1 Einleitung

Diese Anlage zu C_11255 beschreibt Änderungen an gematik Spezifikationen bezüglich der Herausgabe von Gerätekarten des Typs gSMC-KT.

Hinweis: Gemäß Kapitel 2 werden bestimmte Teile aus [gemSpec_KT] entfernt. Dazu ist folgendes anzumerken:

1. *Absatz vor TIP1-A_6717 entfällt ersatzlos.*
2. *TIP1-A_6717 entfällt ersatzlos.*
3. *TIP1-A_7016 wird ersetzt durch A_23234.*
4. *TIP1-A_6718 entfällt ersatzlos.*
5. *TIP1-A_6719 wird ersetzt durch A_23235 und A_23358.*
6. *Absatz zwischen TIP1-A_6719 und TIP1-A_6720 wird ersetzt durch den Hinweis nach A_23235 und den Hinweis nach A_23358.*
7. *TIP1-A_6720 wird ersetzt durch A_23233.*
8. *A_18934 wird ersetzt durch A_23234.*

2 Änderungen an gemSpec_KT

2.1 Streichung

Der Absatz oberhalb von [gemSpec_KT#TIP1-A_6717] und [gemSpec_A_18934] sowie alle dazwischenliegenden Absätze und Anforderungen aus [gemSpec_KT] werden durch neue Passagen ersetzt, die im folgenden Unterkapitel dieser Anlage beschrieben werden.

2.2 Neue Anforderungen

2.2.1 Änderung 1

Unmittelbar oberhalb von [gemSpec_KT#TIP1-A_3180] wird folgende Anforderung neu eingefügt:

A_23356 - Kompatibilität eines eHealth-Kartenterminals mit gSMC-KT
Ein eHealth-Kartenterminal MUSS mit allen spezifikationskonformen Karten des Typs gSMC-KT interoperabel sein. **[<=]**

2.2.2 Änderung 1

Unmittelbar oberhalb von [gemSpec_KT#TIP1-A_3413] wird folgender Passus neu eingefügt:

A_23357 - Auslieferung eHKT mit gSMC-KT
Der eHealth-Kartenterminal Hersteller MUSS ein eHealth-Kartenterminal mit einer gSMC-KT ausliefern, welche den Anforderungen gemäß A_23233 entspricht. **[<=]**

2.2.3 Änderung 2

Unmittelbar unterhalb von [gemSpec_KT#TIP1-A_3413 wird folgender Passus neu eingefügt:

A_23235 - Prüfung vor einem Pairing
Der eHealth-Kartenterminal Hersteller MUSS es dem Administrator eines eHealth-Kartenterminals ermöglichen, die Authentizität und Integrität der gSMC-KT vor dem Pairing zwischen Konnektor und eHealth-Kartenterminal zu prüfen. Dazu MUSS der Hersteller diesbezügliche Prüfmöglichkeiten im Handbuch des eHealth-Kartenterminals beschreiben und den Administrator auf diese Prüfung vor dem Pairing hinweisen. **[<=]**

Hinweis: A_23235 ist als Handreichung für den Administrator gedacht, welche Prüfungen nach Empfang einer gSMC-KT und vor deren Verwendung durchzuführen sind. Die in A_23235 angesprochenen Punkte sprechen nur einen Teil der Prüfungen an, die ein Administrator sinnvollerweise durchführt. Beispielhaft werden im Folgenden weitere grundlegende Prüfungen angeführt, welche anbieterspezifisch anzupassen sind:

1. *Sinnvollerweise verwendet ein Administrator nur solche gSMC-KT, die tatsächlich bestellt wurden.*

2. *Beim Empfang bietet sich an Verpackung und Karten auf Unversehrtheit zu prüfen.*
3. *Idealerweise wird der angegebenen Absender mit dem erwarteten Absender abgeglichen. Dazu ist es notwendig, dass der Herausgebers Angaben zu Versandadressen zur Verfügung stellt. Möglicherweise finden sich derartige Angaben auf der Webseite des Herausgebers.*
4. *Für den Administrator bietet es sich an, die gSMC-KT optisch auf eventuelle Manipulationen auf dem Transportweg zu prüfen. Hierbei sind die erwarteten optischen Merkmale einer gSMC-KT hilfreich.*

2.2.4 Kapitel zur Herausgabe einer gSMC-KT

Vor Anhang A wird in [gemSpec_KT] ein neues Kapitel mit folgendem Inhalt neu aufgenommen:

5 Herausgeber gSMC-KT

Die gematik berechtigt zugelassene Hersteller von eHealth-Kartenterminals und zugelassene Anbieter für den Kartentyp SMC-B, Karten des Typs gSMC-KT für den Produktivbetrieb auszugeben.

A_23233 - Verwendung zugelassener Gerätekarten gSMC-KT
Der Herausgeber einer gSMC-KT MUSS für den Produktivbetrieb ausschließlich solche Gerätekarten des Typs gSMC-KT herausgeben, die von der gematik zugelassen sind und folgender Version entsprechen:

1. [gemProdT_gSMC-KT_ObjSys_G2_1_PTV_4.4.1-2] Version 1.0.0 oder neuer

[<=]

Hinweis: Gemäß A_23233 werden nur solche gSMC-KT angeboten, die "dual personalisiert sind", also sowohl eine RSA-basierte Identität besitzen, als auch eine, welche auf der Kryptographie mit elliptischen Kurven basiert.

A_23234 - Prüfung personalisierter gSMC-KT
Der Herausgeber einer gSMC-KT MUSS durch Prüfung sicherstellen, dass er nur solche Karten herausgibt, die spezifikationskonform personalisiert wurden. **[<=]**

A_23358 - Prüfung vor dem Einsetzen einer gSMC-KT
Der Herausgeber einer gSMC-KT MUSS es dem Administrator eines eHealth-Kartenterminals ermöglichen, die Authentizität und Integrität der gSMC-KT zu prüfen. Dazu MUSS er diesbezügliche Prüfmöglichkeiten beschreiben und den Administrator auf diese Prüfung hinweisen. **[<=]**

Hinweis: A_23358 ist als Handreichung für den Administrator gedacht, welche Prüfungen nach Empfang einer gSMC-KT und vor deren Verwendung durchzuführen sind. Die in A_23358 angesprochenen Punkte sprechen nur einen Teil der Prüfungen an, die ein Administrator sinnvollerweise durchführt. Beispielhaft werden im Folgenden weitere grundlegende Prüfungen angeführt, welche anbieterspezifisch anzupassen sind:

1. *Sinnvollerweise verwendet ein Administrator nur solche gSMC-KT, die tatsächlich bestellt wurden.*
2. *Beim Empfang bietet sich an Verpackung und Karten auf Unversehrtheit zu prüfen*
3. *Idealerweise wird der angegebenen Absender mit dem erwarteten Absender abgeglichen. Dazu ist es notwendig, dass der Herausgeber Angaben zu*

Versandadressen zur Verfügung stellt. Möglicherweise finden sich derartige Angaben auf der Webseite des Herausgebers.

4. *Für den Administrator bietet es sich an, die gSMC-KT optisch auf eventuelle Manipulationen auf dem Transportweg zu prüfen. Hierbei sind die erwarteten optischen Merkmale einer gSMC-KT hilfreich.*

© gematik – öffentlich_Entwurf

3 Änderungen an gemSpec_PKI

Es wird das Kapitel 5.5. wie folgt angepasst:

5.5 gSMC-KT – eHealth-Kartenterminal

Für gSMC-KT ausgestellte Zertifikate werden nicht statusgeprüft. Für diese Zertifikate muss ein TSP somit keinen Sperrdienst und keine Statusauskünfte bereitstellen.

Siehe dazu auch Anhang A der [gemRL_TSL_SP_CP#AnhA].

Das Zertifikat eines gSMC-KT enthält nur Informationen über die Identität des SMKT, des Geräteherstellers sowie des Zertifikateherausgebers. Die Bedeutung des Zertifikats beschränkt sich auf folgende Aspekte:

- die gSMC-KT basiert auf einer hierfür durch die gematik zugelassenen Chipkartenplattform
- das Zertifikat wurde durch einen hierfür durch die gematik zugelassenen TSP-X.509 nonQES an einengSMC-KT Herausgeber ~~KT-Hersteller~~ ausgestellt

Das Zertifikat einer ~~s~~ gSMC-KT repräsentiert nach dem Pairing die Identität eines eHealth-Kartenterminals.

5.5.1 Definition der Kartenterminalidentität

Die Identität einer gSMC-KT ist durch den *SubjectDN* (*subject distinguishedName*) des Zertifikats gegeben mit folgendem Aufbau:

- **`commonName = [ICCSN des gSMC-KT]`**
- **`organizationName = [Name des Herausgebers gSMC-KT ~~Kartenterminal-Herstellers~~],`**
- **`countryName = [Herkunftsland des Herausgebers gSMC-KT ~~Kartenterminal-Herstellers~~]`**

5.5.2 X.509 Zertifikatsprofile der gSMC-KT

5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT

GS-A_4604-01 - Umsetzung Zertifikatsprofil C.SMKT.AUT
Der TSP-X.509 nonQES MUSS C.SMKT.AUT gemäß Tab_PKI_241 umsetzen.

Tabelle 1: Tab_PKI_241 C.SMKT.AUT gSMC-KT

Element	Inhalt	Kar.	
certificate	C.SMKT.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		

		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	ICCSN der gSMC-KT	1	
		organizationalUnitName	Relevante Einheit des Herausgebers gSMC-KT	0-1	
		organizationName	Name des Herausgebers gSMC-KT	1	
		countryName	Herkunftsland des Herausgebers gSMC-KT	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Kartenterminals	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Herausgebers gSMC-KT	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smkt_aut>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}		0	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}		0	FALSE

			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_kt> gemäß [gemSpec_OID#GS-A_4446] professionOID = OID <oid_kt> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

127 **[<=]**

4 Änderungen an gemKPT_PKI_TIP

Es werden Anpassungen in Kapitel 2.7.3 wie folgt vorgenommen:

2.7.3 Kartenherausgeber

Kartenherausgeber (Gesellschafterorganisationen (ORG), Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller sowie weitere gSMC-KT Herausgeber) sind für die Herausgabe von eGK, HBA, SMC-B, gSMC-K und gSMC-KT zuständig. Die gematik ist für die Herausgabe von Prüfkarten zuständig.

(...)

2.7.3.4 Herausgeber von gSMC-K und gSMC-KT

~~Gerätehersteller~~ Konnektorhersteller sind für die Herausgabe von gerätebezogenen Sicherheitsmodulen (gSMC-K, ~~gSMC-KT~~) zuständig. Kartenterminal-Hersteller sowie weitere gSMC-KT Herausgeber sind für die Herausgabe von gerätebezogenen Sicherheitsmodulen (gSMC-KT) berechtigt. Als weitere gSMC-KT Herausgeber gelten zugelassene SMC-B Anbieter.

Sie veranlassen die Erstellung und Herausgabe einer gSMC-K bzw. gSMC-KT. ~~Zu Geräthersstellern gehören beispielsweise Kartenterminalhersteller.~~

(...)

Es werden Anpassungen in Kapitel 2.9.4 wie folgt vorgenommen:

2.9.4 Staging der Zertifikate im Kartenterminal

Der ~~Kartenterminalhersteller~~ gSMC-KT Herausgeber ist Antragsteller für die Zertifikate der gSMC-KT und liefert ~~das Gerät einschließlich des~~ das gerätebezogene Sicherheitsmodul des Kartenterminals (gSMC-KT) inklusive Zertifikat aus. ~~Der Kartenterminalhersteller ist der für die gSMC-KT verantwortliche Kartenherausgeber.~~

Zu diesem Zeitpunkt gibt es keinen Zusammenhang zwischen dem Zertifikat der gSMC-KT und der Identität irgendeines eHealth-Kartenterminals.

(...)

Es werden Anpassungen in Kapitel 2.9.6 wie folgt vorgenommen:

2.9.6 Verantwortlichkeiten für den Zertifikats-Lebenszyklus

(...)

Besonderheiten des Kartenterminals

~~Da das gSMC-KT-Zertifikat keinen Verweis auf ein bestimmtes Gerät enthält, wird für diese Zertifikate die Rolle des Herstellers von dem Herausgeber der gSMC-KT eingenommen.~~

Die Rolle des Betreibers wird bei Kartenterminals durch den Karteninhaber der~~s~~ gSMC-KT, (die Organisation, die das Kartenterminal in seiner Umgebung einsetzt) eingenommen.

(...)

2.9.6.5 Hersteller einer Komponente

Hersteller Kartenterminal

Der Kartenterminalhersteller kann ~~agiert~~ als Kartenherausgeber agieren und ist verantwortlich für die initiale Bereitstellung des für das Kartenterminal benötigten gerätespezifischen Sicherheitsmoduls gSMC-KT.

(...)

© gematik – öffentlich_Entwurf