst später.

118 **3.4 Ende 2025**

119 [Kommentar: Der Änderungseintrag C\\_11325 legt dazu in gemSpec\\_Krypt fest, dass die](#)  
120 [Gültigkeitszeiträume der RSA Algorithmen "zulässig bis gemäß \[SOG-IS-2020\]" sind.](#)  
121 [Daher ist der 31. Dezember 2025 aus \[SOG-IS-2020\] der mit den Gesellschaftern](#)  
122 [vereinbarte Stichtag.](#)

123 [Empfehlung: Im Freitext von Kapitel 4.6 sollte besser nicht der Stichtag mit „Ende 2025“](#)  
124 [hart kodiert werden, sondern explizit auf die Festlegungen von \[SOG-IS-2020\] bzw. auf](#)  
125 [gemSpec\\_Krypt GS-A\\_4357-02 verwiesen werden.](#)

126 [Gelöst durch: Der Text am Anfang von Kapitel 4.6 verweist nun auf GS-A\\_4357-\\*](#).

127

128

129

130

131