

Einführung der Gesundheitskarte

Errata zu Release 1.5.1 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb

führt zu

Release 1.5.2

Version:	1.0.0
Stand:	11.01.2016
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_R1.5.2]

Betroffene Produkttypen	Neue Produkttypversion
Konnektor (VSDM)	1.6.0
Konnektor (QES)	2.7.0
VPN-Zugangsdienst	1.4.1
Mobiles Kartenterminal	1.3.0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_4788	CardTerminalService.xsd	DisplayMsg-Element	Der CardTerminalService des Konnektors erlaubt dem Aufrufer der Operationen EjectCard und RequestCard optional eine Zeichenkette "DisplayMsg" als Parameter im Aufruf mitzugeben, damit sie der Konnektor an das Kartenterminal übergibt und sie dort zur Anzeige gebracht werden. Die Schnittstelle zum KT verwendet CardTerminalService.xsd als Beschreibung. Dort ist fälschlicherweise eine Zeichenkettenlänge von 200 Zeichen fester Länge angegeben anstatt, wie es KTs nur zulassen, maximal 48 Zeichen. Deshalb muss die Datei CardTerminalService.xsd entsprechend angepasst werden..	Das Feld DisplayMsg in CardTerminalService.xsd wird wie folgt angepasst: <pre><element name="DisplayMsg"> <simpleType> <restriction base="string"> <maxLength value="48"/> </restriction> </simpleType> </element></pre>	CardTerminalService.xsd gemProdT_Kon (VSDM) gemProdT_Kon (QES)
C_4905	gemSpec_Kon	TIP1-A_4562 TIP1-A_4565 TIP1-A_4712	TIP1-A_4710 verbietet das Protokollieren personenbezogener Daten, aber CARD/INSERTED und CARD/REMOVED protokollieren aktuell auch CARDHOLDERNAME und KVNR. Auch die Protokollierung erfolgreicher Kryptooperationen schreibt diese Werte.	siehe Begleitdokument "C_4905_Anlage"	gemSpec_Kon
C_4983	gemProdT_SMC-B_PTV4.3.0 gemProdT_HBA_PTV4.2.0	siehe Anlage	Die Erfüllung einer Reihe von Anforderungen, insbesondere im Zusammenhang mit der Aufbringung privaten Schlüsselmaterials auf HBA und SMC-B kann nicht durch Testmaßnahmen im Rahmen der Personalisierungsvalidierung nachgewiesen werden. Für den Nachweis im Rahmen des Bestätigungsverfahrens ist daher für die betroffenen Anforderungen eine Herstellererklärung abzugeben.	Die betroffenen Anforderungen werden innerhalb der Produktypsteckbriefe für HBA und SMC-B verschoben jeweils aus Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test" in Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung" . Welche Anforderungen im Einzelnen betroffen sind, ist dem Begleitdokument "C_4983_Anlage" zu entnehmen.	gemProdT_SMC-B_PTV4.3.0 gemProdT_HBA_PTV4.2.0
C_4862	gemProdT_SMC-B_PTV4.3.0	Kapitel 3.3	Bei den beiden Anforderungen handelt es sich um Bemaßungen der Karte und der Kontakte. Da die Prüfung dieser Anforderungen bereits über die Zulassung des SMC-B Objektsystems erfolgt, macht die Prüfung im Rahmen der Personalisierung keinen Sinn.	Kapitel 3.3 der Anforderungen zur elektrischen, mechanischen und physikalischen Eignung mit den AFOs Card-G2-A_3478 und Card-G2-A_3513 wird entfernt	gemProdT_SMC-B_PTV4.3.0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5014	gemSpec_mobKT	TIP1-A_4957; TIP1-A_3816; TIP1-A_4271; Fließtext	<p>Gemäß [TIP1-A_3816] muss ein mobKT Karten mit unbekanntem Versionsnummern (COS-Versionsnummer und Objektsystemversionsnummer) als inkompatibel bewerten und die Verarbeitung der Karten ablehnen.</p> <p>Für G1plus-Karten (nur eGK) stellt dies kein Problem dar, da das zu unterstützende Set von G1plus-Karten abschließend festgelegt ist: es werden nur G1plus-eGKs mit COS-Version: 3.0.0 und eGK-Objektsystem-Version 3.0.1 unterstützt.</p> <p>Für G2-Karten ist diese Anforderung falsch, da zum einen das Set an zu unterstützenden Versionsnummern im ORS1-Release nicht abschließend festgelegt werden kann. Darüber hinaus würden bei Beibehaltung dieser Anforderung auch für den Anwendungszweck des mobKT (Lesen und Zwischenspeichern der VSD) kompatible G2-Karten grundsätzlich abgelehnt werden, wenn die Versionsnummer nicht im mobKT hinterlegt ist. Dies würde auch zukünftige G2-Kartenversionen betreffen, die durch das mobKT eigentlich technisch verarbeitet werden könnten.</p> <p>Eine Anpassung von [TIP1-A_4957], [TIP1-A_3816] und [TIP1-A_4271] ist zwingend notwendig, damit das mobKT auch zukünftige zum heutigen Zeitpunkt nicht bekannte G2-Kartenversionen unterstützen kann, wenn diese technisch verarbeitbar sind.</p> <p>Wird diese Änderung nicht durchgeführt, so wird ausschließlich das zum Zeitpunkt der Einreichung des Zulassungsobjekts bekannte Set an G2-Karten unterstützt. Alle anderen G2-Karten werden per se als inkompatibel abgelehnt und dementsprechend nicht unterstützt.</p>	Anpassungen hierzu siehe "C_5014_Anlage_20150918".	gemSpec_mobKT
C_4959	gematik_Pers_SMC-B.xsd		<p>Dem in der Schemadatei „gematik_Pers_SMC-B.xsd“ definierten Element „AntragsStatus“ ist kein Typ zugeordnet. Die fehlende Angabe stellt eine Abweichung zur Spezifikation gemSpec_Pers_SMC-B (Version 3.2.0) dar. Das Element „AntragsStatus“: weist eine unterschiedliche Groß-/Kleinschreibung im gematik_Pers_SMC-B.xsd gegenüber dem HBA-Pendant auf.</p>	<p>In gematik_Pers_SMC-B.xsd wird der Datentyp von AntragsStatus ergänzt:</p> <p>alt: <element name="AntragsStatus"/></p> <p>neu <element name="AntragsStatus" type="gematik:AntragStatusKey" /></p> <p>Im Element HbaAntragExport wird die Schreibweise „Antragsstatus“ an die anderen Fundstellen angepasst: AntragsStatus.</p>	gematik_Pers_SMC-B.xsd

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_4980	gematik_Pers_SMC-B.xsd, gematik_Pers_HBA.xsd, gemSpec_Pers_HBA.doc, gemSpec_Pers_SMC-B.doc		Die E-Mail-Regexp, die im Schema mitgegeben wird, erlaubt keine E-Mail-Adressen mit 2 Punkten hinter dem @. Somit lassen sich durchaus im Feld verwendete Adressen nicht für die Kommunikation / Hinterlegung im Zertifikat verwenden.	Um auch E-Mails mit der angegebenen Struktur übertragen zu können und von künftigen Änderungen im Standard unabhängig zu sein (Freigabe von Umlauten etc.), wird für die E-Mail-Adresse die Einschränkung auf ein Pattern aufgehoben. Der Datentyp EMailType wird gelöscht; das Element KommType wird wie folgt geändert: alt: <complexType name="KommType"> ... <element name="EMail" type="gematik:EMailType" minOccurs="0"></element> ... </complexType> neu: <complexType name="KommType"> ... <element name="EMail" type="string" minOccurs="0"></element> ... </complexType>	gematik_Pers_SMC-B.xsd, gematik_Pers_HBA.xsd, gemSpec_Pers_HBA.doc, gemSpec_Pers_SMC-B.doc
C_5024	gemSpec_Pers_HBA	Kapitel 2.2.1	In der Datenstruktur HbaFreigabe fehlt das Element EFN (elektronische Fortbildungsnummer). Es muss aber die Möglichkeit geben, auch diese Angabe zu übertragen, da sie (verpflichtender) Bestandteil der elektronischen Antragsfreigabe bei den HBA der Ärzteschaft ist.	HbaFreigabe wird um das optionale Element EFN erweitert. ALT: <element name="ProfessionItem" type="gematik:ProfessionItemKey" minOccurs="unbounded"/> <element name="TelematikID" type="gematik:String128Type"/> NEU: <element name="ProfessionItem" type="gematik:ProfessionItemKey" minOccurs="unbounded"/> <element name="EFN" type="gematik:EFN_Type" minOccurs="0"/> <element name="TelematikID" type="gematik:String128Type"/>	gemSpec_Pers_HBA gematik_Pers_HBA.xsd
C_5039	gemSpec_ZugD	TIP1-A_4368	Gemäß der bisherigen Formulierung in TIP1-A_4368 darf am SIS zum Internet keine Veränderung der DiffServ-Flag Werte erfolgen. Diese Forderung entspricht nicht dem ausgewiesenen Verhalten eines Application-Level-Gateway (ALG), welches gesetzte DSCP Werte generell verwirft und ggfs. gemäß manueller Konfiguration neu setzt. Gleichzeitig besteht ein Widerspruch zu TIP1-A_4345 wo die Verwendung eines ALG für das SIS gefordert ist.	TIP1-A_4368: alt: TIP1-A_4368 VPN-Zugangsdienst, DiffServ-Behandlung SIS zum Internet Der Secure Internet Service (SIS) des VPN-Zugangsdienstes MUSS an der Schnittstelle Sicherheitsgateway zum Internet die DiffServ-gemäße Behandlung von Datenverkehr unterstützen. Die Erkennung und/oder Verarbeitung der DiffServ-Flags darf die Werte nicht verändern. neu: TIP1-A_4368 VPN-Zugangsdienst, DiffServ-Behandlung SIS zum Internet Der Secure Internet Service (SIS) des VPN-Zugangsdienstes MUSS an der Schnittstelle Sicherheitsgateway zum Internet die DiffServ-gemäße Behandlung von Datenverkehr unterstützen. Das setzen der DiffServ-Markierung erfolgt manuell bei Anpassung der Sicherheitsbaseline entsprechend TIP1-A_4345 und wird für ausgesuchte bandbreiten-sensitive Protokolle vorgesehen (z.B. Voice over IP oder Video Konferenzen ...).	gemSpec_VPN_ZugD

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_4961	gematik_Pers_SMC-B.xsd, gematik_Pers_HBA.xsd, gemSpec_Pers_HBA.doc, gemSpec_Pers_SMC-B.doc		Es hat sich herausgestellt, dass bei Antragstellung eine Vielzahl von Erklärungen/Zustimmungen erteilt werden, die bisher nicht im Export-Datensatz abgebildet werden können. Damit lässt sich die Anforderung zum Export aller Antragsinformationen im vorgegebenen Format nicht erfüllen. Die Angaben zu den Erklärungen/ Zustimmungen des Antragstellers bei Antragstellung werden für den Export im Schema ergänzt.	Änderung gemäß Begleitdokument "C_4961_Anlage"	gematik_Pers_SMC-B.xsd, gematik_Pers_HBA.xsd, gemSpec_Pers_HBA.doc, gemSpec_Pers_SMC-B.doc
C_5036	CertificateService.xsd		In der Schemadatei CertificateService.xsd des Zertifikatsdienstes ist ein Fehler in Zeile 16: <element name="CtID" type="string"/> Der 3. Buchstabe von CtID ist ein kleines L anstatt eines großen I. Der Schreibfehler kann zu Behinderungen bei der Nutzung der SOAP-Schnittstelle des Konnektors führen. Das Element CtID wird in den Schemadateien des Kartenterminal-Dienstes in der richtigen Schreibweise verwendet, so dass beide Schreibweisen an der Außenschnittstelle des Konnektors auftreten.	In der Schemadatei wird in Zeile 16 im Element <element name="CtID" type="string"/> der 3. Buchstabe von CtID durch ein großes i statt eines kleinen L ersetzt. Die zweistellige Schemaversion bleibt erhalten, die Version der Schemadatei wird von "6.0.0" auf "6.0.1" hochgezählt.	CertificateService.xsd
C_5040	gemSpec_SMC_OPT	Card-G2-A_2012, Card-G2-A_2014	Der Aufdruck auf der SMC-B wird an die aktuell definierten Profilbezeichnungen gemäß [gemSpec-PKI] angepasst. Die Struktur des Aufdrucks wird so geändert, dass auch bei dreistelligen Profilbezeichnungen nicht mehr als 10 Zeichen gedruckt werden müssen.	Änderung gemäß Begleitdokument "C_5040_Anlage"	gemSpec_SMC_OPT
C_4899	gemSpec_PKI	Kap. 5.3.4, Tab_PKI_238, Tab_PKI_239, Tab_PKI_240; Anhang A, Kap. DKG, Tabelle 106: Tab_SMCB_KV-T	Die Tabelle 106: Tab_SMCB_KV-T beschreibt die Ausprägungen der SMC-B-Zertifikatsprofile für die DKTIG. Darin wird die Belegung des Attributes "organizationName" im Distinguished Name des Subject-Feldes verboten. Dies widerspricht den generischen Zertifikatsprofilen für die SMC-B, welche bisher die Belegung des Attributes "organizationName" explizit fordern. Dieser Widerspruch ist aufzulösen. Auch wurde vereinbart, dass in den SMC-B-Zertifikaten für die DKTIG im Attribut serialNumber andere eindeutige Identifier als die Institutionskennzeichen verwendet werden können. Darüber hinaus ist die verwendete Tabellenreferenz zwei Mal im Dokument vorhanden und damit nicht mehr eindeutig.	Siehe Begleitdokument "C_4899_C_5044_Anlage"	gemSpec_PKI
C_5044	gemSpec_PKI	Kap. 4.8.3.2 Kap. 5.3.4 Anhang A	Die Anforderungslage zur Admission-Erweiterung und deren Beschreibung sind unvollständig, insbesondere in Bezug auf das Setzen der admLssionAuthority (Zulassungsstelle). Die Formulierungen im Kapitel zur Admission-Erweiterung müssen deshalb geschärft werden, und in den SMC-B-Zertifikatsprofilen und in den sektorspezifischen Ausprägungen dieser muss angegeben werden, dass die admissionAuthority gesetzt werden kann.	Siehe Begleitdokument "C_4899_C_5044_Anlage"	gemSpec_PKI
C_4953	ARV_706.3_Spec_SST_KSR	Kap. 5.1.1; 6.1.1.4; 6.1.1.7; A7.2; 5.2	Die Spezifikation zu den KSR Schnittstellen ARV_706.3_Spec_SST_KSR hat die unterstützten Optionen der Update-Paket-Signaturen bisher nicht beschrieben. Damit die Hersteller von Konnektoren und Kartenterminals die Update-Pakete korrekt signieren können, wurde die Beschreibung der Signaturen erweitert. Weiterhin wurde das Berechtigungs- und Rollenkonzept optimiert (zwei Berechtigungsgruppen zusammengelegt).	Siehe ARV_706.3_Spec_SST_KSR, Version 1.9.0	ARV_706.3_Spec_SST_KSR

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_4958	gemSpec_SST_Komponenten-PKI	ganzes Dokument	Zur Bedienung der Schnittstellen der PKI für Dienste und Komponenten zur Ausstellung und Sperrung von Zertifikaten sind gegenüber der Version 1.4.0 des Dokumentes weitere Präzisierungen, Erläuterungen und Beispiele nötig.	Siehe gemSpec_SST_Komponenten-PKI, Version 1.9.3 mit gestaffelten Änderungsmarkierungen.	gemSpec_SST_Komponenten-PKI
C_4957	ARV_706.3_Spec_SST_gematik-Root-CA	Kapitel 4.4 & 4.5.1	Die Antragsdaten und der Sperrprozess müssen genauer beschrieben werden, damit es für Nutzer verständlich ist.	Siehe ARV_706.3_Spec_SST_gematik-Root-CA, Version 1.2.0	ARV_706.3_Spec_SST_gematik-Root-CA

Änderungen in [gemSpec_PKI]:

- Änderungen gemäß C_5044 sind in **Gelb** markiert
- Änderungen gemäß C_4899 sind in **Grün** markiert

4.8.3.2 Admission

Die Extension Admission enthält Angaben zur Registrierung und zu der beruflichen Zulassung (und somit auch zu daraus ableitbaren Autorisierungsinformationen) sowohl als Text als auch in Form einer maschinenlesbaren OID.

Für die verschiedenen Zertifikatstypen sind dies jeweils:

- die Berufsgruppen (HBA/BA),
- der Status als Versicherte/-r (eGK),
- der Typ der Institution (SMC-B) oder
- die technische Rolle (Komponentenzertifikate).

Außerdem können die Telematik-ID und die registrierende bzw. zulassende Stelle (admissionAuthority) in Admission eingetragen werden (in HBA-, BA- und SMC-B-Zertifikaten).

Die Extension Admission beinhaltet die Berufsgruppen (HBA, eGK), den Typ der Institution (SMC-B) oder die technische Rolle (Komponentenzertifikate) sowohl als Text als auch in Form einer maschinenlesbaren OID. Außerdem wird die Telematik-ID (nur in HBA-, BA und SMC-B-Zertifikaten) in Admission abgelegt.

☒ GS-A_4717 TI-spezifische Vorgabe zur Nutzung der Extension Admission

TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN bei Verwendung der Extension Admission {id-commonpki-at 3} die Struktur in X.509-Zertifikaten entsprechend Tab_PKI_226 erstellen. ☒

Tabelle 16: Tab_PKI_226 Struktur Admission

#	ASN.1 DEFINITION	TI-SPEZIFISCHE VORGABEN
1	id-isismtt-at-admission OBJECT IDENTIFIER ::= {id-isismtt-at 3}	
2	id-isismtt-at-namingAuthorities OBJECT IDENTIFIER ::= {id-isismtt-at 11}	
3	AdmissionSyntax ::= SEQUENCE {	
4	admissionAuthority GeneralName OPTIONAL,	Angabe (optional) der admissionAuthority auf der obersten Ebene der Extension in Form eines Distinguished Name (directoryName). In den jeweiligen Zertifikatsprofilen und -ausprägungen wird dieser Distinguished Name in Textform gemäß [RFC4514] dargestellt.

Anlage zu C_4899 SMC-B-Zertifikate DKG und
C_5044 admissionAuthority in X.509-Zertifikaten

5	<pre> contentsOfAdmissions SEQUENCE OF Admissions } </pre>	Diese Sequenz MUSS genau ein Element vom Typ Admissions enthalten.
6	<pre> Admissions ::= SEQUENCE { </pre>	
7	<pre> admissionAuthority [0] EXPLICIT GeneralName OPTIONAL, </pre>	
8	<pre> namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL, </pre>	
9	<pre> professionInfos SEQUENCE OF ProfessionInfo } </pre>	Diese Sequenz MUSS ein Element vom Typ ProfessionInfo enthalten.
...		
14	<pre> ProfessionInfo ::= SEQUENCE { </pre>	
15	<pre> namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL, </pre>	
16	<pre> professionItems SEQUENCE OF DirectoryString (SIZE(1..128)), </pre>	professionItems enthält ein Element von Typ DirectoryString Für DirectoryString MUSS die Kodierung UTF8String verwendet werden.
17	<pre> professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL, </pre>	Dieses Element MUSS eine OID enthalten.
18	<pre> registrationNumber PrintableString(SIZE(1..128)) OPTIONAL, </pre>	<p>Dieses Feld enthält die Telematik-ID.</p> <p>Dieses Feld SOLL genau ein Element enthalten. (Telematik-ID SOLL in allen Zertifikaten von HBA, BA und SMC B enthalten sein. Ausnahme: QES Zertifikat des HBA der Ärzte)</p>
19	<pre> addProfessionInfo OCTET STRING OPTIONAL } </pre>	

5.3.4 X.509 Zertifikatsprofile der SMC-B

5.3.4.1 C.HCI.AUT – Authentisierung SMC- B

☒ GS-A_4600 Umsetzung Zertifikatsprofil C.HCI.AUT

Der TSP-X.509 nonQES MUSS C.HCI.AUT gemäß Tab_PKI_238 umsetzen. ☒

Tabelle 25: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B

Element	Inhalt *)	Kar.	
Certificate	C.HCI.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	Distinguished Name (DN) der Aussteller-CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	Erste zwei Zeilen des Adressfeldes	1	
title	Titel des Verantwortlichen/Inhabers	0-1	
surName	Nachname des Verantwortlichen/Inhabers	0-1	
givenName	Vorname des Verantwortlichen/Inhabers	0-1	
serialNumber	Ti-weit eindeutige Identifikationsnummer	1	
streetAddress	Strasse, Hausnummer	0-1	
postalCode	Postleitzahl	0-1	
localityName	Stadt	0-1	
stateOrProvinceName	Bundesland	0-1	
organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1	+
countryName	DE	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 der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	TRUE
SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen	0-1 0-1	FALSE

Element	Inhalt *)	Kar.	
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smc_b_aut>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

*) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu entnehmen

5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B

☒ GS-A_4601 Umsetzung Zertifikatsprofil C.HCI.ENC

Der TSP-X.509 nonQES MUSS C.HCI.ENC gemäß Tab Tab_PKI_239 umsetzen. ☒

Tabelle 26: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B

Element	Inhalt *)	Kar.	
certificate	C.HCI.ENC		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
issuer	Distinguished Name (DN) der Aussteller-CA		
validity	Gültigkeit des Zertifikats (von – bis)		

Anlage zu C_4899 SMC-B-Zertifikate DKG und
C_5044 admissionAuthority in X.509-Zertifikaten

Element	Inhalt *)	Kar.	
subject			
commonName	Erste zwei Zeilen des Anschriftenfeldes	1	
title	Titel des Verantwortlichen/Inhabers	0-1	
surName	Nachname des Verantwortlichen/Inhabers	0-1	
givenName	Vorname des Verantwortlichen/Inhabers	0-1	
serialNumber	Ti-weit eindeutige Identifikationsnummer	1	
streetAddress	Strasse, Hausnummer	0-1	
postalCode	Postleitzahl	0-1	
localityName	Stadt	0-1	
stateOrProvinceName	Bundesland	0-1	
organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1 1	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt# GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FAL-SE
KeyUsage {2 5 29 15}	keyEncipherment dataEncipherment	1 1	TRUE
SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen	0-1 0-1	FAL-SE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smc_b_enc>	1 0-1 1	FAL-SE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FAL-SE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FAL-SE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FAL-SE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,<C=DE> professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FAL-SE
ExtendedKeyUsage {2 5 29 37}		0	

Element	Inhalt *)	Kar.	
	<i>andere Erweiterungen</i>	0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
signature	Wert der Signatur		

*) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu entnehmen

5.3.4.3 C.HCI.OSIG – Signatur SMC-B

☒ GS-A_4602 Umsetzung Zertifikatsprofil C.HCI.OSIG

Der TSP-X.509 nonQES MUSS C.HCI.OSIG gemäß Tab_PKI_240 umsetzen. ☒

Tabelle 27: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B

Element	Inhalt *)	Kar.	
certificate	C.HCI.OSIG		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	Distinguished Name (DN) der Aussteller-CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	Erste zwei Zeilen des Anschriftenfeldes	1	
title	Titel des Verantwortlichen/Inhabers	0-1	
surName	Nachname des Verantwortlichen/Inhabers	0-1	
givenName	Vorname des Verantwortlichen/Inhabers	0-1	
serialNumber	Ti-weit eindeutige Identifikationsnummer	1	
streetAddress	Strasse, Hausnummer	0-1	
postalCode	Postleitzahl	0-1	
localityName	Stadt	0-1	
stateOrProvinceName	Bundesland	0-1	
organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1 4	
countryName	DE	1	
<i>andere Attribute</i>		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		

Element	Inhalt *)	Kar.	
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FAL-SE
KeyUsage {2 5 29 15}	nonRepudiation	1	TRUE
SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen	0-1 0-1	FAL-SE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smc_b_osig>	1 0-1 1	FAL-SE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FAL-SE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FAL-SE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FAL-SE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FAL-SE
ExtendedKeyUsage {2 5 29 37}		0	
andere Erweiterungen		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
signature	Wert der Signatur		

*) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu entnehmen

Anhang A

Sektorspezifische Ausprägungen der SMC-B Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap 5.3.4 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HCI.AUT
- C.HCI.ENC
- C.HCI.OSIG

Während der Erprobungsphase ORS1 enthalten die Zertifikate im Feld **Certificate-Policies** zusätzlich die Policy-OID der „Policy für SMC-B Zertifikate während Erprobung“¹. Nach Abschluss der Erprobungsphase sowie Finalisierung sektorspezifischer Parameter und Prozesse wird diese OID entsprechend abgelöst. Die während der Erprobungsphase ausgegebenen Zertifikate behalten ihre Gültigkeit bis zu ihrem zeitlichen Ablauf.

KZBV

Tabelle 103: Tab_SMCB_KZBV SMC-B-Zertifikate für Sektor KZBV

Element	Inhalt	Kar.
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG	
tbsCertificate		
version	siehe Kap 5.3.4	
serialNumber	siehe Kap 5.3.4	
signature	siehe Kap 5.3.4	
issuer	siehe Kap 5.3.4	
validity	siehe Kap 5.3.4	
subject		
commonName	Gemäß Freigabedaten der zuständigen KZV	1
title	nicht belegt	0
surName	nicht belegt	0
givenName	nicht belegt	0
serialNumber	TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN>	1
streetAddress	nicht belegt	0

¹ „Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL - Sektorspezifische Präzisierung für SMC-B-Zertifikate in Erprobungsphase ORS1“. [oid_policy_gem_or_cp_smcb_erprobung].

Element	Inhalt	Kar.		
postalCode	nicht belegt	0		
	localityName	nicht belegt	0	
	stateOrProvinceName	nicht belegt	0	
	organizationalUnit-Name	nicht belegt	0	
	organizationName	Telematik-ID gemäss Freigabedaten der zuständigen KZV	1	
	countryName	siehe Kap 5.3.4	1	
	andere Attribute		0	
	subjectPublicKeyInfo	siehe Kap 5.3.4		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
	KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE
	SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
	BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	TRUE
CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: policyIdentifier = <oid_policy_gem_or_cp_smcb_erprobung>	1	FALSE	
CRLDistribution-Points {2 5 29 31}	CDP des TSP für das betreffende Zertifikat	1	FALSE	
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE	
AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE	
Admission {1 3 36 8 3 3}	admissionAuthority = {O=<von der KZBV benannte attributbestätigende Stelle - zuständige KZV>,C=DE} professionItem = <oid_zahnarztpraxis> professionOID = <oid_zahnarztpraxis> registrationNumber = <Telematik-ID gemäss Freigabedaten der zuständigen KZV>	1 1 1 1	FALSE	
ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	1	FALSE	
andere Erweiterungen		0		
signatureAlgorithm	siehe Kap 5.3.4			
signature	siehe Kap 5.3.4			

KBV KV-Telematik ARGE

Die nachfolgende Profiltabelle der durch die KV-Telematik ARGE betreuten Sektoren gilt für die Sektoren:

Niedergelassene Vertragsärzte (KV)

Niedergelassene Psychologische Psychotherapeuten (KV)

Niedergelassene Kinder- und Jugendlichenpsychotherapeuten (KV)

Nicht-Vertragsärzte (KBV)

Tabelle 104: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KV-Telematik-ARGE

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	Erste zwei Zeilen der Anschriftenzone (DIN5008), somit „Kurzname“ der Institution, so wie für das Anschriftenfeld definiert.	1	
title	Titel des Verantwortlichen/Inhabers	0-1	
surName	Familiename des Verantwortlichen/Inhabers	0-1	
givenName	Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt)	0-1	
serialNumber	TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN>	1	
streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	0-1	
postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	0-1	
localityName	Stadt des Institut-Standortes	0-1	
stateOrProvinceName	Bundesland des Institut-Standortes	0-1	
organizationalUnit-Name	nicht belegt	0	
organizationName	9-stellige Betriebsstättennummer (z.B. „121234512“) der Praxis als eindeutige Nummer. Für privat abrechnende Ärzte wird hier eine 10-stellige Ersatznummer eingefügt.	1	
countryName	siehe Kap 5.3.4	1	
andere Attribute		0	
subjectPublicKeyInfo	siehe Kap 5.3.4		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE

Element	Inhalt	Kar.	
SubjectAltNames {2 5 29 17} BasicConstraints {2 5 29 19} CertificatePolicies {2 5 29 32} CRLDistribution-Points {2 5 29 31} AuthorityInfoAccess {1 3 6 1 5 5 7 1 1} AuthorityKeyIdentifier {2 5 29 35} Admission {1 3 36 8 3 3} ExtendedKeyUsage {2 5 29 37} andere Erweiterungen	siehe Kap 5.3.4	0-1	FALSE
	siehe Kap 5.3.4	1	TRUE
	siehe Kap 5.3.4 zusätzlich: policyIdentifier = <oid_policy_gem_or_cp_smcb_erprobung>	1	FALSE
	CDP des TSP für das betreffende Zertifikat	1	FALSE
	siehe Kap 5.3.4	1	FALSE
	siehe Kap 5.3.4	1	FALSE
	admissionAuthority: nicht gesetzt professionItem = <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut> professionOID = <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut> registrationNumber = siehe Tabelle Tab_SMCB_TID_KV-T (Es wird genau eine Admission-Struktur verwendet, mit je genau einem Element: professionInfo, professionItem, registrationNumber)	0 1 1 1	FALSE
	siehe Kap 5.3.4	1	FALSE
		0	
signatureAlgorithm	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		

Tabelle 105: Tab_SMCB_TID_KV-T Aufbau Telematik-ID in SMC-B-Zertifikaten der Sektoren der KV-Telematik-ARGE

Präfix	Separator	Fortsatz	SMC für:									
1 (Arztpraxen)	-	2 (SMC)	0 (KV System registrierte Betriebsstätte)	KV-Nr.	BSNR				frei wählbar			
				x	x	x	x	x	x	x	x	x
			1 (privat abrechnender Arzt)	generierte, neunstellige Nummer								
				x	x	x	x	x	x	x	x	x

DKG

Die nachfolgende Profiltabelle der DKTIG gilt für den Sektor:

Krankenhäuser (DKTIG)

Tabelle 106: Tab_SMCB_DKTIGTab_SMCB_KV-T SMC-B-Zertifikate für Sektor der DKTIG

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	Gemäss Freigabedaten der DKTIG.	1	
title	nicht belegt	0	
surName	nicht belegt	0	
givenName	nicht belegt	0	
serialNumber	Institutionskennzeichen des Krankenhauses TI-weit eindeutiger Identifier	1	
streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	1	
postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	1	
localityName	Stadt des Institut-Standortes	1	
stateOrProvinceName	Bundesland des Institut-Standortes	1	
organizationalUnit-Name	nicht belegt	0	
organizationName	nicht belegt abgeleitet aus dem Institutionskennzeichen eines Krankenhauses	0 0-1	
countryName	siehe Kap 5.3.4	1	
andere Attribute		0	
subjectPublicKeyInfo	siehe Kap 5.3.4		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE
SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	TRUE

Element	Inhalt	Kar.	
CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: policyIdentifier = <oid_policy_gem_or_cp_smcb_erprobung>	1	FALSE
CRLDistribution-Points {2 5 29 31}	siehe Kap 5.3.4	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=<von der DKG benannte attributbestätigende Stelle>,C=DE} professionItem = <Krankenhaus> professionOID = <oid_krankenhaus> registrationNumber = siehe Tabelle Tab_SMCB_TID_DKTIG	1 1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		

Tabelle 107: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der DKTIG

Präfix s. Kap 4.7.2.1	Separator s. Kap 4.7.2.2	Fortsatz s. Kap 4.7.2.3
Krankenhaus		SMC-B Kennzeichen + Institutsindividuelle Kennzeichnung
5	-	2 <gem. Freigabedaten der DKTIG>

B5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
...	
[RFC4514]	RFC 4514 (Juni 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names https://tools.ietf.org/html/rfc4514
...	

☒ **TIP1-A_4562 Reaktion auf „Karte entfernt“**

Empfängt der Kartendienst das Ereignis „CT/SLOT_FREE“, so MUSS der Konnektor:

- das über die im Ereignis gemeldeten Parameter CtID und SlotNo in CM_CARD_LIST adressierte CardObject CARD identifizieren
- für dieses CardObject folgendes Ereignis absetzen:
TUC_KON_256{„CARD/REMOVED“; Op; Info; <Params>} wobei <Params> mit folgenden Werten belegt werden MUSS:
 - „CardHandle=\$CARD.CARDHANDLE;
 - Type=\$CARD.TYP;
 - CardVersion=\$CARD.VER;
 - ICCSN=\$CARD.ICCSN
 - CtID=\$CARD.CTID
 - SlotID=\$CARD.SLOTID
 - InsertTime=\$CARD.INSERTTIME
 - CardHolderName=\$CARD.CARDHOLDERNAME
 - KVNR=\$CARD.KVNR“
- das zugehörige CardObject aus CM_CARD_LIST entfernen

CardHolderName und KVNR DÜRFEN NICHT protokolliert werden. ☒

☒ **TIP1-A_4565 TUC_KON_001 „Karte öffnen“**

Der Konnektor MUSS den technischen Use Case “Karte öffnen“ gemäß TUC_KON_001 umsetzen.

Tabelle 53: TAB_KON_734 - TUC_KON_001 „Karte öffnen“

Element	Beschreibung
Name	TUC_KON_001 „Karte öffnen“
Beschreibung	Der TUC initialisiert ein Card-Object basierend auf einer physikalischen Karte und fügt es CM_CARD_LIST zu. Die Karten kann erst im Anschluss unter Verwendung des erzeugten CardHandles verwendet werden.
Auslöser	<ul style="list-style-type: none"> • Der Kartenterminaldienst meldet das Belegen eines KT-Slots
Vorbedingungen	<ul style="list-style-type: none"> • In CtID/SlotNo steckt eine Karte
Eingangsdaten	<ul style="list-style-type: none"> • CtID • SlotNo
Komponenten	Karte, Kartenterminal, Konnektor

Element	Beschreibung
Ausgangsdaten	Keine
Standardablauf	<p>1. Prüfe, ob unter CtID und SlotNo ein Eintrag in CM_CARD_LIST vorhanden ist. Wenn bereits ein Eintrag vorhanden ist, lösche diesen.</p> <p>2. Erzeuge neuen Card-Object-Eintrag in CM_CARD_LIST und</p> <p>a) Generiere CARD.CARDHANDLE. mit folgenden Anforderungen:</p> <ul style="list-style-type: none"> ▪ Das CardHandle MUSS innerhalb CM_CARD_LIST eindeutig sein ▪ Ein ungültig gewordenes CardHandle DARF innerhalb von 48h NICHT als neues CardHandle vergeben werden <p>b) Befülle CARD.CTID und CARD.SLOTNO mit den Eingangsdaten</p> <p>c) Ermittle und befülle (soweit durch Karte unterstützt) die folgenden Daten:</p> <ul style="list-style-type: none"> ▪ CARD.ICCSN ▪ CARD.TYPE (mögliche Werte siehe Tabelle 1: TAB_KON_500 Wertetabelle Kartentypen) ▪ CARD.CARDVERSION ▪ CARD.INSERTTIME (=aktuelle Systemzeit) ▪ CARD.CARDHOLDERNAME (aus X.509-AUT-Zertifikat) ▪ CARD.KVNR (nur für eGK, aus C.CH.AUT) ▪ CARD.CERTEXPIRATIONDATE (=validity aus X.509-AUT-Zertifikat) <p>X.509-AUT-Zertifikat bezeichnet für eGK das C.CH.AUT-Zertifikat, für HBA das C.HP.AUT-Zertifikat und für SMC-B das C.HCI.AUT-Zertifikat.</p> <p>3. Rufe TUC_KON_256{„CARD/INSERTED“; Op; Info; <Params>} mit <Params> belegt aus dem CARD-Object: „CardHandle=\$; CardType=\$; CardVersion=\$; ICCSN=\$;CtID=\$; SlotID=\$;InsertTime=\$; CardholderName=\$; KVNR=\$; CertExpirationDate=\$“</p> <p>CardHolderName und KVNR DÜRFEN NICHT protokolliert werden.</p>
Varianten/Alternativen	<p>a) Im Falle der KVK gibt es kein EF.ATR, EF.GDO und EF.DIR. Es wird daher lediglich der ATR ausgewertet, den das Kartenterminal beim Stecken der Karte liefert.</p>
Fehlerfälle	<p>(-> 2c) Karte/Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode <gemäß [gemSpec_COS]/[SICCT]></p> <p>Alle anderen Fehler beim Zugriff auf die Karte führen dazu, dass keine weiteren Zugriffsversuche unternommen werden. Es wird jedoch trotzdem die Karte in die interne Liste des Konnektors aufgenommen. Konnte bis zu diesem Zeitpunkt Card.Type noch nicht bestimmt werden, wird UNKNOWN verwendet. Schritt 3 wird in jedem Fall aufgerufen.</p>

Element	Beschreibung
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine



☒ TIP1-A_4712 Protokollierung erfolgreicher Kryptooperationen

Wenn LOG_SUCCESSFUL_CRYPTOPS = Enabled MUSS der Konnektor alle erfolgreich durchlaufenen Außenoperationen protokollieren, in denen mit Schlüsselmaterial der gesteckten Karten kryptographische Operationen durchgeführt wurden. Dazu MUSS er TUC_KON_256{"LOG/CRYPTO_OP"; Sec; Info; „Operation=\$Operationsname;<für alle betroffenen Schlüssel:>Karte=\$ICCSN;Keyref=<Referenz auf den Schlüssel>; CARD_HANDLE=\$CardHandle; CardHolderName=\$CardHolderName“; no-Disp} aufrufen. ☒

In gematik_Pers_HBA.xds und und gematik_Pers_SMC-B.xds werden die Elemente HbaAntragExport bzw. SmcbAntragExport um die Abbildung von Erklärungen des Antragstellers erweitert. Aufgrund der Einführung des neuen Elementes "ErklaerungAntragsteller" muss die Versionsnummer des Schemas auf 1.2.0 erhöht werden.

1. Erweiterung der Übergabedatenstruktur des HBA

Das optionale Element *DatNutzTI* in HbaAntragExport wird ersetzt durch das Element *ErklaerungAntragsteller*, das mehrfach enthalten sein kann. Damit können sowohl Einzelerklärungen als auch Sammelerklärungen übertragen werden.

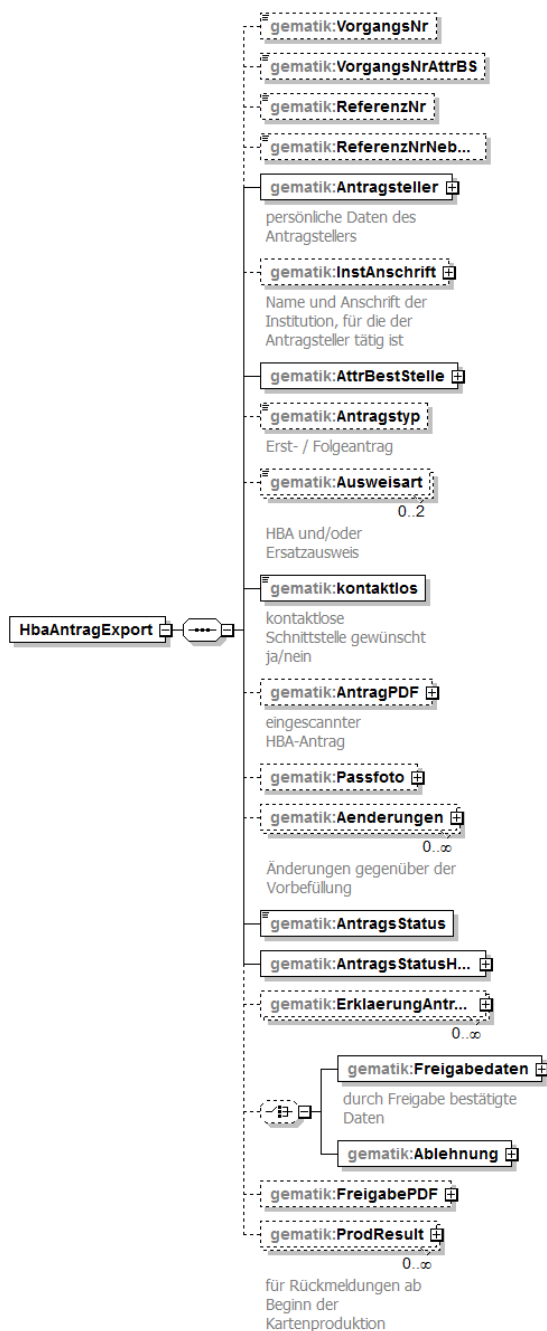


Abbildung 1: Struktur von HbaAntragExport

2. Erweiterung der Übergabedatenstruktur der SMC-B

Das optionale Element *DatNutzTI* in *SmcbAntragExport* wird ersetzt durch das Element *ErklärungAntragsteller*, das mehrfach vorhanden sein kann:

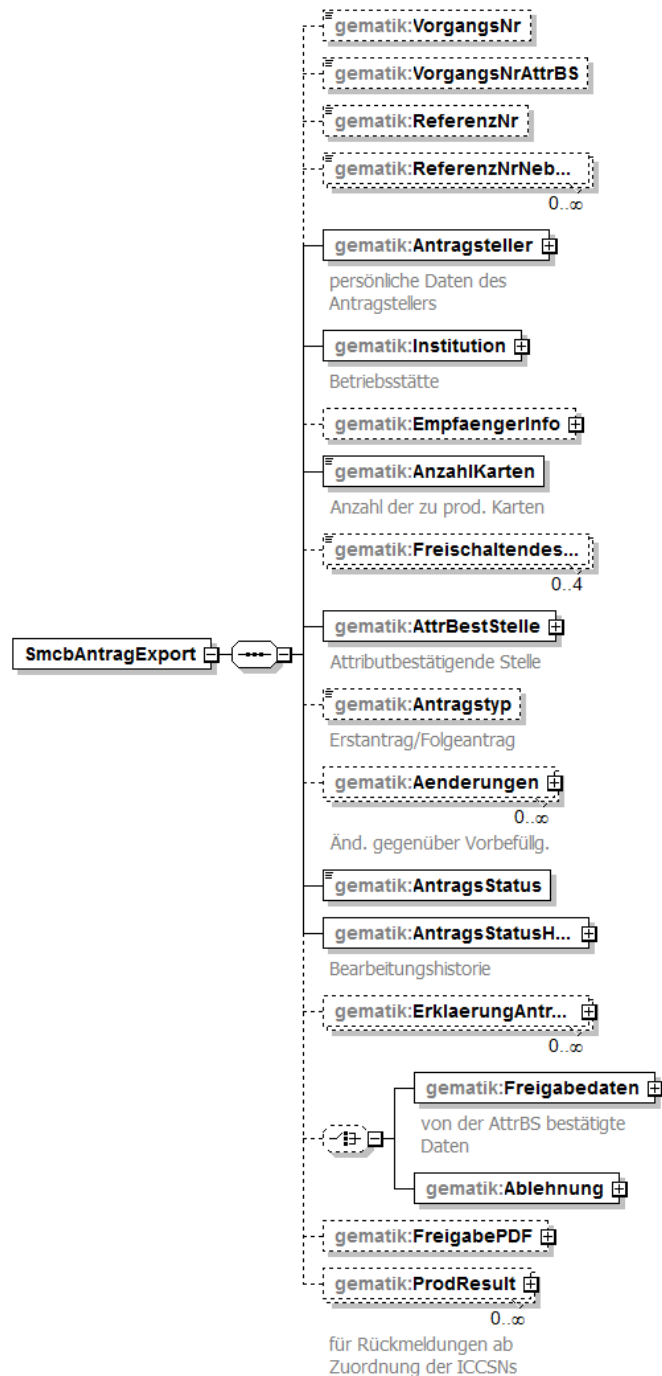


Abbildung 2: Struktur von **SmcbAntragExport**

3. Änderungen in den Datenstrukturen xxxAntragExport

Tabelle 7: Tab_SMC-B_Pers_002 Felder von SmcbAntragExport

bzw.

Tabelle 7: Tab_HBA_Pers_003 Felder von HbaAntragExport

Datenfeld	Element/ Attribut	P/ O	Feldtyp	Bemerkung
...
AntragsSta- tusHistorie	AntragsSta- tusHistorie	P	AntragsSta- tusHisto- ryType	Historie der Statusänderungen vor Verzwei- gung in einzelne Karten (darin aktueller Sta- tus redundant enthalten)
Mit Nutzung der Daten einverstanden	DatNutzTI	O	xs:boolean	<p>Mit diesem Datum teilt der TSP der AttrBS mit, ob der Antragsteller der Aufnahme seiner Zertifikate in ein Verzeichnis der Telematikinfrastruktur (TI) und der Verwendung seiner Daten zur Suche innerhalb der TI zugestimmt hat.</p> <p>Der Antragsteller kann schon jetzt zustimmen. Dies kann später von Anwendungen für z.B. eine vertrauliche Kommunikation oder für andere Dienste, die diese Zertifikate benötigen, genutzt werden. Die Zustimmung zur Aufnahme kann auch später noch abgefragt werden.</p> <p>Die Zustimmung nach Signaturgesetz zur Veröffentlichung der Zertifikate beim ZDA ist eine Sache zwischen Antragsteller und ZDA und wird nicht an die AttrBS übertragen.</p>
	ErklaerungAnt- klaerungAn- tragsteller	P	Erklaerun- genType	Erklärungen des Antragstellers
...

3.2 ErklarungType

Mit Elementen dieses Typs können die Erklärungen des Antragstellers zu Einzelaspekten oder summarische Erklärungen übertragen werden. Bspw. kann das Einverständnis mit der Nutzung der Daten in der TI, mit der Veröffentlichung der Zertifikate beim ZDA oder mit der Weitergabe der Daten an die Kammer erklärt werden.

Titel und Wortlaute der Erklärungen werden von den Sektoren vorgegeben.

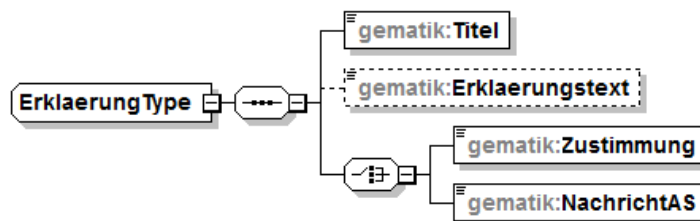


Abbildung 3: Struktur von ErklarungType

Tabelle 1: Felder von ErklarungType

Element/ Attribut	P/ O	Feldtyp	Bemerkung
Titel	P	xs:string	Name der Erklärung
Erklärungstext	O	xs:string	Wortlaut der Erklärung.
Zustimmung	P	xs:boolean	Willenserklärung des Antragstellers (Kenntnisnahme bzw. Zustimmung / Ablehnung); „true“, wenn ein Wert im Antrag gesetzt wurde, sonst „false“. (genau dann vorhanden, wenn NachrichtAS nicht enthalten ist)
NachrichtAS	P	xs:string	Vom Antragsteller eingegebener Text, z.B. Name der vorherigen Kammer (genau dann vorhanden, wenn Zustimmung nicht enthalten ist)

4. Änderungen an den XML-Schemata

Die obengenannten Änderungen werden in die Schemas eingearbeitet.

4.1 Das optionale Element *DatNutzTI* in *HbaAntragExport* bzw. *SmcbAntragExport* wird ersetzt durch das Element *ErklarungAntragsteller*, das mehrfach enthalten sein kann:

ALT:

```
<element name="DatNutzTI" type="boolean" minOccurs="0">
  <annotation>
    <documentation>Einverständnis mit Aufnahme der Zertifikate in Verzeichnis
    innerhalb der TI</documentation>
  </annotation>
</element>
```

NEU:

```
<element name="Erklarung" type="gematik:ErklarungType" minOccurs="0"
maxOccurs="unbounded"/>
```

4.2 In gematik_HBA_SMC-B_Typen.xsd wird die Definition von *ErklaerungType* hinzugefügt:

NEU:

```
<complexType name="ErklaerungType">  
  <sequence>  
    <element name="Titel" type="string"/>  
    <element name="Erklaerungstext" type="string" minOccurs="0"/>  
    <choice>  
      <element name="Zustimmung" type="boolean" default="false"/>  
      <element name="NachrichtAS" type="string"/>  
    </choice>  
  </sequence>  
</complexType>
```

Änderungen in gemProdT_SMC-B_PTV4.2.0

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_SMC-B_PTV4.2.0]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

**Tabelle 1: Anforderungen zur funktionalen Eignung
"Produkttest / Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	
Card-G2-A_2008	Formfaktor SMC-B	gemSpec_SMC_OPT
Card-G2-A_2010	Layout Vorderseite SMC-B, Ausweisnummer	gemSpec_SMC_OPT
Card-G2-A_2013	Ausrichtung Text-Regionen 1-3 SMC-B	gemSpec_SMC_OPT
Card-G2-A_2015	Schriftgröße ID-000 SMC-B	gemSpec_SMC_OPT
Card-G2-A_3035	Auswahl der Absicherung der Kartenadministration	gemSpec_SMC-B_ObjSys
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys
Card-G2-A_3353	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3355	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3356	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3357	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.GS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3358	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3359	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3361	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3363	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3367	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3368	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3369	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENG.R2048	gemSpec_SMC-B_ObjSys
	[...]	

Tabelle 2: Anforderungen zur funktionalen Eignung "Herstellereklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	
Card-G2-A_2008	Formfaktor SMC-B	gemSpec_SMC_OPT
Card-G2-A_2010	Layout Vorderseite SMC-B, Ausweisnummer	gemSpec_SMC_OPT
Card-G2-A_2013	Ausrichtung Text Regionen 1-3 SMC-B	gemSpec_SMC_OPT
Card-G2-A_2015	Schriftgröße ID-000 SMC-B	gemSpec_SMC_OPT
Card-G2-A_3035	Auswahl der Absicherung der Kartenadministration	gemSpec_SMC-B_ObjSys
Card-G2-A_3375	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_SMC-B_ObjSys
Card-G2-A_3353	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3355	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3356	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3357	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_SMC-B_ObjSys
Card-G2-A_3358	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3359	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3361	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_SMC-B_ObjSys
Card-G2-A_3363	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_SMC-B_ObjSys
Card-G2-A_3367	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3368	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048	gemSpec_SMC-B_ObjSys
Card-G2-A_3369	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048	gemSpec_SMC-B_ObjSys

Änderungen in gemProdT_HBA_PTV4.2.0

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_HBA_PTV4.2.0]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	
Card-G2-A_3005	Auswahl der Absicherung der Kartenadministration	gemSpec_HBA_ObjSys
Card-G2-A_3010	K_Initialisierung und K_Personalisierung: Kontakthlose Schnittstelle wird nicht genutzt	gemSpec_HBA_ObjSys
Card-G2-A_3277	K_Personalisierung und K_Initialisierung: Konformität kontakthlose Schnittstelle	gemSpec_HBA_ObjSys
Card-G2-A_3325	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_HBA_ObjSys
Card-G2-A_3287	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3288	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys
Card-G2-A_3289	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys
Card-G2-A_3290	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_HBA_ObjSys
Card-G2-A_3291	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_HBA_ObjSys
Card-G2-A_3292	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_HBA_ObjSys
Card-G2-A_3294	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_HBA_ObjSys
Card-G2-A_3296	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_HBA_ObjSys
Card-G2-A_3298	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3305	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3306	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3314	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048	gemSpec_HBA_ObjSys
Card-G2-A_2090	K_Initialisierung: Inhalt von EF.SSEC	gemSpec_HBA_ObjSys
	[...]	

Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellereklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	
Card-G2-A_3005	Auswahl der Absicherung der Kartenadministration	gemSpec_HBA_ObjSys
Card-G2-A_3010	K_Initialisierung und K_Personalisierung: Kontaktlose Schnittstelle wird nicht genutzt	gemSpec_HBA_ObjSys
Card-G2-A_3277	K_Personalisierung und K_Initialisierung: Konformität kontaktlose Schnittstelle	gemSpec_HBA_ObjSys
Card-G2-A_3325	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_HBA_ObjSys
Card-G2-A_3287	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3288	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys
Card-G2-A_3289	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys
Card-G2-A_3290	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_HBA_ObjSys
Card-G2-A_3291	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_HBA_ObjSys
Card-G2-A_3292	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_HBA_ObjSys
Card-G2-A_3294	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_HBA_ObjSys
Card-G2-A_3296	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_HBA_ObjSys
Card-G2-A_3298	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3305	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3306	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048	gemSpec_HBA_ObjSys
Card-G2-A_3314	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048	gemSpec_HBA_ObjSys
Card-G2-A_2090	K_Initialisierung: Inhalt von EF.SSEC	gemSpec_HBA_ObjSys
	[...]	

Das Kapitel [gemSpec_mobKT#5.2.2.1] „Identifikation des Kartentyps und der Version“ wird wie folgt angepasst:

...

☒ **TIP1-A_4957 Mobiles KT: Unterstützung Kartenversionen von eGK, HBA und SMC-B**

Der Mini-AK des Mobilten Kartenterminals MUSS die Versionen für [eGK], [HBA] und [SMC-B] unterstützen, wenn die Versionen des Betriebssystems und des Objektsystems der jeweiligen Karte dem Mini-AK bekannt sind. ☒

Die Kartenversion der Kartentypen eGK, HBA und SMC-B setzt sich aus der Version des Betriebssystems (COS) und der Objektsystemversion des jeweiligen Kartentyps zusammen. Im Rahmen der Prüfung auf Karten-Inkompatibilität gemäß [TIP1-A_3816] sind diese beiden Versionsnummern zu berücksichtigen.

Für die Generation 1 plus der eGK sind diese Informationen in [gemeGK_Fach] bzw. SRQ zu [gemeGK_Fach] zu finden.

Für die Karten-Generation 2 werden zum jeweiligen Release, in welchem der Produkttypsteckbrief des Mobilten Kartenterminals enthalten ist, die Versionen der zu unterstützenden Karten veröffentlicht.

~~Der fachanwendungsspezifische Teil der Versionierung ist also hier nicht zu betrachten. Der Ablageort und die konkreten Werte der Versionsnummern von Betriebssystem und Objektsystem der zu unterstützenden Karten finden sich in den Produkttypsteckbriefen der entsprechenden Karten. Für die Generation 1 plus der eGK sind diese Informationen in [gemeGK_Fach] bzw. SRQ zu [gemeGK_Fach] zu finden.~~

☒ **TIP1-A_3816 Mobiles KT: Karten-Inkompatibilität als Ergebnis der Kompatibilitätsprüfung**

Der Mini-AK des Mobilten Kartenterminals MUSS in einem ersten Schritt, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion kleiner als alle durch den Mini-AK zu unterstützenden Kartenversionen gemäß [TIP1-A_4957] ist oder die ermittelte Kartenversion nicht gemäß [TIP1-A_4957] bekannt und kleiner als die größte zu unterstützende Kartenversion ist, von einer inkompatiblen Karte ausgehen und die weitere Verarbeitung der Karte direkt abrechnen.

Der Mini-AK des Mobilten Kartenterminals MUSS in einem zweiten Schritt, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion größer als alle durch den Mini-AK zu unterstützenden Kartenversionen gemäß [TIP1-A_4957] ist, von einer kompatiblen Karte ausgehen und versuchen, diese zu verarbeiten.

~~Der Mini-AK des Mobilten Kartenterminals MUSS, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion zu keiner dem Mini-AK bekannten gemäß [TIP1-A_4957] kompatibel ist, von einer inkompatiblen Karte ausgehen und sicherstellen, dass diese Karte im Rahmen von Anwendungen nicht genutzt wird. ☒~~

Das bedeutet, dass der Mini-AK des Mobilten Kartenterminals zunächst unbekannte ältere Versionen (mindestens die Version des Betriebssystems oder die Objektsystemversion des jeweiligen Kartentyps ist kleiner als die zu unterstützenden Versionen) bzw. unbekannte Versionen, die aber kleiner als die größte ihm bekannte Version sind, als inkom-

patibel identifiziert und die Verarbeitung der zugehörigen Karte direkt mit einer Fehlermeldung gemäß [TIP1-A_4271] abbricht.

Der Mini-AK muss dann bei unbekanntem neueren Versionen (mindestens die Version des Betriebssystems oder die Objektsystemversion des jeweiligen Kartentyps ist größer als die zu unterstützten Versionen) von einer kompatiblen Karte ausgehen und versuchen, diese zu verarbeiten.

Das heißt, es liegt in diesem Fall immer eine Versionsverletzung vor.

☒ **TIP1-A_4271 Mobiles KT: Fehlermeldung Karten Inkompatibilität**

Der Mini-AK des Mobil Kartenterminals MUSS, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion zu keiner dem Mini-AK bekannten gemäß [TIP1-A_4957] kompatibel ist, eine geeignete Fehlermeldung auf dem erweiterten Display des Mobil Kartenterminals darstellen. ☒

...

Sachlage:

In [gemSpec_SMC_OPT] befassen sich zwei Anforderungen mit dem Aufdruck der Profilnummer auf der Vorderseite einer SMC-B. Card-G2-A_2012 besagt, dass in der Region 3 der Karte (d.i. rechts unten) das Wort „Profil“ und rechtsbündig darüber die Profilnummer des organisationsbezogenen Profils aufgedruckt werden (Profilnummer < 50) soll. Card-G2-A_2014 legt den Aufdruck für den ID-000-Bereich fest, wobei auch hier die Profilnummer höchstens zweistellig sein kann und numerisch sein muss.

Dies entspricht nicht der aktuellen Festlegung der Profilnummern in [gemSpec_PKI]. In den Tabellen Tab_PKI_918, Tab_PKI_919 und Tab_PKI_254 gibt es u.a. die Profile 2A und 2ZA, aber kein Profil 2.

Der Aufdruck auf der SMC-B ist an die aktuell definierten Profilbezeichnungen anzupassen. Anstelle des Begriffs „Profilnummer“ wird für die SMC-B der Begriff „Profilbezeichnung“ verwendet, da es sich nicht um eine rein numerische Angabe handelt.

Änderung 1:

Im Bereich 3 wird der Aufdruck erweitert:

Alt:

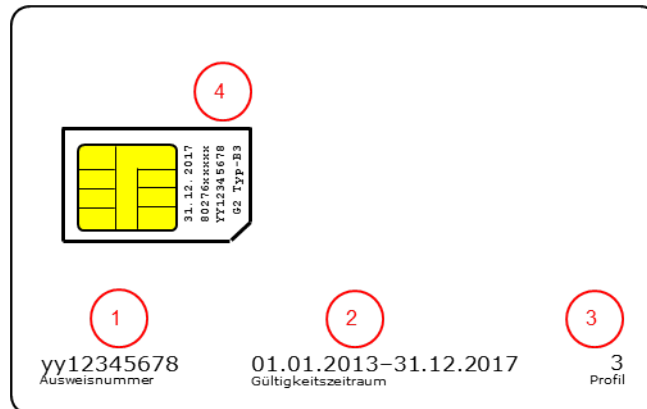


Abbildung 1: Abb_SMCOPT_02 – Gemeinsames Basis-Layout der SMC-B der Generation 2 mit Kennzeichnung der Kartenregionen

Neu:

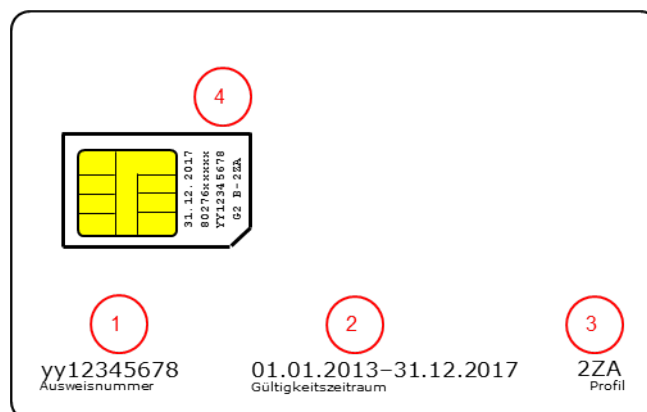


Abbildung 2: Abb_SMCOPT_02 – Gemeinsames Basis-Layout der SMC-B der Generation 2 mit Kennzeichnung der Kartenregionen

☒ Card-G2-A_2012 Layout Vorderseite SMC-B, Profil

Auf die Vorderseite der SMC-B MUSS gemäß Abbildung Abb_SMCOPT_02, Region 3, das Wort „Profil“ und rechtsbündig darüber die **Profilnummer** Profilbezeichnung des organisationsbezogenen Profils aufgedruckt werden (**Profilnummer < 50**). SMC-Bs, die keinem Profil zugeordnet werden und damit keine Rechte zum Zugriff auf die eGK besitzen, MÜSSEN anstelle der Profilnummer den Aufdruck „-“ erhalten.

Die Profilbezeichnung ist die auf den Text „CHA.“ folgende Zeichenkette in der Spalte Zugriffsprofil der Tabelle „Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung“.

☒

Änderung 2:

Im Bereich 4 (ID-000-Bereich) ist der Druckbereich eng begrenzt. Die Struktur des Aufdrucks wird so geändert, dass auch bei dreistelligen Profilnummern nicht mehr als 10 Zeichen gedruckt werden müssen.

☒ **Card-G2-A_2014 Layout Vorderseite SMC-B, ID-000-Bereich**

Rechts vom Chip MÜSSEN gemäß Abbildung Abb_SMCOPT_02, Region 4, folgende Werte rechtsbündig und um 90° nach links gedreht auf den ID-000-Bereich der SMC-B aufgedruckt werden:

- ...
- Generation, Kartentyp und Profilnummer
In der vierten Zeile stehen die Generation, der Kartentyp und das Profil. Dabei gilt folgender Aufbau:
 - Ein „G“ gefolgt von der Generationsnummer 2
 - Ein Leerzeichen
 - ~~Das Wort „Typ“~~
 - ~~Ein Bindestrich (sollte die Profilnummer zweistellig sein, kann der Bindestrich entfallen)~~
 - Die Kennzeichnung des Kartentyps: B
 - Ein Bindestrich
 - Die Profilnummer des personen- bzw. organisationsbezogenen Profils. Als Profilbezeichnung ist die auf den Text „CHA.“ folgende Zeichenkette in der Spalte Zugriffsprofil der Tab_PKI_254 zu verwenden. ☒

Beispiel:

alt: G2 Typ-B2

neu: G2 B-2A, G2 B-2ZA