Elektronische Gesundheitskarte und Telematikinfrastruktur

Errata 1 zur Zertifikatserstellung und Personalisierung

Online-Produktivbetrieb (Stufe 1)

Version:	1.0.0
Stand:	05.12.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_1_Zertifikatserstellung_Personalisierung]

Betroffene Produkttypen

Trust Service Provider X.509 (nonQES) - eGK - 1.5.0 / 1.7.1-0 / 1.7.2-0
Trust Service Provider X.509 (nonQES) - HBA - 1.7.2-0
Trust Service Provider X.509 (nonQES) - SMC-B - 1.8.0-0 / 1.9.1-0
Trust Service Provider X.509 (nonQES) - Komp - 1.8.0-2
SMC-B (personalisiert) - 4.4.0-2

ID	Dokument	Quelle	Beschreibung der Änderung	**Anpassung** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6639	gemSpec_Krypt	Tab_KRYPT_002 Tab_KRYPT_003	**Keine Beschränkung der RSA-Zertifikatsgültigkeitsdauern nach Ende 2023** Ein TSP-X.509nonQES darf die Gültigkeitsdauer von RSA basierten X.509-Zertifikaten nicht mit Ende 2023 begrenzen, wenn dadurch die Zertifikatsgültigkeitsdauer von 5 Jahren verringert wird. Die Durchsetzung der Zulässigkeitsbeschränkung von RSA mit weniger als 3000 Bit Schlüssellänge erfolgt durch die Heraussnahme des TSP-Zertifikats aus der TSL zum Ende der Zulässigkeit. Zusätzlich wird die Referenz für die Kryprographievorgaben vom BSI-Algorithmenkatalog auf den SOG-IS-Katalog geändert.	Siehe C_6639_Anlage	gemSpec_Krypt gemProdT_X509_TSP_nonQES_Komp gemProdT_X509_TSP_nonQES_eGK gemProdT_X509_TSP_nonQES_HBA gemProdT_X509_TSP_nonQES_SMC-B
C_6654	gemSpec_HBA_ObjSys, gemSpec_SMC-B_ObjSys	HPC.CS.R2048, HPC.AUTR_CVC.R2048, CA_SMC.CS:R2048, SMC.AUTR_CVC.R2048	**Personalisierung der RSA-CVC-Objekte mit Leerwerten ab dem 01.01.2019** Ab dem 01.01.2019 ist die Verwendung von G1-CVC-Zertifikaten gemäß gemSpec_Krypt und BSI-TR-03116-1 nicht mehr gestattet. Für HBA und SMC-B der Generation G2 muss festgelegt werden, mit welchen Daten die vorhandenen Container für diese Schlüssel und Zertifikate befüllt werden müssen.	Siehe C_6654_Anlage	gemSpec_HBA_ObjSys, gemProdT_HBA, gemSpec_SMC-B_ObjSys, gemProdT_SMC-B

Änderungsbedarf in gemSpec_Krypt

(Änderungen in Kap. 2.1.1.1 Digitale nicht-qualifizierte elektronische Signaturen)

…

Tabelle: Tab_KRYPT_002 Algorithmen für X.509-Identitäten zur Erstellung nicht-qualifizierter Signaturen für die Schlüsselgeneration „RSA“

Anwendungsfall	Vorgaben
Art und Kodierung des öffentlichen Schlüssels	RSA (OID 1.2.840.113549.1.1.1) zu verwendende Schlüssellänge: 2048 Bit, zulässig bis Ende 2023 [BSI-TR-03116-1], vgl. auch A_15590
Signatur eines Zertifikats Signatur einer OCSP-Response Signatur eines OCSP-Responder-Zertifikates Signatur einer CRL Signatur des Zertifikats das Basis der Signaturprüfung einer CRL ist	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) zu verwendende Schlüssellänge: 2048 Bit, zulässig bis Ende 2023 [BSI-TR-03116-1], vgl. auch A_15590

A_15590 – Zertifikatslaufzeit bei Erstellung von X.509-Zertifikaten mit RSA 2048 Bit

Ein TSP-X.509-nonQES, der X.509-Zertifikate erstellt auf Basis der Schlüsselgeneration „RSA“ (d. h., für den die Vorgaben aus Tab_KRYPT_002 gelten), MUSS das Ende der Zertifikatsgültigkeitsdauer für das auszustellende Zertifikat unabhängig von der in Tab_KRYPT_002 festgelegten Endedaten der Zulässigkeit der verwendeten RSA-Schlüssellängen festlegen.

<=

Erläuterung: Die technische Durchsetzung des Endes der Zulässigkeit von RSA mit weniger als 3000 Bit Schlüssellänge in X.509-Zertifikaten erfolgt durch die Herausnahme der entsprechenden RSA-basierten Sub-CA-Zertifikate aus der TSL zum Zeitpunkt des Ablaufens der Zulässigkeit (gemäß TIP1-A_2062). Ein TSP muss bzgl. der Zertifikatsgültigkeitsdauer der von ihm ausgegebenen Zertifikate das nach Spezifikationslage definierte Verhalten zeigen (i. A. Zertifikatsgültigkeitsdauer der ausgegebenen Zertifikate von 5 Jahren). Ein TSP kann auch mit dem Kartenherausgeber beliebige Gültigkeitsdauern unter 5 Jahren für die Laufzeit der vom TSP ausgegebenen Zertifikate vereinbaren.

(Änderungen in Kap. 2.1.1.2 Qualifizierte elektronische Signaturen)

…

Tabelle: Tab_KRYPT_003 Algorithmen für X.509-Identitäten zur Erstellung qualifizierter elektronischer Signaturen für die Schlüsselgeneration „RSA“

Anwendungsfälle	Vorgaben
Signatur des VDA-Zertifikats	Nachdem die eIDAS-Verordnung das Signaturgesetz vollständig abgelöst hat, steht es einem VDA frei zu entscheiden welche Signatur (bspw. signiert von einer beliebigen VDA-internen CA) sein VDA-Zertifikat haben soll. Insbesondere kann die Signatur mit einem Nicht-RSA-Verfahren erstellt werden. Eine auswertende Komponente muss mit beliebigen (also auch nicht-RSA basierten) Signaturen eines VDA-Zertifikats umgehen können (bspw. Signatur des VDA-Zertifikats nicht auswerten, Authentizität und Integrität des Zertifikats wird über die Vertrauensliste sichergestellt).
Art und Kodierung des öffentlichen EE-Schlüssels	RSA-Signaturvariante: **Entweder** OID 1.2.840.113549.1.1.1 (rsaEncryption) (zulässig bis Ende 2022 [SOG-IS-2018]) **oder** OID 1.2.840.113549.1.1.10 (id-RSASSA-PSS) [RFC-5756]. (ohne zeitliche Beschränkung der Zulässigkeit [SOG-IS-2018]) Die Auswahl obliegt dem EE-Zertifikatsausgebenden VDA. RSA-Schlüssellänge: zu verwendende Schlüssellänge: 2048 Bit, zulässig bis Ende ~~2022~~ 2024 [SOG-IS-2018]
Signatur eines Zertifikats, Signatur einer OCSP-Response oder Signatur eines OCSP-Responder-Zertifikates	**Entweder** sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) ~~zu verwendende Schlüssellänge: 2048 Bit, zulässig bis Ende 2018~~ (zulässig bis Ende 2022 [SOG-IS-2018]) **oder** id-RSASSA-PSS (1.2.840.113549.1.1.10) [RFC-5756] (ohne zeitliche Beschränkung der Zulässigkeit [SOG-IS-2018]) zu verwendende Schlüssellänge: 2048 Bit, zulässig bis Ende ~~2022~~ 2024 [SOG-IS-2018] Die Hashfunktion für die Hashwertberechnung der TBSCertificate-Datenstruktur MUSS eine nach ~~[ALGCAT]~~ [SOG-IS-2018] zulässige Hashfunktion („Agreed Hash Function“) sein. Als Hashfunktion SOLL SHA-256 [FIPS-180-4] verwendet werden. Als MGF MUSS MGF1 [PKCS#1] verwendet werden. Die innerhalb der MGF1 verwendete Hashfunktion MUSS die gleiche Hashfunktion sein, wie die Hashfunktion der Hashwertberechnung der TBSCertificate-Datenstruktur. (Dies entspricht der Empfehlung aus [RFC-5756] bzw. [RFC-

	4055, 3.1] und dient der Komplexitätsreduktion.) Die Saltlänge MUSS mindestens 256 Bit betragen. (Die Maximallänge des Salts ergibt sich nach [PKCS#1] in Abhängigkeit von der Länge des Moduls.)

…

(Abschnitt 3.3.2)

Mit der mittelfristigen Anhebung des zu erreichenden Sicherheitsniveaus auf 120 Bit (vgl. ~~[ALGCAT]~~ [SOG-IS-2018] und [BSI-TR-03116-1]) werden die folgenden Ciphersuiten mittelfristig verpflichtend.

…

(Abschnitt 4)

Dazu lehnt sie sich an die sehr starken kryptographischen Vorgaben für die qualifizierte elektronische Signatur ~~[ALGCAT]~~ [SOG-IS-2018] an.

…

(Abschnitt 5)

Für den qualifizierten Vertrauensraum ist ab Ende ~~2022~~ 2024 ~~[ALGCAT]~~ [SOG-IS-2018] und für die TI ab Ende 2023 ein Sicherheitsniveau von mindestens 120 Bit für alle kryptographischen Verfahren vorgeschrieben [BSI-TR-03116-1].

…

6.5.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
…	…
[BSI-TR-02102-1]	BSI TR-02102-1 Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ ~~Version 2016-01, Stand 15.02.2016~~ Version 2018-02, Stand 29.05.2018 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index

	_htm.html
[BSI-TR-02102-2]	BSI TR-02102-3 Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2018-01 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[BSI-TR-02102-3]	BSI TR-02102-3 Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)“ ~~Version 2016-01~~ Version 2018-01 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[BSI-TR-03116-1]	Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für ~~Projekte der Bundesregierung, Version: 3.19, Fassung Dezember 2015, 03.12.2015~~ Projekte der Bundesregierung, Version: 3.20, Fassung September 2018, 21.09.2018 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html
…	…
[SOG-IS-2018]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.1, June 2018 https://www.sogis.org/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf
…	…

Grund der Änderung:

Ab dem 01.01.2019 ist die Verwendung von G1-CVC-Zertifikaten gemäß [gemSpec_Krypt] und BSI-TR-03116-1 nicht mehr gestattet. Die notwendigen RSA-CVC-Zertifikate des HBA und der SMC-B zum Freischalten von eGK G1+ dürfen ab diesem Zeitpunkt nicht mehr durch die TSP ausgestellt werden.

SMC-B und HBA der Generation G2.1 werden erst nach diesem Datum zugelassen und enthalten keine Container für diese Schlüssel und Zertifikate, sind also funktional zur Freischaltung der eGK G1+ nicht geeignet. Eine Personalisierung der Schlüssel und RSA-CVC-Zertifikate entfällt daher grundsätzlich.

SMC-B und HBA der Generation G2 enthalten die Container für die Schlüssel und Zertifikate zur Freischaltung der eGK G1+. Eine Personalisierung dieser Container ist daher notwendig, erfolgt jedoch zukünftig mit „Leerwerten“.

Die hier dargestellte Änderung legt fest, wie die betroffenen Container des HBA und der SMC-B der Generation G2 ab dem 01.01.2019 in der Personalisierung befüllt werden müssen.

gemSpec_HBA_ObjSys wird wie folgt geändert:

Card-G2-A_3283 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048

Bei der Personalisierung von EF.C.HPC.AUTR_CVC.R2048 MÜSSEN die in Tab_HBA_ObjSys_092 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 15: Tab_HBA_ObjSys_092 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	‘01 55’ Oktett = 341 Oktett	bis 31.12.2018
body	C.HPC.AUTR_CVC.R2048 passend zu dem privaten Schlüssel in PrK.HPC.AUTR_CVC.R2048 [gemSpec_PKI]	~~siehe [gemSpec_COS]~~ bis 31.12.2018
positionLogicalEndOfFile	‚0‘ oder ‚01 55‘, passend zur Personalisierung des Attributs *body*	ab 01.01.2019
body	unbefüllt oder vollständig ‚00 …00‘	ab 01.01.2019

[<=]

Card-G2-A_3281 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_HPC.CS.R2048

Bei der Personalisierung von EF.C.CA_HPC.CS.R2048 MÜSSEN die in Tab_HBA_ObjSys_089 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 11: Tab_HBA_ObjSys_089 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	‘01 4B’ Oktett = 331 Oktett	bis 31.12.2018
body	C.CA_HPC.CS.R2048 gemäß [gemSpec_PKI]	bis 31.12.2018
positionLogicalEndOfFile	‚0‘ oder ‚01 4B‘, passend zur Personalisierung des Attributs *body*	ab 01.01.2019
body	unbefüllt oder vollständig ‚00 …00‘	ab 01.01.2019
body Option_Erstellung_von_Testkarten	C.CA_HPC.CS.R2048 gemäß [gemSpec_PKI] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]

[<=

Card-G2-A_3287 - K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048

Bei der Personalisierung von PrK.HPC.AUTR_CVC.R2048 MÜSSEN die in Tab_HBA_ObjSys_098 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab_HBA_ObjSys_098 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	~~wird personalisiert~~ bis 31.12.2018
keyAvailable	True	bis 31.12.2018
privateKey	Moduluslänge 2048 Bit Herstellerspezifisch „nicht nutzbar“ (z.B. mit Zufallswerten)	ab 01.01.2019
keyAvailable	Wildcard , passend zum Attribut *privateKey*	ab 01.01.2019

[<=]

gemSpec_SMC-B_ObjSys wird wie folgt geändert:

Card-G2-A_3348 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048

Bei der Personalisierung von EF.C.SMC.AUTR_CVC.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_071 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 14: Tab_SMC-B_ObjSys_071 Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'0155' Oktett = 341 Oktett	bis 31.12.2018
body	C.SMC.AUTR_CVC.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.SMC.AUTR_CVC.R2048	bis 31.12.2018
positionLogicalEndOfFile	‚0' oder ‚01 55', passend zur Personalisierung des Attributs *body*	ab 01.01.2019
body	unbefüllt oder vollständig ‚00 …00'	ab 01.01.2019
positionLogicalEndOfFile Ausprägung_ORG	~~Wildcard~~ ‚0' oder ‚01 55', passend zur Personalisierung des Attributs *body*	~~Entsprechend dem Verfahren des Personalisierers und dem Attribut body~~
body Ausprägung_ORG	~~Leer~~ ~~oder '00 … 00'~~ unbefüllt oder vollständig ‚00 …00'	~~Entsprechend dem Verfahren des Personalisierers und passend zu positionLogicalEndOfFile~~

[<=]

Card-G2-A_3346 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.R2048

Bei der Personalisierung von EF.C.CA_SMC.CS.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_068 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 10: Tab_SMC-B_ObjSys_068 Personalisierte Attribute von MF / EF.C.CA_SMC.CS.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'01 4B' Oktett = 331 Oktett	bis 31.12.2018
body	C.CA_SMC.CS.R2048 gemäß [gemSpec_PKI]	bis 31.12.2018
positionLogicalEndOfFile	‚0' oder ‚01 4B', passend zur Personalisierung des Attributs *body*	ab 01.01.2019
body	unbefüllt oder vollständig ‚00 …00'	ab 01.01.2019
positionLogicalEndOfFile Ausprägung_ORG	~~Wildcard~~ 0' oder ‚01 4B', passend zur Personalisierung des Attributs *body*	~~Entsprechend dem Verfahren des Personalisierers und~~

		~~dem Attribut body~~
body *Ausprägung_ORG*	~~Leer~~ ~~oder '00 … 00'~~ unbefüllt oder vollständig ‚00 …00'	~~Entsprechend dem Verfahren des Personalisierers und dem Wert von positionLogicalEndOfFile~~
body Option_Erstellung_von_Testkarten	C.CA_SMC.CS.R2048 gemäß [gemSpec_PKI] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]

[<=**]**

Card-G2-A_3353 - K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048

Bei der Personalisierung von PrK.SMC.AUTR_CVC.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_077 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab_SMC-B_ObjSys_077 Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	bis 31.12.2018
keyAvailable	True	bis 31.12.2018
privateKey Ausprägung_*ORG*	Moduluslänge 2048 Bit Herstellerspezifisch „nicht nutzbar" (z.B. mit Zufallswerten)	~~Entsprechend dem Verfahren des Personalisierers~~
keyAvailable Ausprägung_*ORG*	~~False,~~ ~~ggf. True~~ Wildcard, passend zum Attribut *privateKey Ausprägung _ORG*	~~Entsprechend dem Verfahren des Personalisierers~~
privateKey	Moduluslänge 2048 Bit Herstellerspezifisch „nicht nutzbar" (z.B. mit Zufallswerten)	ab 01.01.2019
keyAvailable	Wildcard , passend zum Attribut *privateKey*	ab 01.01.2019

[<=**]**