

Einführung der Gesundheitskarte

Spezifikation der gSMC-K Objektsystem

Version: 3.10.0
Revision: \main\rel_online\rel_ors1\rel_opb1\26
Stand: 28.10.2016
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: [gemSpec_gSMC-K_ObjSys]

Dokumentinformationen

Änderung zur Vorversion

Überarbeitung der Dokumente für den Online-Produktivbetrieb (Stufe 1), als Grundlage für Produktivzulassungen und den bundesweiten Rollout.

Dokumentenhistorie

Version	Stand	Kap./Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.9.18	06.06.12		zur Abstimmung freigegeben	gematik
3.0.0	24.08.12		Einfügen von EF.EnvironmentalSettings	gematik
3.1.0	17.01.13		Harmonisierung mit der Struktur der anderen ObjSys-Spezifikationen	gematik
3.2.0 RC	23.10.13		redaktionelle Korrekturen, Fehlerkorrekturen, AFO zu <i>persistenPublicKeyList</i> hinzugefügt, Attribut shareable wurde für alle Ordner und Dateien hinzugefügt, Ändern der Flaglist-Darstellung, Fehlerkorrekturen gemäß Kommentaren	gematik
3.3.0 RC	19.12.13		Zuordnung der AFOs zu Initialisierung und Personalisierung, Überarbeitung der Struktur, Einfügen von EF.KeyInfo, Modifizieren von EF.ATR, EF.DIR und EF.Version, Modifizieren von EF.GDO, Kommentare wurden eingearbeitet	gematik
3.4.0	21.02.14		Einfügen einer Liste offener Punkte, Änderungen aus Kommentarliste TSI, Expiration Date für Sicherheitsanker festgelegt, Kommentare Iteration 2b	gematik
3.5.0	27.03.14		Einarbeitung Fehlerkorrektur Iteration 2b	gematik
3.6.0	06.06.14		Einarbeitung Änderungen Iteration 3	gematik
3.7.0	26.08.14		Einarbeitung weitere Änderungen Iteration 3, Einfügen Schlüssel und Zertifikate für CVC-Admin, Einfügen Option_Erweiterung_herstellerspezifische_Schlüssel_01	gematik
3.8.0	17.07.15		Folgende Errata eingearbeitet: R.1.4.1, R1.4.2, R1.4.3, R1.4.5	Technik / SPE
3.9.0	24.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Einarbeitung Änderungsliste	
3.10.0	28.10.16		freigegeben	gematik

Inhaltsverzeichnis

Änderung zur Vorversion	2
Dokumentenhistorie.....	2
Inhaltsverzeichnis	4
1 Einordnung des Dokumentes	8
1.1 Zielsetzung.....	8
1.2 Zielgruppe	8
1.3 Geltungsbereich	8
1.4 Abgrenzung des Dokuments	9
1.5 Methodik.....	9
1.5.1 Nomenklatur	9
1.5.2 Verwendung von Schlüsselworten.....	11
1.5.3 Komponentenspezifische Anforderungen	11
2 Optionen.....	12
2.1 Option_Erstellung_von_Testkarten.....	12
2.2 Option_Erweiterung_herstellerspezifische_Schlüssel_01	12
3 Lebenszyklus von Karte und Applikation.....	13
4 Anwendungsübergreifende Festlegungen	14
4.1 Mindestanzahl logischer Kanäle.....	14
4.2 Kryptobox.....	14
4.3 Optionale Funktionspakete.....	14
4.3.1 Kontaktlose Schnittstelle.....	14
4.3.2 USB-Schnittstelle (optional)	14
4.4 Attributstabellen	15
4.4.1 Attribute eines Ordners.....	15
4.4.2 Attribute einer Datei (EF)	16
4.5 Zugriffsregeln für besondere Kommandos.....	16
4.6 TransportStatus für Passwortobjekte	16
4.7 Attributswerte und Personalisierung	16
4.8 Kartenadministration.....	17
5 Dateisystem der gSMC-K	19

5.1	Attribute des Objektsystems	19
5.1.1	ATR-Kodierung und technische Eigenschaften ATR-Kodierung	20
5.2	Allgemeine Struktur.....	21
5.3	Root-Anwendung und Dateien auf MF-Ebene	22
5.3.1	MF	22
5.3.2	MF / EF.ATR	23
5.3.3	MF / EF.DIR	24
5.3.4	MF / EF.EnvironmentSettings	25
5.3.5	MF / EF.GDO	27
5.3.6	MF / EF.KeyInfo.....	28
5.3.7	MF / EF.Version2.....	29
5.3.8	MF / EF.C.CA_SAK.CS.E256	30
5.3.9	MF / EF.C.CA_SAK.CS.E384	32
5.3.10	MF / EF.PuK.RCA.CS.R2048	32
5.3.11	MF / EF.C.RCA.CS.E256.....	34
5.3.12	MF / EF.C.SMC.AUT_CVC.E256.....	35
5.3.13	MF / EF.C.SMC.AUT_CVC.E384	37
5.3.14	MF / PIN.AK.....	38
5.3.15	MF / PIN.NK	39
5.3.16	MF / PIN.Pers	41
5.3.17	MF / PIN.SAK	43
5.3.18	MF / PrK.SMC.AUT_CVC.E256.....	44
5.3.19	MF / PrK.SMC.AUT_CVC.E384	46
5.3.20	Herstellerspezifische Schlüssel.....	47
5.3.20.1	MF / PrK.KONN.AUT.R2048.....	47
5.3.20.2	MF / PrK.KONN.AUT2.R2048	49
5.3.20.3	MF / PrK.KONN.AUT.R3072	50
5.3.20.4	MF / PrK.KONN.AUT.E256	51
5.3.20.5	MF / PrK.KONN.AUT.E384	51
5.3.20.6	MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	52
5.3.20.7	MF / PrK.KONN.ENC2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	54
5.3.20.8	MF / PrK.KONN.ENC.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	55
5.3.20.9	MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	56
5.3.20.10	MF / PrK.KONN.TLS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	57
5.3.20.11	MF / PrK.KONN.TLS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	58
5.3.20.12	MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	59
5.3.20.13	MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	61
5.3.20.14	MF / PrK.SDS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	62
5.3.20.15	MF / PrK.SDS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	63
5.3.20.16	MF / PrK.GP.R2048	64

5.3.20.17	MF / PuK.GP.R2048	65
5.3.20.18	MF / PrK.GP2.R2048	66
5.3.20.19	MF / PrK.GP.R3072	67
5.3.20.20	MF / PrK.GP.E256	68
5.3.20.21	MF / PrK.GP.E384	68
5.3.21	Sicherheitsanker zum Import von CV-Zertifikaten	69
5.3.21.1	MF / PuK.RCA.CS.E256	69
5.3.22	Asymmetrische Kartenadministration	71
5.3.22.1	MF / PuK.RCA.ADMINCMS.CS.E256	72
5.3.23	Symmetrische Kartenadministration	73
5.3.23.1	MF / SK.CMS.AES128	74
5.3.23.2	MF / SK.CMS.AES256	75
5.3.23.3	MF / SK.CUP.AES128	76
5.3.23.4	MF / SK.CUP.AES256	77
5.4	MF / DF.AK	78
5.4.1	MF /DF.AK/ EF.C.AK.AUT.R2048	80
5.4.2	MF / DF.AK / PrK.AK.AUT.R2048	81
5.4.3	MF /DF.AK/ EF.C.AK.AUT2.XXXX	83
5.4.4	MF / DF.AK / PrK.AK.AUT2.R2048	84
5.4.5	MF / DF.AK / PrK.AK.AUT.R3072	85
5.4.6	MF / DF.AK / PrK.AK.AUT.E256	86
5.4.7	MF / DF.AK / PrK.AK.AUT.E384	87
5.4.8	MF / DF.AK / PrK.AK.CA_PS.R2048	87
5.4.9	MF / DF.AK / PrK.AK.CA_PS2.R2048	89
5.4.10	MF / DF.AK / PrK.AK.CA_PS.R3072	89
5.4.11	MF / DF.AK / PrK.AK.CA_PS.E256	90
5.4.12	MF / DF.AK / PrK.AK.CA_PS.E384	91
5.5	MF / DF.NK	92
5.5.1	MF / DF.NK / EF.ActKey	93
5.5.2	MF / DF.NK / EF.CardInfo	94
5.5.3	MF / DF.NK / EF.CFSMACKKey	95
5.5.4	MF / DF.NK / EF.ConfigUser	96
5.5.5	MF /DF.NK/ EF.C.NK.VPN.R2048	97
5.5.6	MF / DF.NK / PrK.NK.VPN.R2048	98
5.5.7	MF /DF.NK/ EF.C.NK.VPN2.XXXX	100
5.5.8	MF / DF.NK / PrK.NK.VPN2.R2048	101
5.5.9	MF / DF.NK / PrK.NK.VPN.R3072	101
5.5.10	MF / DF.NK / PrK.NK.VPN.E256	102
5.5.11	MF / DF.NK / PrK.NK.VPN.E384	103
5.5.12	MF / DF.NK / PrK.CFS.R2048	103
5.5.13	MF / DF.NK / PuK.CFS.R2048	105
5.5.14	MF / DF.NK / PrK.CFS2.R2048	106
5.5.15	MF / DF.NK / PrK.CFS.R3072	107
5.5.16	MF / DF.NK / PrK.CFS.E256	108
5.5.17	MF / DF.NK / PrK.CFS.E384	108
5.6	MF / DF.SAK	109
5.6.1	MF / DF.SAK / EF.C.SAK.AUT.R2048	111
5.6.2	MF / DF.SAK / PrK.SAK.AUT.R2048	112
5.6.3	MF / DF.SAK / EF.C.SAK.AUT2.XXXX	114

5.6.4	MF / DF.SAK / PrK.SAK.AUT2.R2048	115
5.6.5	MF / DF.SAK / PrK.SAK.AUT.R3072	116
5.6.6	MF / DF.SAK / PrK.SAK.AUT.E256	116
5.6.7	MF / DF.SAK / PrK.SAK.AUT.E384	117
5.6.8	MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	118
5.6.9	MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	119
5.6.10	MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384	121
5.6.11	MF / DF.SAK / PrK.SAK.AUTD_CVC.E384	121
5.6.12	MF / DF.SAK / PrK.SAK.CA_xTV.R2048	122
5.6.13	MF / DF.SAK / PrK.SAK.CA_xTV2.R2048	123
5.6.14	MF / DF.SAK / PrK.SAK.CA_xTV.R3072	124
5.6.15	MF / DF.SAK / PrK.SAK.CA_xTV.E256	125
5.6.16	MF / DF.SAK / PrK.SAK.CA_xTV.E384	126
5.6.17	MF / DF.SAK / PrK.SAK.SIG.R2048	126
5.6.18	MF / DF.SAK / PrK.SAK.SIG2.R2048	128
5.6.19	MF / DF.SAK / PrK.SAK.SIG.R3072	128
5.6.20	MF / DF.SAK / PrK.SAK.SIG.E256	129
5.6.21	MF / DF.SAK / PrK.SAK.SIG.E384	130
5.7	MF / DF.Sicherheitsanker	131
5.7.1	MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA.....	132
5.7.2	MF / DF.Sicherheitsanker / EF.C.TSL.CA_1	133
5.7.3	MF / DF.Sicherheitsanker / EF.C.TSL.CA_2.....	135
5.7.4	MF/DF.Sicherheitsanker / PIN.BNetzA_RCA.....	136
5.7.5	MF/DF.Sicherheitsanker / PIN.TSL_CA.....	138
5.8	Zusätzliche Applikationen und Dateien	139
5.9	EF.GeneralPurpose (kann nach Ausgabe der gSMC-K nachgeladen werden)	140
5.10	Laden einer neuen Anwendung oder Anlegen eines EFs oder Sperren von Schlüsseln nach Ausgabe der gSMC-K.....	141
Anhang A	- Verzeichnisse	142
A1	- Abkürzungen.....	142
A2	- Glossar	142
A3	- Abbildungsverzeichnis.....	143
A4	- Tabellenverzeichnis.....	143
A5	- Referenzierte Dokumente.....	149
A5.1	- Dokumente der gematik.....	149
A5.2	- Weitere Dokumente	149

1 Einordnung des Dokumentes

1.1 Zielsetzung

Dieses Dokument beschreibt die Kartenschnittstelle der gerätespezifischen Security Module Card Typ K (gSMC-K) zum Einsatz in Konnektoren.

Die Spezifikation beinhaltet Anwendungen der gSMC-K unter den folgenden, rein kartenorientierten Gesichtspunkten:

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

Somit definiert dieses Dokument eine Reihe von Datencontainern, Schlüsselobjekten und Passwörtern. Zudem werden hier die Sicherheitsmechanismen für diese Objekte festgelegt, d. h. es wird festgelegt, welchen Instanzen es unter welchen Voraussetzungen möglich ist, auf Inhalte der Container zuzugreifen, Operationen mit den Schlüsselobjekten durchzuführen etc. Die Semantik und die Syntax der Inhalte in den Datencontainern ist dagegen nicht Gegenstand dieses Dokumentes.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von Chipkartenbetriebssystemen und an Anwendungsprogrammierer, die unmittelbar mit der gSMC-K kommunizieren, wie etwa Softwareentwickler für Konnektoren.

Zudem richtet es sich an die Produzenten einer gSMC-K, welche die gSMC-K konfigurieren und personalisieren.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Der Inhalt des Dokumentes ist verbindlich für die Erstellung von chipkartenbasierten Sicherheitsmodulen gSMC-K, die in Konnektoren zur Anwendung kommen.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der

Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung des Dokuments

Das Dokument [gemSpec_COS] beschreibt die Funktionalität eines eGK/HBA/SMC-Betriebssystems, ohne konkret eine Konfiguration zu nennen. Dieses Dokument beschreibt die Dateistruktur einer gSMC-K und setzt dabei die in [gemSpec_COS] spezifizierte Funktionalität voraus. Welchem Zweck die hier aufgeführten Dateien, Schlüssel und Passwörter dienen, ist nicht Gegenstand dieses Dokumentes.

Die äußere Gestaltung einer gSMC-K ist in [gemSpec_SMC_OPT] festgelegt.

1.5 Methodik

1.5.1 Nomenklatur

Dieses Dokument verwendet dieselbe Nomenklatur wie [gemSpec_COS].

'1D'	Hexadezimale Zahlen und Oktettstrings werden in Hochkommata eingeschlossen.
x y	Das Symbol steht für die Konkatenierung von Oktettstrings oder Bitstrings: '1234' '5678' = '12345678'.

- In [gemSpec_COS] wurde ein objektorientierter Ansatz für die Beschreibung der Funktionalität des Betriebssystems gewählt. Deshalb wurde dort der Begriff "Passwortobjekt" verwendet, wenn Instanzen für eine Benutzerverifikation besprochen wurden. Da in diesem Dokument lediglich numerische Ziffernfolgen als Verifikationsdaten eines Benutzers verwendet werden, wird hier statt Passwortobjekt vielfach der Begriff PIN gewählt, wenn keine Gefahr besteht, dass es zu Verwechslungen kommt zwischen den Verifikationsdaten und der Instanz des Objektes, in denen sie enthalten sind (zur Erinnerung: Ein Passwortobjekt enthält neben den Verifikationsdaten auch einen Identifier, eine Zugriffsregel, eine PUK, ...).

Bei Referenzierungen wird durch die Zusatzangabe „#Nummer“ auf ein spezifisches Kapitel oder eine Festlegung in dem referenzierten Dokument Bezug genommen.

Der Begriff "Wildcard" wird in diesem Dokument im Sinn eines "beliebigen, herstellerspezifischen Wertes, der nicht anderen Vorgaben widerspricht" verwendet.

Für die Authentisierung der Zugriffe durch ein CMS auf die dafür vorgesehenen Objekte können entweder symmetrische Verfahren mit AES-Schlüsseln oder alternativ asymmetrische Verfahren mit CV-Zertifikaten verwendet werden. Für beide Verfahren sind die Schlüsselobjekte in dieser Spezifikation spezifiziert.

Die in diesem Dokument referenzierten Flaglisten `cvc_FlagList_CMS` und `cvc_FlagList_TI` sind normativ in [gemSpec_PKI#6.7.5] und die dazugehörigen OIDs `oid_cvc_fl_cms` und `oid_cvc_fl_ti` sind normativ in [gemSpec_OID] definiert.

Gemäß [gemSpec_COS#(N022.400)] wird die Notwendigkeit einer externen Rollenauthentisierung für Karten der Generation 2 mit einer Flaglist wie folgt dargestellt: `AUT(OID, FlagList)` wobei `OID` stets aus der Menge `{oid_cvc_fl_cms, oid_cvc_fl_ti}` ist und `FlagList` ein sieben Oktett langer String, in welchem im Rahmen dieses Dokumentes genau ein Bit gesetzt ist. Abkürzend wird deshalb in diesem Dokument lediglich die Nummer des gesetzten Bits angegeben in Verbindung mit der `OID`. Ein gesetztes Bit `i` in Verbindung mit der `oid_cvc_fl_cms` wird im Folgenden mit `flagCMS.i` angegeben und ein gesetztes Bit `j` in Verbindung mit der `oid_cvc_fl_ti` wird im Folgenden mit `flagTI.j` angegeben.

Beispiele:

Langform	Kurzform
Informativ: <code>AUT(CHA.1)</code>	<code>C.1</code>
Informativ: <code>AUT(CHA.7)</code>	<code>C.7</code>
Informativ: <code>AUT(CHA.2) OR AUT(CHA.3)</code>	<code>C.2.3</code>
Informativ: <code>PWD(PIN) AND [AUT(CHA.2) OR AUT(CHA.3)]</code>	<code>PWD(PIN) AND [C.2.3]</code>
<code>AUT(oid_cvc_fl_cms, '00010000000000')</code>	<code>flagCMS.15</code>
<code>AUT(oid_cvc_fl_ti, '00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')</code>	<code>flagTI.15 OR flagTI.16</code>
<code>PWD(PIN) AND [AUT(oid_cvc_fl_cms, '00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')]</code>	<code>PWD(PIN) AND [flagCMS.15 OR flagTI.16]</code>
<code>SmMac(oid_cvc_fl_cms, '00800000000000')</code>	<code>SmMac(flagCMS.08)</code>

Um die Zugriffsregeln für administrative Zugriffe in den einzelnen Tabellen übersichtlich darstellen zu können, werden folgende Abkürzungen verwendet:

<code>AUT_CMS</code>	OR OR AND AND	{ <code>SmMac(SK.CMS.AES128)</code> (<code>SK.CMS.AES256</code>) <code>SmMac(flagCMS.08)</code> } <code>SmCmdEnc</code> <code>SmRspEnc</code>
<code>AUT_CUP</code>	OR OR AND AND	{ <code>SmMac(SK.CUP.AES128)</code> <code>SmMac(SK.CUP.AES256)</code> } <code>SmMac(flagCMS.10)</code> } <code>SmCmdEnc</code> <code>SmRspEnc</code>

In der obigen Tabelle, wie auch an anderen Stellen im Dokument werden aus Gründen der besseren Lesbarkeit häufig mehrere Zugriffsarten zusammengefasst und dafür eine Zugriffsbedingung angegeben. Beispielsweise (`READ, UPDATE`) nur, wenn `SmMac(CAN) AND SmCmdEnc AND SmRspEnc`. Dabei ist folgendes zu beachten:

Dabei ist folgendes zu beachten:

- Für Kommandonachrichten ohne Kommandodaten ist der Term `SmCmdEnc` sinnlos.

- b. Für Antwortnachrichten ohne Antwortdaten ist der Term SmRspEnc sinnlos.
- c. Die Spezifikation ist wie folgt zu interpretieren:
 - 1. Falls eine Kommandonachricht keine Kommandodaten enthält, dann ist es zulässig den Term SmCmdEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
 - 2. Falls eine Antwortnachricht keine Antwortdaten enthält, dann ist es zulässig den Term SmRspEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
- d. Für die Konformitätsprüfung eines Prüflings gilt bei der Beurteilung von Zugriffsbedingungen:
 - 1. Falls für eine Zugriffsart keine Kommandodaten existieren, dann ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmCmdEnc zu verwenden.
 - 2. Falls für eine Zugriffsart keine Antwortdaten existieren, dann ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmRspEnc zu verwenden.

1.5.2 Verwendung von Schlüsselworten

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

☒ **Card-G2-A_0000 <Titel der Afo>**

Text / Beschreibung☒

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

1.5.3 Komponentenspezifische Anforderungen

Da es sich beim vorliegenden Dokument um die Spezifikation einer Schnittstelle zwischen mehreren Komponenten handelt, ist es möglich, die Anforderungen aus der Sichtweise jeder der Komponenten zu betrachten. Die normativen Abschnitte tragen deshalb eine Kennzeichnung, aus wessen Sichtweise die Anforderung primär betrachtet wird.

Tabelle 1: Tab_gSMC-K_ObjSys_001 Liste der Komponenten, aus deren Sicht Anforderungen betrachtet werden

Komponente	Beschreibung
K_Initialisierung	Instanz, welche eine Chipkarte im Rahmen der Initialisierung befüllt
K_Personalisierung	Instanz, welche eine Chipkarte im Rahmen der Produktion individualisiert
K_COS	Betriebssystem einer Smartcard
K_externe Welt	Instanz, die außerhalb der Karte liegt

2 Optionen

Dieses Unterkapitel listet Funktionspakete auf, die für eine Zulassung einer gSMC-K der Generation 2 nicht zwingend erforderlich sind.

2.1 Option_Erstellung_von_Testkarten

☒ **Card-G2-A_3250 K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten**

Die gSMC-K KANN als Testkarte ausgestaltet werden. Soweit in dieser Spezifikation Anforderungen an Testkarten von den Anforderungen an Produktivkarten abweichen, wird dies an der entsprechenden Stelle aufgeführt. ☒

2.2 Option_Erweiterung_herstellerspezifische_Schlüssel_01

Zur sicheren Nutzung des Konnektors benötigen bestimmte Hersteller zusätzliche Schlüsselobjekte auf der gSMC-K, die im MF gespeichert werden sollen.

☒ **Card-G2-A_3336 K_Initialisierung und K_Personalisierung: Vorgaben für die Option_Erweiterung_herstellerspezifische_Schlüssel_01**

Falls eine gSMC-K die Option_Erweiterung_herstellerspezifische_Schlüssel_01

1. unterstützt, dann MÜSSEN zusätzlich zu allen nicht gekennzeichneten Anforderungen auch alle Anforderungen erfüllt werden, die mit Option_Erweiterung_herstellerspezifische_Schlüssel_01 gekennzeichnet sind.
2. nicht unterstützt, dann DÜRFEN mit Option_Erweiterung_herstellerspezifische_Schlüssel_01 gekennzeichnete Anforderungen NICHT relevant für funktionale Tests sein. ☒

3 Lebenszyklus von Karte und Applikation

Diese Spezifikation gilt nicht für die Vorbereitungsphase von Applikationen oder deren Bestandteile. Sie beschreibt lediglich den Zustand des Objektsystems in der Nutzungsphase.

Die Nutzungsphase einer Applikation oder eines Applikationsbestandteils beginnt, sobald sich ein derartiges Objekt, wie in der Spezifikation der Anwendung definiert, verwenden lässt. Die Nutzungsphase einer Applikation oder eines Applikationsbestandteils endet, wenn das entsprechende Objekt gelöscht oder terminiert wird.

Hinweis (1) Die in diesem Kapitel verwendeten Begriff Vorbereitungsphase und Nutzungsphase werden in [gemSpec_COS#4] definiert.

4 Anwendungsübergreifende Festlegungen

Zur Umsetzung dieses Kartentyps ist ein Betriebssystem hinreichend, welches folgende Optionen enthält:

- Unterstützung von mindestens vier logischen Kanälen.
- Unterstützung der Kryptoboxfunktionalität.

4.1 Mindestanzahl logischer Kanäle

☒ **Card-G2-A_2538 K_Initialisierung: Anzahl logischer Kanäle**

Für die Anzahl logischer Kanäle, die von einer gSMC-K zu unterstützen ist, gilt:

- a) Die maximale Anzahl logischer Kanäle MUSS gemäß [ISO7816-4#Tab.88] in den Historical Bytes in EF.ATR angezeigt werden.
- b) Die gSMC-K MUSS mindestens vier logische Kanäle unterstützen. Das bedeutet, die in den Bits b3b2b1 gemäß [ISO7816-4#Tab.88] kodierte Zahl MUSS mindestens '011' = 3 oder größer sein. ☒

4.2 Kryptobox

☒ **Card-G2-A_2873 K_gSMC-K: Kryptobox**

Für das Objektsystem der gSMC-K MUSS ein COS verwendet werden, das die Kryptobox implementiert hat. ☒

4.3 Optionale Funktionspakete

4.3.1 Kontaktlose Schnittstelle

☒ **Card-G2-A_3040 K_Terminal: Ausschluss kontaktlose Schnittstelle**

Die in der Spezifikation [gemSpec_COS#11.2] zusätzlich zur kontaktbehafteten Schnittstelle gemäß [gemSpec_COS#11.2.1] als optional definierte Schnittstelle zur kontaktlosen Datenübertragung gemäß ISO/IEC 14443 (siehe [gemSpec_COS#11.2.3]) DARF für die gSMC-K NICHT genutzt werden. ☒

4.3.2 USB-Schnittstelle (optional)

☒ **Card-G2-A_2995 K_gSMC-K: USB-Schnittstelle**

Falls eine gSMC-K die Option_USB_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_USB_Schnittstelle implementiert hat. ☒

☒ **Card-G2-A_2996 K_gSMC-K: Vorhandensein einer USB-Schnittstelle**

Falls eine gSMC-K die Option_USB_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,

- a) das die Option_USB_Schnittstelle implementiert hat.
- b) das die Option_USB_Schnittstelle nicht implementiert hat. ☒

4.4 Attributstabellen

☒ **Card-G2-A_2532 K_Initialisierung: Änderung von Zugriffsregeln**

Die in diesem Dokument definierten Zugriffsregeln DÜRFEN in der Nutzungsphase NICHT veränderbar sein. ☒

Dieses Dokument legt das Verhalten aller Objekte im Security Environment SE#1 normativ fest. Das Verhalten in Security Environments mit einer anderen Nummer als SE#1 wird durch dieses Dokument nicht festgelegt.

Alle Angaben zu Objekten (Ordern, Dateien, Passworten und Schlüsseln) in diesem Dokument beziehen sich ausschließlich auf das Security Environment SE#1.

☒ **Card-G2-A_2533 K_Initialisierung: Verwendung von SE#1**

Alle Objekte MÜSSEN sich in SE#1 wie angegeben verwenden lassen. ☒

☒ **Card-G2-A_3192 K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs**

Jedes Objekt KANN in SE verwendbar sein, die verschieden sind von SE#1. ☒

☒ **Card-G2-A_3193 K_Initialisierung: Eigenschaften der Objekte in anderen SEs**

Falls ein Objekt in einem von SE#1 verschiedenen SE verwendbar ist, dann MUSS es dort dieselben Eigenschaften wie in SE#1 besitzen. ☒

4.4.1 Attribute eines Ordners

☒ **Card-G2-A_2535 K_Initialisierung: Ordnerattribute**

Enthält eine Tabelle mit Ordnerattributen

- a) keinen applicationIdentifier (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.
- b) einen oder mehrere AID, dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
- c) keinen fileIdentifier (FID),
 - 1. so DARF dieser Ordner sich NICHT mittels eines *fileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.1] selektieren lassen, es sei denn es handelt sich um den Ordner *root*, dessen optionaler *fileIdentifier* den Wert '3F00' besitzen MUSS.

2. so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden. ☒

4.4.2 Attribute einer Datei (EF)

☒ **Card-G2-A_2536 K_Initialisierung: Dateiattribute**

Enthält eine Tabelle mit Attributen einer Datei keinen *shortFileIdentifier*, so DARF sich dieses EF NICHT mittels *shortFileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.2] selektieren lassen. ☒

☒ **Card-G2-A_2665 K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“**

Für transparente EFs MUSS der Wert von „positionLogicalEndOfFile“, soweit nicht anders spezifiziert, auf die Anzahl der tatsächlich belegten Bytes gesetzt werden. ☒

4.5 Zugriffsregeln für besondere Kommandos

Gemäß [gemSpec_COS] gilt:

☒ **Card-G2-A_2537 K_Initialisierung: Zugriffsregeln für besondere Kommandos**

Die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT MUSS stets ALWAYS sein, unabhängig vom *lifeCycleStatus* und unabhängig vom aktuellen Security Environment. ☒

4.6 TransportStatus für Passwortobjekte

☒ **Card-G2-A_3201 K_Personalisierung und K_Initialisierung: Zuordnung zu transportStatus für die Passwortobjekte der gSMC-K**

Die Attribute transportStatus für alle Passwortobjekte dieser Karte (PIN.AK, PIN.NK, PIN.Pers, PIN.SAK, PIN.BNetzA_RCA, PIN.TSL_CA) MÜSSEN für eine konkrete Karte denselben Wert aufweisen. Der Wert MUSS aus der Menge {regularPassword, Leer-PIN, Transport-PIN} gewählt werden. ☒

4.7 Attributwerte und Personalisierung

Die in diesem Dokument festgelegten Attribute der Objekte berücksichtigen lediglich fachlich motivierte Use Cases. Zum Zwecke der Personalisierung ist es unter Umständen und je nach Personalisierungsstrategie erforderlich, von den in diesem Dokument festgelegten Attributwerten abzuweichen.

Beispielsweise ist es denkbar, dass für die Datei EF.GDO das Attribut *lifeCycleStatus* nach der Initialisierung auf dem in [gemSpec_COS] nicht normativ geforderten Wert „Initialize“ steht und für diesen Wert die Zugriffsregeln etwa ein Update Binary Kommando erlauben. In diesem Fall wiche nicht nur der Wert des Attributes *lifeCycleStatus*, sondern

auch der des Attributes `interfaceDependentAccessRules` von den Vorgaben dieses Dokumentes ab. Nach Abschluss der Personalisierung wäre dann der Wert des Attributes `lifeCycleStatus` bei korrekter Personalisierung spezifikationskonform auf dem Wert „Operational state (activated)“ aber in `interfaceDependentAccessRules` fände sich für den Zustand „Initialize“ immer noch „Update Binary“. Im Rahmen einer Sicherheitsbetrachtung wäre diese Abweichung als unkritisch einzustufen, wenn sichergestellt ist, dass der Zustand „Initialize“ unerreichbar ist.

Denkbar wäre auch, dass die Personalisierung so genannte Ini-Tabellen und spezielle Personalisierungskommandos nutzt, die Daten, die mit dem Kommando übergeben werden, an durch die Ini-Tabelle vorgegebene Speicherplätze schreibt. In dieser Variante wären die Attribute von EF.GDO auf den ersten Blick konform zu dieser Spezifikation, obwohl durch das Personalisierungskommando ein Zugriff auf das Attribut `body` bestünde, der so eventuell nicht in den Zugriffsregeln sichtbar wird und damit gegen die allgemeine Festlegung „andere (Kommandos) NEVER“ verstieße. Im Rahmen einer Sicherheitsbetrachtung wäre diese Abweichung als unkritisch einzustufen, wenn sichergestellt ist, dass die Personalisierungskommandos nach Abschluss der Personalisierung irreversibel gesperrt sind.

Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:

☒ **Card-G2-A_3261 K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung**

Zur Unterstützung herstellerspezifischer Personalisierungsprozessen KÖNNEN die Werte von Attributen eines Kartenproduktes von den Festlegungen dieses Dokumentes abweichen. Hierbei MÜSSEN Abweichungen auf solche beschränkt sein, die hinsichtlich ihrer Wirkung in der personalisierten Karte sowohl fachlich wie sicherheitstechnisch der in der Spezifikation vorgegebenen Werten entsprechen. ☒

4.8 Kartenadministration

In den Kapiteln 5.3.22 und 5.3.23 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen einem Kartenadministrationssystem (z.B. einem CUPs) und einer Karte beschrieben, die bei der Ausgabe der Karte angelegt werden müssen.

☒ **Card-G2-A_2994 K_Personalisierung: Absicherung der Kartenadministration**

Bei der Personalisierung MUSS der Schlüssel `PuK.RCA.ADMIN.CS` für die asymmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden. ☒

☒ **Card-G2-A_3592 Symmetrische Kartenadministration**

Bei der Personalisierung KÖNNEN die Schlüssel (`SK.CMS` und `SK.CUP`) für die symmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden. ☒

☒ **Card-G2-A_3593 Schlüsselspeicherung**

Der Kartenherausgeber MUSS sicherstellen, dass die Schlüssel zur Absicherung der Kartenadministration mindestens bis zum Ablauf der Zertifikate der Karte sicher

verwahrt werden und bei Bedarf an ein Kartenadministrationssystem (z.B. ein CUpS) übergeben werden können. ☒

5 Dateisystem der gSMC-K

Dieses Kapitel beschreibt die Konfiguration des Dateisystems, wobei folgende Applikationen berücksichtigt werden:

- MF siehe Kapitel 5.3.1
- DF.AK siehe Kapitel 5.4
- DF.NK siehe Kapitel 5.5
- DF.SAK siehe Kapitel 5.6
- DF.Sicherheitsanker siehe Kapitel 5.7

☒ **Card-G2-A_2540 K_Initialisierung: Normative Anforderungen**

Alle normativen Anforderungen des Kapitels 5 und seiner Unterkapitel MÜSSEN für die gSMC-K gelten. ☒

☒ **Card-G2-A_2541 K_Personalisierung: zusätzliche Ordner**

Die gSMC-K KANN Ordner enthalten, die in diesem Dokument nicht genannt sind. ☒

☒ **Card-G2-A_2542 K_Personalisierung: zusätzliche Objekte**

Jeder Ordner, der in diesem Dokument spezifiziert ist, KANN zusätzliche Objekte (Ordner, Dateien, Passwörter oder Schlüssel) enthalten. ☒

5.1 Attribute des Objektsystems

Das Objektsystem gemäß [gemSpec_COS] enthält folgende Attribute:

☒ **Card-G2-A_2543 K_Initialisierung: Wert des Attributes *root***

Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_gSMC-K_ObjSys_004 sein. ☒

☒ **Card-G2-A_2544 K_Personalisierung und K_Initialisierung: Wert des Attributes *answerToReset***

Die Werte der Attribute *coldAnswerToReset* und *warmAnswerToReset* MÜSSEN den Vorgaben der Anforderungen Card-G2-A_2547, Card-G2-A_2548, Card-G2-A_2997 und Card-G2-A_3041 entsprechen. ☒

☒ **Card-G2-A_2545 K_Personalisierung: Wert des Attributes *iccsn8***

Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein (siehe Kapitel 5.3.5). ☒

☒ **Card-G2-A_2546 K_Initialisierung: Inhalt persistentPublicKeyList**

In der *persistentPublicKeyList* MÜSSEN alle in dieser Spezifikation enthaltenen öffentlichen Schlüssel enthalten sein. ☒

☒ **Card-G2-A_3191 K_Initialisierung: Größe persistentPublicKeyList**

Für das Attribut *persistentPublicKeyList* MUSS so viel Speicherplatz bereitgestellt werden, dass mindestens fünf weitere öffentliche Signaturprüfchlüssel einer Root-CA mittels Linkzertifikaten persistent importierbar sind ☒

☒ **Card-G2-A_3268 K_Initialisierung: Wert von *pointInTime***

Das Attribut *pointInTime* MUSS den Wert '0000 0000 0000' = 2000.00.00 haben. Der Wert MUSS initialisiert werden. ☒

☒ **Card-G2-A_3514 K_Personalisierung: personalisierter Wert von *pointInTime***

Das Attribut *pointInTime* MUSS im Rahmen der Personalisierung auf den Wert von CED eines Endnutzerzertifikates gesetzt werden. Falls es mehrere Endnutzerzertifikate gibt, so ist das CED mit dem größten Wert zu verwenden. ☒

5.1.1 ATR-Kodierung und technische Eigenschaften ATR-Kodierung

Für die gSMC-K gelten die Konventionen für die technischen Eigenschaften, ATR und Übertragungsprotokolle aus [gemSpec_COS] für die elektrische Schnittstelle. Die gSMC-K ist als Plug-In-Karte (ID-000) für die Nutzung in entsprechenden Kartenterminals vorgesehen.

☒ **Card-G2-A_2547 K_Personalisierung und K_Initialisierung: ATR-Kodierung**

Die ATR-Kodierung MUSS die in Tab_gSMC-K_ObjSys_002 dargestellten Werte besitzen.

Tabelle 2: Tab_gSMC-K_ObjSys_002 ATR-Kodierung

Zeichen	Wert	Bedeutung
TS	'3B'	Initial Character (direct convention)
T0	'9x'	Format Character (TA1/TD1 indication, x = no. of HB)
TA1	'xx'	Interface Character (FI/DI, erlaubte Werte: siehe [gemSpec_COS#N024.100])
TD1	'81'	Interface Character, (T=1, TD2 indication)
TD2	'B1'	Interface Character, (T=1, TA3/TB3/TD3 indication)
TA3	'FE'	Interface Character (IFSC coding)
TB3	'45'	Interface Character, (BWI/CWI coding)
TD3	'1F'	Interface Character, (T=15, TA4 indication)
TA4	'xx'	Interface Character (XI/UI coding)
Ti	HB	Historical Bytes (maximal 15 Oktett)
TCK	XOR	Check Character (exclusive OR)

☒

☒ **Card-G2-A_2548 K_Personalisierung und K_Initialisierung: TC1 Byte im ATR**

Der ATR SOLL ein TC1 Byte mit dem Wert 'FF' enthalten. In diesem Fall MUSS T0 auf den Wert 'Dx' gesetzt werden. ☒

☒ **Card-G2-A_2997 K_Personalisierung und K_Initialisierung: Historical Bytes im ATR**

Das Attribut answerToReset SOLL keine Historical Bytes enthalten. ☒

☒ **Card-G2-A_3041 K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes**

Falls answerToReset Historical Bytes enthält, dann MÜSSEN

- a. diese gemäß [ISO7816-4] kodiert sein.
- b. die dort getroffenen Angaben konsistent sein zu Angaben im EF.ATR. ☒

5.2 Allgemeine Struktur

In dem zugehörnden Kapitel sind alle Objekte eines Typs gemeinsam dargestellt; die jeweils gültigen Parameter sind in einer Tabelle beschrieben.

Die Abbildung 1 zeigt die allgemeine Struktur der gSMC-K.

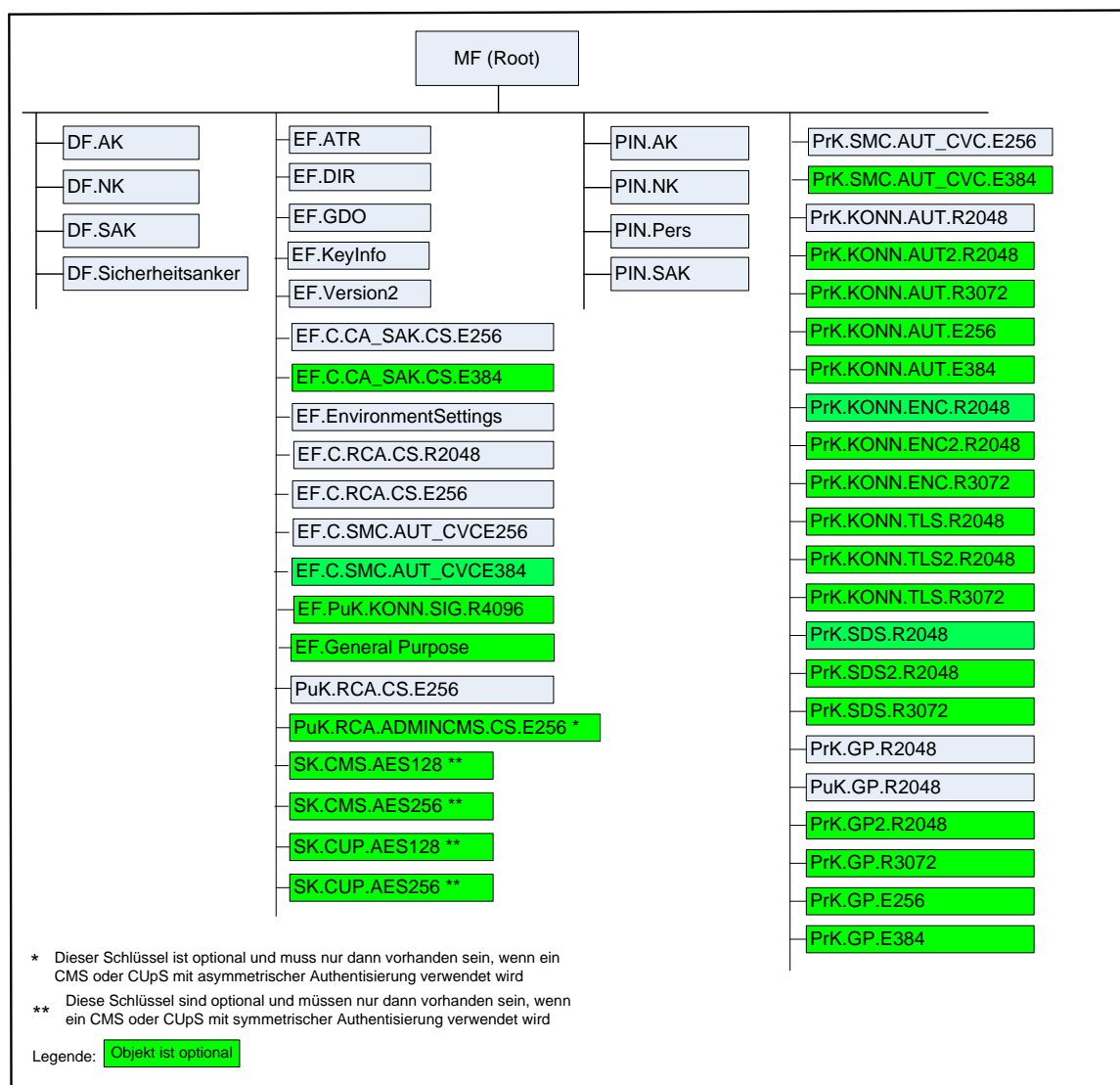


Abbildung 1: Abb_gSMC-K_ObjSys_001 Dateistruktur einer gSMC-K auf oberster Ebene

5.3 Root-Anwendung und Dateien auf MF-Ebene

5.3.1 MF

Diese Applikation beinhaltet allgemeine Datenelemente und Informationen, die dem Betrieb der Chipkarte als solche dienen, oder allen Anwendungen gleichermaßen zur Verfügung stehen.

☒ Card-G2-A_2553 K_Initialisierung: Initialisierte Attribute von MF

MF MUSS die in Tab_gSMC-K_ObjSys_004 dargestellten Werte besitzen.

Tabelle 3: Tab_gSMC-K_ObjSys_004 - Initialisierte Attribute von MF

Attribute	Wert	Bemerkung
Objektyp	Ordner	
applicationIdentifier	'D276 0001 4480 01'	
fileIdentifier	'3F 00'	falls vorhanden
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
FINGERPRINT	Wildcard	
GET RANDOM	ALWAYS	
LOAD APPLICATION	PWD(PIN.Pers) OR AUT_CMS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (2) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (3) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.3 im Allgemeinen irrelevant.

5.3.2 MF / EF.ATR

Die transparente Datei EF.ATR enthält Informationen zur maximalen Größe einer APDU in Sende- und Empfangsrichtung sowie zur Identifizierung des Betriebssystems.

☒ Card-G2-A_2554 K_Initialisierung: Initialisierte Attribute von MF / EF.ATR

Das Objekt EF.ATR MUSS die in Tab_gSMC-K_ObjSys_005 dargestellten Werte besitzen.

Tabelle 4: Tab_gSMC-K_ObjSys_005 - Initialisierte Attribute von MF / EF.ATR

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 01'	siehe Hinweis (5)
shortFileIdentifier	'1D' = 29	
numberOfOctet	herstellerspezifisch	
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	

<i>shareable</i>	True	
<i>body</i>	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY WRITE BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (4) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: *ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY*.

Hinweis (5) Der Wert des Attributs *fileIdentifier* ist in [ISO7816-4] festgelegt.

☒ **Card-G2-A_3251 K_Initialisierung: Initialisiertes Attribut *numberOfOctet* von MF / EF.ATR**

Das Attribut *numberOfOctet* MUSS so gewählt werden, dass nach Abschluss der Initialisierungsphase entweder

- genau 23 Oktette für die Artefakte PT_Pers und PI_Personalisierung frei bleiben, falls PI_Kartenkörper initialisiert wird, oder
- genau 41 Oktette für die Artefakte PI_Kartenkörper, PT_Pers und PI_Personalisierung frei bleiben. ☒

5.3.3 MF / EF.DIR

Die Datei EF.DIR enthält eine Liste mit Anwendungs-Templates gemäß [ISO7816-4].

☒ **Card-G2-A_2563 K_Initialisierung: Initialisierte Attribute von MF / EF.DIR**

Das Objekt EF.DIR MUSS die in Tab_gSMC-K_ObjSys_009 dargestellten Werte besitzen.

Tabelle 5: Tab_gSMC-K_ObjSys_009 Initialisierte Attribute von MF / EF.DIR

Attribute	Wert	Bemerkung
Objektyp	linear variables Elementary File	
<i>fileIdentifier</i>	'2F 00'	siehe Hinweis (7)
<i>shortFileIdentifier</i>	'1E' = 30	siehe Hinweis (7)
<i>numberOfOctet</i>	'006E' Oktett = 110 Oktett	

<i>maxNumRecords</i>	8 Rekord	
<i>maxRecordLength</i>	32 Oktett	
<i>flagRecordLCS</i>	False	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>recordList</i>		
Rekord 1	'61-09-(4F 07 D27600014480 01)'	MF siehe 5.3.1
Rekord 2	'61-08-(4F 06'D27600014402)'	AK siehe 5.4
Rekord 3	'61-08-(4F 06 D27600014403)'	NK siehe 5.5
Rekord 4	'61-08-(4F 06 D27600014404)'	SAK, siehe 5.6
Rekord 5	'61-08-(4F 06 D27600014405)'	Sicherheitsanker siehe 5.7
Rekord 6	nicht vorhanden, MUSS mittels APPEND RECORD	siehe Hinweis (8)
...	angelegt werden	
...	...	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
APPEND RECORD	PWD(PIN.Pers) OR AUT_CMS	siehe Hinweis (9)
DELETE RECORD	AUT_CMS	siehe Hinweis (9)
READ RECORD	ALWAYS	
SEARCH RECORD		
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (6) Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind:

ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, DELETE RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, TERMINATE, UPDATE RECORD, WRITE RECORD.

Hinweis (7) Die Werte von *fileIdentifier* und *shortFileIdentifier* sind in [ISO7816-4] festgelegt.

Hinweis (8) Weitere Records existieren nur, wenn optionale Applikationen vorhanden sind.

Hinweis (9) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.10.

5.3.4 MF / EF.EnvironmentSettings

In EF.EnvironmentSettings wird die Information gespeichert, über welche der Konnektor erkennen kann, in welcher Umgebung er betrieben wird.

☒ **Card-G2-A_2565 K_Initialisierung: Initialisierte Attribute von MF / EF.EnvironmentSettings**

Das Objekt EF.EnvironmentSettings MUSS die in Tab_gSMC-K_ObjSys_010 dargestellten Werte besitzen.

Tabelle 6: Tab_gSMC-K_ObjSys_010 Initialisierte Attribute von MF / EF.EnvironmentSettings

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 13'	
shortFileIdentifier	'13' = 19	
numberOfOctet	'0100' Oktett = 256 Oktett	
positionLogicalEndOfFile	'0'	wird personalisiert
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (10) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

☒ **Card-G2-A_3394 K_Personalisierung: Personalisierte Attribute von MF / EF.EnvironmentSettings**

Bei der Personalisierung von EF.EnvironmentSettings MÜSSEN die in Tab_gSMC-K_ObjSys_090 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 7: Tab_gSMC-K_ObjSys_090 Attribute von MF / EF.EnvironmentSettings

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	1	

body	gemäß [gemSpec_Karten_Fach_TIP]	
------	---------------------------------	--



5.3.5 MF / EF.GDO

In EF.GDO wird das Datenobjekt ICCSN gespeichert, welches die Kennnummer der Karte enthält.

☒ **Card-G2-A_2566 K_Initialisierung: Initialisierte Attribute von MF / EF.GDO**

Das Objekt EF.GDO MUSS die in Tab_gSMC-K_ObjSys_011 dargestellten Werte besitzen.

Tabelle 8: Tab_gSMC-K_ObjSys_011 Initialisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifizier	'2F 02'	
shortFileIdentifizier	'02' = 2	
numberOfOctet	'0C' Oktett = 12 Oktett	
positionLogicalEndOfFile	Wildcard	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Wildcard	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (11) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

☒ **Card-G2-A_2567 K_Personalisierung: Personalisiertes Attribut von EF.GDO**

Bei der Personalisierung von EF.GDO MÜSSEN die in Tab_gSMC-K_ObjSys_177 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 9: Tab_gSMC-K_ObjSys_177 Personalisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	'0C' Oktett = 12 Oktett	
<i>body</i>	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	



5.3.6 MF / EF.KeyInfo

Die Datei EF.KeyInfo enthält die Information darüber, welche Datei- und Schlüsselreferenzen aktuell zu verwenden sind und welches Gültigkeitsende sie haben.

☒ Card-G2-A_3392 K_Initialisierung: Attribute von MF / EF.KeyInfo

EF.KeyInfo MUSS die in Tab_gSMC-K_ObjSys_150 dargestellten initialisierten Attribute besitzen.

Tabelle 10: Tab_gSMC-K_ObjSys_150 Initialisierte Attribute von MF / EF.KeyInfo

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
<i>fileIdentifier</i>	'2F 1A'	
<i>shortFileIdentifier</i>	'1A' = 26	
<i>maxNumRecords</i>	30 Rekord	
<i>maxRecordLength</i>	36 Oktett	
<i>flagRecordLCS</i>	False	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>recordList</i>	Rekord 1 'XX...YY' Rekord 2 'XX...YY' ... Rekord 30 'XX...YY'	Der Rekordeinhalt wird in [gemSpec_Karten_Fach_TIP] festgelegt.
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ RECORD SEARCH RECORD	ALWAYS	

Attribute	Wert	Bemerkung
UPDATE RECORD	AUT_CMS OR AUT_CUP	siehe Hinweis (13)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	



Hinweis (12) Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate

Hinweis (13) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar

5.3.7 MF / EF.Version2

Die Datei EF.Version2 enthält die Versionsnummern sowie Produktidentifikatoren grundsätzlich veränderlicher Elemente der Karte:

- Version des Produkttyps des aktiven Objektsystems (inkl. Kartenkörper)
- Herstellerspezifische Produktidentifikation der Objektsystemimplementierung
- Versionen der Befüllvorschriften für verschiedene Dateien dieses Objektsystems

Die konkrete Befüllung ist in [gemSpec_Karten_Fach_TIP] beschrieben.

Elemente, die nach Initialisierung durch Personalisierung oder reine Kartennutzung nicht veränderlich sind, werden in EF.ATR versioniert.

Card-G2-A_2568 K_Initialisierung: Initialisierte Attribute von MF / EF.Version2

Das Objekt EF.Version2 MUSS die in Tab_gSMC-K_ObjSys_012 dargestellten Werte besitzen.

Tabelle 11 Tab_gSMC-K_ObjSys_012 Initialisierte Attribute von MF / EF.Version2

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 11'	
shortFileIdentifier	'11' = 17	

<i>numberOfOctet</i>	'003C' Oktett = 60 Oktett	
<i>positionLogicalEndOfFile</i>	passend zum Inhalt	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
UPDATE BINARY SET LOGICAL EOF	AUT_CMS	siehe Hinweis (15)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (14) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap.5.10.

5.3.8 MF / EF.C.CA_SAK.CS.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SAK.CS.E256 einer CA enthält. Das Zertifikat lässt sich mittels MF / PuK.RCA.CS.E256 (siehe Kapitel 5.3.21) prüfen. Der im Zertifikat enthaltene öffentliche Schlüssel dient der Verifizierung von weiteren Zertifikaten, die im Dateisystem enthalten sind (siehe zum Beispiel Kapitel 5.6.8).

Card-G2-A_2561 K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E256

Das Objekt EF.C.CA_SAK.CS.E256 MUSS die in Tab_gSMC-K_ObjSys_007 dargestellten Werte besitzen.

Tabelle 12: Tab_gSMC-K_ObjSys_007 Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E256

Attribute	Wert	Bemerkung
<i>Objektyp</i>	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 07'	
<i>shortFileIdentifier</i>	'07' = 7	
<i>numberOfOctet</i>	'011D' Oktett = 285 Oktett	

<i>positionLogicalEndOfFile</i>	Wildcard	wird personalisiert
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (17)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (17)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (15) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (16) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

Card-G2-A_3393 K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SAK.CS.E256

Bei der Personalisierung von EF.C.CA_SAK.CS.E256 MÜSSEN die in Tab_gSMC-K_ObjSys_087 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 13: Tab_gSMC-K_ObjSys_087 Attribute von MF / EF.C.CA_SAK.CS.E256

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	'00DC' Oktett = 220 Oktett	
<i>body</i>	C.CA_SAK.CS.E256 gemäß [gemSpec_PKI#6.7.1]	
<i>body</i> Option_Erstellung _von_Testkarten	C.CA_SAK.CS.E256 gemäß [gemSpec_PKI#6.7.1] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1 .2]



5.3.9 MF / EF.C.CA_SAK.CS.E384

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SAK.CS.E384 einer CA enthält. Der im Zertifikat enthaltene öffentliche Schlüssel dient der Verifizierung von weiteren Zertifikaten, die im Dateisystem enthalten sind (siehe zum Beispiel Kapitel 5.6.10).

☒ Card-G2-A_2562 K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E384

Das Objekt EF.C.CA_SAK.CS.E384 MUSS die in Tab_gSMC-K_ObjSys_008 dargestellten Werte besitzen.

Tabelle 14: Tab_gSMC-K_ObjSys_008 Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E384

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 0D'	
shortFileIdentifier	'0D' = 13	
numberOfOctet	'011D' Oktett = 285 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird später nachgeladen
Zugriffsregeln		
accessRules	identisch zu EF.C.CA_SAK.CS.E256	



5.3.10 MF / EF.PuK.RCA.CS.R2048

Diese Datei enthält den öffentlichen Schlüssel der CVC-Root-CA der Generation 1. Das Zertifikat kann vom Konnektor ausgelesen werden, um mit dem Schlüssel als Gegenstelle einer eGK G1 deren Echtheit zu überprüfen.

☒ Card-G2-A_3252 K_Initialisierung: Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048

Das Objekt EF.PuK.RCA.CS.R2048 MUSS die in Tab_gSMC-K_ObjSys_176 dargestellten Werte besitzen.

Tabelle 15: Tab_gSMC-K_ObjSys_176 Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 14'	

<i>shortFileIdentifier</i>	'14' = 20	
<i>numberOfOctet</i>	'01 10' Oktett = 272 Oktett	
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette	
<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden. Für Option_Erstellung_von_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden.		
<i>body</i>	Öffentlicher Schlüssel mit Modulslänge 2048 Bit, TLV-codiert mit dem Wert der CVC-Root-CA aus der PU gemäß [gemSpec_CVC_TSP#4.5]	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (21)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (17) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (18) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

☒ **Card-G2-A_3580 K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten**

Bei der Personalisierung von EF.PuK.RCA.CS.R2048 für Testkarten MUSS das in Tab_gSMC-K_ObjSys_148 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 16:Tab_gSMC-K_ObjSys_148 Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten

Attribute	Wert	Bemerkung
<i>body</i>	Öffentlicher Schlüssel mit Modulslänge 2048 Bit, TLV-codiert, mit dem Wert der CVC-Root-CA aus der RU/TU	Details siehe [gemSpec_TK#3.1.2]



5.3.11 MF / EF.C.RCA.CS.E256

Diese Datei enthält den zum Zeitpunkt der gSMC-K-Produktion ältesten noch verwendbaren Schlüssel PuK.RCA.CS.E256 in Form eines „self-signed“ CV-Zertifikates. Das Zertifikat kann vom Konnektor ausgelesen werden, um mit dem Schlüssel als Gegenstelle einer eGK G2 deren Echtheit zu überprüfen.

☒ **Card-G2-A_2666 K_Initialisierung: Initialisierte Attribute von MF / EF.C.RCA.CS.E256**

Das Objekt EF.C.RCA.CS.E256 MUSS die in Tab_gSMC-K_ObjSys_084 dargestellten Werte besitzen.

Tabelle 17: Tab_gSMC-K_ObjSys_084 Initialisierte Attribute von MF / EF.C.RCA.CS.E256

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 15'	
<i>shortFileIdentifier</i>	'15' = 21	
<i>numberOfOctet</i>	'DC' Oktett = 220 Oktett	
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden.		
Für Option_Erstellung_von_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden.		
<i>body</i>	„self-signed“ CV-Zertifikat mit einem öffentlichen Schlüssel mit Domainparameter = brainpoolP256r1 codiert gemäß [TR-03110-3#Table 17] mit dem Wert der CVC-Root-CA aus der PU gemäß [gemSpec_CVC_TSP#4.5]	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (21)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	siehe Hinweis (3)
------	----------------------	-------------------



Hinweis (19) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: *ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.*

Hinweis (20) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

☒ **Card-G2-A_3581 K_Personalisierung: Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten**

Bei der Personalisierung von EF.C.RCA.CS.E256 für Testkarten MUSS das in Tab_gSMC-K_ObjSys_149 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 18: Tab_gSMC-K_ObjSys_149 Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten

Attribute	Wert	Bemerkung
body	„self-signed“ CV-Zertifikat mit einem öffentlichen Schlüssel mit Domainparameter = brain-poolP256r1 codiert gemäß [TR-03110-3#Table 17] mit dem Wert der CVC-Root-CA aus der RU/TU	gemäß [gemSpec_TK#3.1.2]



5.3.12 MF / EF.C.SMC.AUT_CVC.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_PKI], welches den öffentlichen Schlüssel PuK.SMC.AUT_CVC.E256 zum zugehörigen privaten Schlüssel (siehe Kapitel 5.3.18) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_SAK.CS.E256 (siehe Kapitel 5.3.8) prüfen.

☒ **Card-G2-A_3280 K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256**

EF.C.SMC.AUT_CVC.E256 MUSS die in Tab_gSMC-K_ObjSys_192 dargestellten Attribute besitzen.

Tabelle 19: Tab_gSMC-K_ObjSys_192 Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 0A'	
shortFileIdentifier	'0A' = 10	
numberOfOctet	'01 1F' Oktett = 287 Oktett	
positionLogi-	Wildcard	wird personalisiert


<i>calEndOfFile</i>		
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	Wildcard	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	



Hinweis (21) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (22) Das Zertifikat enthält eine Flagliste mit dem Wert '00...00'.

☒ Card-G2-A_3328 K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUT_CVC.E256

Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MUSS bei der Personalisierung für die CHR des Zertifikates CHR = '00 05' || IC-CSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2567].

☒ Card-G2-A_3329 K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256

Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von EF.C.SMC.AUT_CVC.E256 die in Tab_gSMC-K_ObjSys_193 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 20: Tab_gSMC-K_ObjSys_193 Personalisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256

Attribute	Wert	Bemerkung
-----------	------	-----------

<i>positionLogicalEndOfFile</i>	'00 DE' Oktett = 222 Oktett	4
<i>body</i>	C.SMC.AUT_CVC.E256 gemäß [gemSpec_PKI]	



5.3.13 MF / EF.C.SMC.AUT_CVC.E384

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_PKI], welches den öffentlichen Schlüssel PuK.SMC.AUT_CVC.E384 zum zugehörigen privaten Schlüssel (siehe Kapitel 5.3.19) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_SAK.CS.E384 (siehe Kapitel 5.3.9) prüfen.

☒ Card-G2-A_3330 K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E384

EF.C.SMC.AUT_CVC.E384 MUSS die in Tab_gSMC-K_ObjSys_194 dargestellten Attribute besitzen.

Tabelle 21: Tab_gSMC-K_ObjSys_194 Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E384

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 0F'	
<i>shortFileIdentifier</i>	'0F' = 15	
<i>numberOfOctet</i>	'01 1F' Oktett = 287 Oktett	
<i>positionLogicalEndOfFile</i>	'0'	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	
Zugriffsregel		
<i>accessRules</i>	identisch zu EF.C.SMC.AUT_CVC.E256	




Hinweis (23) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (24) Das Zertifikat enthält eine Flagliste mit dem Wert '00...00'.

☒ Card-G2-A_3331 K_externe Welt: Festlegung von CHR für EF.C.SMC.AUT_CVC.E384

Falls das asymmetrische Authentifizierungsverfahren genutzt wird, dann MUSS bei der Erstellung des Zertifikats C.SMC.AUT_CVC.E384 für die CHR gelten: CHR = '00 06' ||

ICCSN , wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2567]. 

5.3.14 MF / PIN.AK

Dieses Passwortobjekt wird zur Freischaltung von gewissen Operationen im DF.AK (siehe Kapitel 5.4) verwendet.

Card-G2-A_2569 K_Initialisierung: Initialisierte Attribute von MF / PIN.AK

Das Objekt PIN.AK MUSS die in Tab_gSMC-K_ObjSys_013 dargestellten Werte besitzen.

Tabelle 22: Tab_gSMC-K_ObjSys_013 Initialisierte Attribute von MF / PIN.AK

Attribute	Wert	Bemerkung
Objektyp	Passwortobjekt	
<i>pwdIdentifier</i>	'00' = 0	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	12	
<i>maximumLength</i>	12	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	
<i>PUK</i>	kein Inhalt	keine PUK
<i>pukUsage</i>	0	keine PUK
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (27)
	herstellerspezifisch	siehe Hinweis (27)
CHANGE RD, P1=0	ALWAYS	siehe Hinweis (28)
DISABLE VERIFICATION REQUIREMENT	PWD(PIN.AK)	
ENABLE VERIFICATION REQUIREMENT	ALWAYS	
GET PIN STATUS	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (25) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION RE-

QUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

Hinweis (26) Diese Tabellenzeile gilt für den Fall *transportStatus* gleich Leer-PIN.

Hinweis (27) Diese Tabellenzeile gilt für den Fall *transportStatus* ungleich Leer-PIN.

☒ **Card-G2-A_2570 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AK**

Wenn für PIN.AK als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.AK nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen. ☒

☒ **Card-G2-A_3396 K_Personalisierung: Personalisierte Attribute von MF / PIN.AK**

Wenn der Wert des Attributes *transportStatus* Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.AK die in Tab_gSMC-K_ObjSys_094 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab_gSMC-K_ObjSys_094 Attribute von MF / PIN.AK

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
<i>transportStatus</i>	Transport-PIN	wird gegebenenfalls personalisiert, siehe Hinweis (29)



Hinweis (28) Für *transportStatus* wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando *Change Reference Data* ist es möglich, diesen Wert im Rahmen der Personalisierung auf „*regularPassword*“ zu setzen.

5.3.15 MF / PIN.NK

Dieses Passwortobjekt wird zur Freischaltung von gewissen Operationen im DF.NK (siehe Kapitel 5.5) verwendet.

☒ **Card-G2-A_2571 K_Initialisierung: Initialisierte Attribute von MF / PIN.NK**

Das Objekt PIN.NK MUSS die in Tab_gSMC-K_ObjSys_014 dargestellten Werte besitzen.

Tabelle 24: Tab_gSMC-K_ObjSys_014 Initialisierte Attribute von MF / PIN.NK

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
<i>pwdIdentifier</i>	'01' = 1	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	12	

<i>maxLength</i>	12	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	
<i>PUK</i>	kein Inhalt	keine PUK
<i>pukUsage</i>	0	keine PUK
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (31)
	herstellerspezifisch	siehe [Card-G2-A_2572]
CHANGE RD, P1=0	ALWAYS	siehe Hinweis (32)
DISABLE VERIFICATION REQUIREMENT	PWD(PIN.NK)	
ENABLE VERIFICATION REQUIREMENT	ALWAYS	
GET PIN STATUS	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)




Hinweis (29) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

Hinweis (30) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.

Hinweis (31) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

Card-G2-A_2572 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.NK

Wenn für PIN.NK als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.NK nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerepezifisch umzusetzen. 

Card-G2-A_3397 K_Personalisierung: Personalisierte Attribute von MF / PIN.NK

Wenn der Wert des Attributes transportStatus Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.NK die in Tab_gSMC-K_ObjSys_095 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 25: Tab_gSMC-K_ObjSys_095 Attribute von MF / PIN.NK

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
<i>transportStatus</i>	Transport-PIN	wird gegebenenfalls personalisiert, siehe Hinweis (33)



Hinweis (32) Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

5.3.16 MF / PIN.Pers

Dieses Passwortobjekt wird zur Freischaltung verwendet, wenn im *root*-Verzeichnis neue Dateien oder Applikationen anzulegen sind.

☒ **Card-G2-A_2573 K_Initialisierung: Initialisierte Attribute von MF / PIN.Pers**

Das Objekt PIN.Pers MUSS die in Tab_gSMC-K_ObjSys_015 dargestellten Werte besitzen.

Tabelle 26: Tab_gSMC-K_ObjSys_015 Initialisierte Attribute von MF / PIN.Pers

Attribute	Wert	Bemerkung
Objektyp	Passwortobjekt	
<i>pwdIdentifier</i>	'02' = 2	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	12	
<i>maximumLength</i>	12	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	
<i>PUK</i>	kein Inhalt	keine PUK
<i>pukUsage</i>	0	keine PUK
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (35)
	herstellerspezifisch	siehe [Card-G2-A_2574]

CHANGE RD, P1=0	ALWAYS	siehe Hinweis (36)
DISABLE VERIFICATION REQUIREMENT	PWD(PIN.Pers)	
ENABLE VERIFICATION REQUIREMENT	ALWAYS	
GET PIN STATUS	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (33) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

Hinweis (34) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.

Hinweis (35) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

Card-G2-A_2574 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.Pers

Wenn für PIN.Pers als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.Pers nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerepezifisch umzusetzen.

Card-G2-A_3398 K_Personalisierung: Personalisierte Attribute von MF / PIN.Pers

Wenn der Wert des Attributes *transportStatus* Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.Pers die in Tab_gSMC-K_ObjSys_096 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 27: Tab_gSMC-K_ObjSys_096 Attribute von MF / PIN.Pers

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
<i>transportStatus</i>	Transport-PIN	Wird gegebenenfalls personalisiert, Hinweis (37)



Hinweis (36) Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

5.3.17 MF / PIN.SAK

Dieses Passwortobjekt wird zur Freischaltung von gewissen Operationen im DF.SAK (siehe Kapitel 5.6) verwendet.

☒ **Card-G2-A_2575 K_Initialisierung: Initialisierte Attribute von MF / PIN.SAK**

Das Objekt PIN.SAK MUSS die in Tab_gSMC-K_ObjSys_016 dargestellten Werte besitzen.

Tabelle 28: Tab_gSMC-K_ObjSys_016 Initialisierte Attribute von MF / PIN.SAK

Attribute	Wert	Bemerkung
Objektyp	Passwortobjekt	
<i>pwdIdentifier</i>	'03' = 3	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	12	
<i>maximumLength</i>	12	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	
<i>PUK</i>	kein Inhalt	keine PUK
<i>pukUsage</i>	0	keine PUK
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (39)
	herstellerspezifisch	siehe [Card-G2-A_2576]
CHANGE RD, P1=0	ALWAYS	siehe Hinweis (40)
DISABLE VERIFICATION REQUIREMENT	PWD(PIN.SAK)	
ENABLE VERIFICATION REQUIREMENT	ALWAYS	
GET PIN STATUS	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (37) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE

Hinweis (38) Diese Tabellenzeile gilt für den Fall *transportStatus* gleich *Leer-PIN*.

Hinweis (39) Diese Tabellenzeile gilt für den Fall *transportStatus* ungleich *Leer-PIN*.

☒ **Card-G2-A_2576 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SAK**

Wenn für PIN.SAK als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.SAK nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen. ☒

☒ **Card-G2-A_3399 K_Personalisierung: Personalisierte Attribute von MF / PIN.SAK**

Wenn der Wert des Attributes *transportStatus* *Transport-PIN* ist, MÜSSEN bei der Personalisierung von PIN.SAK die in Tab_gSMC-K_ObjSys_097 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 29: Tab_gSMC-K_ObjSys_097 Attribute von MF / PIN.SAK

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
<i>transportStatus</i>	Transport-PIN	wird gegebenenfalls personalisiert, siehe Hinweis (41)



Hinweis (40) Für *transportStatus* wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando *Change Reference Data* ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

5.3.18 MF / PrK.SMC.AUT_CVC.E256

Dieser Schlüssel wird für die Kryptographie mit elliptischen Kurven im Rahmen von asymmetrischen Authentisierungsprotokollen verwendet. Der zugehörige öffentliche Schlüssel befindet sich in einem CV-Zertifikat, das in der Datei EF.C.SMC.AUT_CVC.E256 gespeichert ist (siehe Kapitel 5.3.12).

☒ **Card-G2-A_3332 K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E256**

PrK.SMC.AUT_CVC.E256 MUSS die in Tab_gSMC-K_ObjSys_195 dargestellten Attribute besitzen.

Tabelle 30: Tab_gSMC-K_ObjSys_195 Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt ELC 256	
<i>keyIdentifier</i>	'05' = 5	

<i>privateElcKey</i>	domainparameter = brainpoolP256r1	
<i>privateElcKey</i>	keyData = AttributNotSet	<i>wird personalisiert</i>
<i>keyAvailable</i>	Wildcard	
<i>numberScenario</i>	0	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS#16.1] {elcAsynchronAdmin, elcSessionkey4SM}	
<i>accessRulesSession keys</i>	Wildcard	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DEACTIVATE	AUT_CMS OR AUT_CUP	
ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
GENERATE ASYMMETRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE	AUT_CMS OR AUT_CUP	
DEACTIVATE	NEVER	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	



Hinweis (41) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

☒ **Card-G2-A_3333 K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUT_CVC.E256**

Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von PrK.SMC.AUT_CVC.E256 die in Tab_gSMC-K_ObjSys_196 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 31: Tab_gSMC-K_ObjSys_196 Personalisierte Attribute von MF / PrK.SMC.AUT_CVC.E256

Attribute	Wert	Bemerkung
<i>keyAvailable</i>	True	
<i>privateElcKey</i>	keyData = eine ganze Zahl im Intervall [1, domainParameter.n – 1]	2



5.3.19 MF / PrK.SMC.AUT_CVC.E384

Dieser Schlüssel wird für die Kryptographie mit elliptischen Kurven im Rahmen von asymmetrischen Authentisierungsprotokollen verwendet. Der zugehörige öffentliche Schlüssel befindet sich in einem CV-Zertifikat, das in der Datei EF.C.SMC.AUT_CVC.E384 gespeichert ist (siehe Kapitel 5.3.13).

☒ **Card-G2-A_3334 K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E384**

PrK.SMC.AUT_CVC.E384 MUSS die in Tab_gSMC-K_ObjSys_197 dargestellten Attribute besitzen.

Tabelle 32: Tab_gSMC-K_ObjSys_197 Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt ELC 384	
<i>keyIdentifier</i>	'06' = 6	
<i>privateElcKey</i>	domainparameter = brainpoolP384r1	
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>numberScenario</i>	0	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS#16.1] {elcAsynchronAdmin, elcSessionkey4SM}	
<i>accessRulesSession keys</i>	irrelevant	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DEACIVATE	AUT_CMS OR AUT_CUP	

ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
GENERATE ASYMMETRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE	AUT_CMS OR AUT_CUP	
DEACTIVATE	NEVER	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	



Hinweis (42) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.3.20 Herstellerspezifische Schlüssel

5.3.20.1 MF / PrK.KONN.AUT.R2048

Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht den Aufbau eines TLS-Kanals sowohl client-seitig, als auch server-seitig. Der öffentliche Teil zu diesem privaten Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

Gemäß [TLS#8.1.1] wird für bestimmte Ciphersuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2 durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus rsaDecipherPKCS1_V1_5.

Gemäß [TLS#7.4.8] wird während der Clientauthentisierung eine Signatur nach [PKCS#1v2.1] durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus signPSS.

☒ **Card-G2-A_2577 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R2048**

Das Objekt PrK.KONN.AUT.R2048 MUSS die in Tab_gSMC-K_ObjSys_017 dargestellten Werte besitzen.

Tabelle 33: Tab_gSMC-K_ObjSys_017 Initialisierte Attribute von MF / PrK.KONN.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
keyIdentifier	'07' = 7	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]: { rsaDecipherPKCS1_V1_5 sign PKCS1_V1_5, signPSS }	siehe Hinweis (45) Hinweis (46)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='84' oder P1='80'	PWD(PIN.Pers)	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	OR PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK)	
PSO Decipher	OR PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK)	
TERMINATE	PWD(PIN.Pers)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (43) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (44) Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.

Hinweis (45) Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

☒ **Card-G2-A_3400 K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.AUT.R2048**

Bei der Personalisierung von PrK.KONN.AUT.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_098 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 34: Tab_gSMC-K_ObjSys_098 Attribute von MF / PrK.KONN.AUT.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	true	



5.3.20.2 MF / PrK.KONN.AUT2.R2048

Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client-seitig, als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der öffentliche Teil zu diesem privaten Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

Gemäß [TLS#8.1.1] wird für bestimmte Ciphersuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2 durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus rsaDecipherPKCS1_V1_5.

Gemäß [TLS#7.4.8] wird während der Clientauthentisierung eine Signatur nach [PKCS#1v2.1] durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus signPSS.

☒ **Card-G2-A_3442 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048**

Das Objekt PrK.KONN.AUT2.R2048 MUSS die in Tab_gSMC-K_ObjSys_152 dargestellten Werte besitzen.

Tabelle 35: Tab_gSMC-K_ObjSys_152 Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'11' = 17	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt

<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS]: { rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, signPSS }	siehe Hinweis (45) Hinweis (46)
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.KONN.AUT.R2048	



5.3.20.3 MF / PrK.KONN.AUT.R3072

Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client- als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Gemäß [TLS#8.1.1] wird für bestimmte Ciphersuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2.2 durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus rsaDecipherPKCS1_V1_5.

Gemäß [TLS#7.4.8] wird während der Clientauthentisierung eine Signatur nach [PKCS#1v2.1] durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus signPSS.

☒ **Card-G2-A_2578 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R3072**

Das Objekt PrK.KONN.AUT.R3072 MUSS die in Tab_gSMC-K_ObjSys_018 dargestellten Werte besitzen.

Tabelle 36: Tab_gSMC-K_ObjSys_018 Initialisierte Attribute von MF / PrK.KONN.AUT.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'0A' = 10	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS]: { rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, signPSS }	Hinweis (47) Hinweis (48)
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.KONN.AUT.R2048	



Hinweis (46) Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.

Hinweis (47) Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

5.3.20.4 MF / PrK.KONN.AUT.E256

Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client-seitig, als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3443 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E256**

Das Objekt PrK.KONN.AUT.E256 MUSS die in Tab_gSMC-K_ObjSys_178 dargestellten Werte besitzen.

Tabelle 37: Tab_gSMC-K_ObjSys_178 Initialisierte Attribute von MF / PrK.KONN.AUT.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'13' = 19	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]: { elcSharedSecretCalculation, signECDSA }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.KONN.AUT.R2048	



Hinweis (48) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.3.20.5 MF / PrK.KONN.AUT.E384

Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client- als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384}

bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_2579 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E384**

Das Objekt PrK.KONN.AUT.E384 MUSS die in Tab_gSMC-K_ObjSys_019 dargestellten Werte besitzen.

Tabelle 38: Tab_gSMC-K_ObjSys_019 Initialisierte Attribute von MF / PrK.KONN.AUT.E384

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 384	
keyIdentifier	'0E' = 14	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]: { elcSharedSecretCalculation, signECDSA }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.KONN.AUT.R2048	



Hinweis (49) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

**5.3.20.6 MF / PrK.KONN.ENC.R2048
(Option_Erweiterung_herstellerspezifische_Schlüssel_01)**

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.

Er unterstützt das Entschlüsseln von Daten.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3337 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R2048
(Option_Erweiterung_herstellerspezifische_Schlüssel_01)**

PrK.KONN.ENC.R2048 MUSS die in Tab_gSMC-K_ObjSys_198 dargestellten Attribute besitzen.

Tabelle 37: Tab_gSMC-K_ObjSys_198 Initialisierte Attribute von MF / PrK.KONN.ENC.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'09' = 9	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM-METRIC KEY PAIR P1='C0' oder P1='C4'	PWD(PIN.Pers)	
GENERATE ASYM-METRIC KEY PAIR P1='81'	ALWAYS	
PSO Decipher	OR PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK)	
PSO Transcipher	OR PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK)	
TERMINATE	PWD(PIN.Pers)	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingungen	Bemerkungen
alle	Herstellerspezifisch	Siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingungen	Bemerkungen
Alle	NEVER	



Hinweis 51: (Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

☒ **Card-G2-A_3338 K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)**

Bei der Personalisierung von PrK.KONN.ENC.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_199 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 38: Tab_gSMC-K_ObjSys_199 Attribute von MF / PrK.KONN.ENC.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	true	



5.3.20.7 MF / PrK.KONN.ENC2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.

Er unterstützt das Entschlüsseln von Daten. Er ist dafür vorgesehen, den Schlüssel PrK.KONN.ENC.R2048 nach Ablauf von dessen Nutzungszeit abzulösen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3339 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)**

PrK.KONN.ENC2.R2048 MUSS die in Tab_gSMC-K_ObjSys_200 dargestellten Attribute besitzen.

Tabelle 39: Tab_gSMC-K_ObjSys_200 Initialisierte Attribute von MF / PrK.KONN.ENC2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'0D' = 13	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>algorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] { rsaDecipherOaep, rsaDecipherPKCS1_V1_5	

	}	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	Identisch zu PrK.KONN.ENC.R2048	



Hinweis 51: (Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

5.3.20.8 MF / PrK.KONN.ENC.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.

Er unterstützt das Entschlüsseln von Daten. Er ist dafür vorgesehen, die Schlüssel PrK.KONN.ENC.R2048 bzw. PrK.KONN.ENC2.R2048 nach Ablauf von deren Nutzungszeit abzulösen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

Card-G2-A_3345 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

PrK.KONN.ENC.R3072 MUSS die in Tab_gSMC-K_ObjSys_201 dargestellten Attribute besitzen.

Tabelle 40: Tab_gSMC-K_ObjSys_201 Initialisierte Attribute von MF / PrK.KONN.ENC.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'0F' = 15	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>algorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] { rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	Identisch zu PrK.KONN.ENC.R2048	



5.3.20.9 MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.

Er unterstützt das Signieren und das Entschlüsseln von Daten. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ Card-G2-A_3372 K Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

PrK.KONN.TLS.R2048 MUSS die in Tab_gSMC-K_ObjSys_202 dargestellten Attribute besitzen.

Tabelle 41: Tab_gSMC-K_ObjSys_202 Initialisierte Attribute von MF / PrK.KONN.TLS.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'10' = 16	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, signPKCS1_V1_5, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASY- METRIC KEY PAIR P1='C0' oder P1='C4'	PWD(PIN.Pers)	
GENERATE ASY- METRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	OR PWD(PIN.AK) PWD(PIN.NK)	

	OR PWD(PIN.SAK)	
PSO Decipher	OR PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK)	
TERMINATE	PWD(PIN.Pers)	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingungen	Bemerkungen
alle	Herstellerspezifisch	Siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingungen	Bemerkungen
Alle	NEVER	



Hinweis 52: (Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

☒ Card-G2-A_3376 K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Bei der Personalisierung von PrK.KONN.TLS.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_203 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 42: Tab_gSMC-K_ObjSys_203 Attribute von MF / PrK.KONN.TLS.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	true	



5.3.20.10 MF / PrK.KONN.TLS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.

Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, den Schlüssel PrK.KONN.TLS.R2048 nach Ablauf von dessen Nutzungszeit abzulösen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3377 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS2.R2048**
(Option_Erweiterung_herstellerspezifische_Schlüssel_01)

PrK.KONN.TLS2.R2048 MUSS die in Tab_gSMC-K_ObjSys_204 dargestellten Attribute besitzen.

Tabelle 43: Tab_gSMC-K_ObjSys_204 Initialisierte Attribute von MF / PrK.KONN.TLS2.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'02' = 2	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>algorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, signPKCS1_V1_5, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	Identisch zu PrK.KONN.TLS.R2048	



5.3.20.11 MF / PrK.KONN.TLS.R3072
(Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerepezifischen Zwecken.

Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, die Schlüssel PrK.KONN.TLS.R2048 bzw. PrK.KONN.TLS2.R2048 nach Ablauf ihrer Nutzungszeit abzulösen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3378 K_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R3072**
(Option_Erweiterung_herstellerspezifische_Schlüssel_01)

PrK.KONN.TLS.R3072 MUSS die in Tab_gSMC-K_ObjSys_205 dargestellten Attribute besitzen.

Tabelle 44: Tab_gSMC-K_ObjSys_205 Initialisierte Attribute von MF / PrK.KONN.TLS.R3072

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'15' = 21	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, signPKCS1_V1_5, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	Identisch zu PrK.KONN.TLS.R2048	



5.3.20.12 MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Diese Datei dient herstellereigenen Zwecken. Sie kann einen öffentlichen Schlüssel des Konnektorherstellers enthalten. Er kann vom Konnektor ausgelesen werden, um extern erhaltene Informationen hinsichtlich ihrer Integrität zu verifizieren.

☒ Card-G2-A_3379 K_Initialisierung: Initialisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

EF.PuK.KONN.SIG.R4096 MUSS die in Tab_gSMC-K_ObjSys_206 dargestellten Attribute besitzen.

Tabelle 45: Tab_gSMC-K_ObjSys_206 Initialisierte Attribute von MF / EF.PuK.KONN.SIG.R4096

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 16'	
shortFileIdentifier	-	
numberOfOctet	'0210' Oktett = 528 Oktett	
positionLogicalEndOfFile	Wildcard	wird personalisiert

<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	Wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
<i>Zugriffsart</i>	<i>Zugriffsbedingung</i>	<i>Bemerkung</i>
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	AUT_CMS OR AUT_CUP	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
<i>Zugriffsart</i>	<i>Zugriffsbedingungen</i>	<i>Bemerkungen</i>
alle	Herstellerspezifisch	Siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
<i>Zugriffsart</i>	<i>Zugriffsbedingungen</i>	<i>Bemerkungen</i>
Alle	NEVER	



Hinweis 53: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

☒ Card-G2-A_3380 K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Wenn EF.PuK.KONN.SIG.R4096 personalisiert wird, MÜSSEN die in Tab_gSMC-K_ObjSys_207 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 46: Tab_gSMC-K_ObjSys_207 Attribute von MF / EF.PuK.KONN.SIG.R4096

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette	
<i>body</i>	Öffentlicher Schlüssel des Konnektorherstellers mit Moduluslänge 4096 Bit codiert gemäß [PKCS#1v2.1#A.1.1]	
<i>body</i> Option_Erstellung_von_Testkarten	Öffentlicher Schlüssel des Konnektorherstellers mit Moduluslänge 4096 Bit codiert gemäß [PKCS#1v2.1#A.1.1]	



5.3.20.13 MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.

Er unterstützt das Signieren und das Entschlüsseln von Daten.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3381 K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)**

PrK.SDS.R2048 MUSS die in Tab_gSMC-K_ObjSys_208 dargestellten Attribute besitzen.

Tabelle 47: Tab_gSMC-K_ObjSys_208 Initialisierte Attribute von MF / PrK.SDS.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'16' = 22	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, signPKCS1_V1_5, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM-METRIC KEY PAIR P1='C0' oder P1='C4'	PWD(PIN.Pers)	
GENERATE ASYM-METRIC KEY PAIR P1='81'	ALWAYS	

PSO CompDigSig	PWD(PIN.NK)	
PSO Decipher	PWD(PIN.NK)	
PSO Transcipher	PWD(PIN.NK)	
TERMINATE	PWD(PIN.Pers)	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingungen	Bemerkungen
Alle	Herstellerspezifisch	Siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingungen	Bemerkungen
Alle	NEVER	



Hinweis 54: (Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

☒ Card-G2-A_3382 K_Personalisierung: Personalisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Bei der Personalisierung von PrK.SDS.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_209 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 48: Tab_gSMC-K_ObjSys_209 Attribute von MF / PrK.SDS.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	true	



5.3.20.14 MF / PrK.SDS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, den Schlüssel PrK.SDS.R2048 nach Ablauf von dessen Nutzungszeit abzulösen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ Card-G2-A_3383 K_Initialisierung: Initialisierte Attribute von MF / PrK.SDS2.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

PrK.SDS2.R2048 MUSS die in Tab_gSMC-K_ObjSys_210 dargestellten Attribute besitzen.

Tabelle 49: Tab_gSMC-K_ObjSys_210 Initialisierte Attribute von MF / PrK.SDS2.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'19' = 25	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, signPKCS1_V1_5, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	Identisch zu PrK.SDS.R2048	



5.3.20.15 MF / PrK.SDS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, die Schlüssel PrK.SDS.R2048 bzw. PrK.SDS2.R2048 nach Ablauf von deren Nutzungszeit abzulösen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ Card-G2-A_3384 K Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R3072 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)

PrK.SDS.R3072 MUSS die in Tab_gSMC-K_ObjSys_211 dargestellten Attribute besitzen.

Tabelle 50: Tab_gSMC-K_ObjSys_211 Initialisierte Attribute von MF / PrK.SDS.R3072

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'1A' = 26	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	

<i>algorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, signPKCS1_V1_5, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	Identisch zu PrK.SDS.R2048	



5.3.20.16 MF / PrK.GP.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Der zugehörige öffentliche Schlüssel ist PuK.GP.R2048 (siehe Kapitel 5.3.20.17). Er lässt sich auch mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2580 K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R2048**

Das Objekt PrK.GP.R2048 MUSS die in Tab_gSMC-K_ObjSys_020 dargestellten Werte besitzen.

Tabelle 39: Tab_gSMC-K_ObjSys_020 Initialisierte Attribute von MF / PrK.GP.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'0C' = 12	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
<i>keyAvailable</i>	WildCard	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS]: { signPSS, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='84' oder P1='80'	PWD(PIN.Pers)	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	

PSO CompDigSig	OR OR	PWD(PIN.AK) PWD(PIN.NK) PWD(PIN.SAK)	
PSO Decipher	OR OR	PWD(PIN.AK) PWD(PIN.NK) PWD(PIN.SAK)	
PSO Transcipher	OR OR	PWD(PIN.AK) PWD(PIN.NK) PWD(PIN.SAK)	
TERMINATE	PWD(PIN.Pers)		
andere	NEVER		
Zugriffsregel für logischen LCS „Operational state (deactivated)“			
Zugriffsart	Zugriffsbedingung		Bemerkung
alle	herstellerspezifisch		siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“			
Zugriffsart	Zugriffsbedingung		Bemerkung
alle	NEVER		



Hinweis (50) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

☒ **Card-G2-A_3401 K_Personalisierung: Personalisierte Attribute von MF / PrK.GP.R2048**

Bei der Personalisierung von PrK.GP.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_101 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 40: Tab_gSMC-K_ObjSys_101 Attribute von MF / PrK.GP.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	true	



5.3.20.17 MF / PuK.GP.R2048

Dieses Objekt enthält den öffentlichen Schlüssel für die Kryptographie mit RSA zu PrK.GP.R2048 (siehe Kapitel 5.3.20.16). Der öffentliche Schlüssel dient der Verschlüsselung von Daten.

☒ **Card-G2-A_2585 K_Initialisierung: Initialisierte Attribute von MF / PuK.GP.R2048**

Das Objekt PuK.GP.R2048 MUSS die in Tab_gSMC-K_ObjSys_027 dargestellten Werte besitzen.

Tabelle 41: Tab_gSMC-K_ObjSys_027 Initialisierte Attribute von MF / PuK.GP.R2048

Attribute	Wert	Bemerkung
Objekttyp	öffentliches RSA Verschlüsselungsobjekt	
<i>keyIdentifier</i>	'00000000000000000000000000000001C'	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
<i>oid</i>	id-RSAES-OAEP = {1.2.840.113549.1.1.7} = '2A864886F70d010107'	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Encipher	ALWAYS	
TERMINATE	PWD(PIN.Pers)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (51) Kommandos, die gemäß [gemSpec_COS#8.6.4.3] mit einem öffentlichen Verschlüsselungsobjekt arbeiten sind: PSO Encipher, TERMINATE

☒ **Card-G2-A_3402 K_Personalisierung: Personalisierte Attribute von MF / PuK.GP.R2048**

Bei der Personalisierung von PuK.GP.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_104 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 42: Tab_gSMC-K_ObjSys_104 Attribute von MF / PuK.GP.R2048

Attribute	Wert	Bemerkung
<i>publicKey</i>	Moduluslänge 2048 Bit	



5.3.20.18 MF / PrK.GP2.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel ist PuK.GP.R2048. Er lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3444 K_Initialisierung: Initialisierte Attribute von MF / PrK.GP2.R2048**

Das Objekt PrK.GP2.R2048 MUSS die in Tab_gSMC-K_ObjSys_153 dargestellten Werte besitzen.

Tabelle 43: Tab_gSMC-K_ObjSys_153 Initialisierte Attribute von MF / PrK.GP2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'0B' = 11	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]: { signPSS, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.GP.R2048	



5.3.20.19 MF / PrK.GP.R3072

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellereigenen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2581 K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R3072**

Das Objekt PrK.GP.R3072 MUSS die in Tab_gSMC-K_ObjSys_021 dargestellten Werte besitzen.

Tabelle 44: Tab_gSMC-K_ObjSys_021 Initialisierte Attribute von MF / PrK.GP.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 3072	
keyIdentifier	'12' = 18	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	

<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS]: { signPSS, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.GP.R2048	



5.3.20.20 MF / PrK.GP.E256

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3446 K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E256**

Das Objekt PrK.GP.E256 MUSS die in Tab_gSMC-K_ObjSys_179 dargestellten Werte besitzen.

Tabelle 45: Tab_gSMC-K_ObjSys_179 Initialisierte Attribute von MF / PrK.GP.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
<i>keyIdentifier</i>	'08' = 8	
<i>privateElcKey</i>	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS]: {elcSharedSecretCalculation, signECDSA }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.GP.R2048	



5.3.20.21 MF / PrK.GP.E384

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungs-

zeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2582 K_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E384**

Das Objekt PrK.GP.E384 MUSS die in Tab_gSMC-K_ObjSys_022 dargestellten Werte besitzen.

Tabelle 46: Tab_gSMC-K_ObjSys_022 Initialisierte Attribute von MF / PrK.GP.E384

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 384	
keyIdentifier	'17' = 23	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]: {elcSharedSecretCalculation, signECDSA }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.GP.R2048	



5.3.21 Sicherheitsanker zum Import von CV-Zertifikaten

In diesem Kapitel wird das öffentliche Signaturprüfobjekt behandelt, das an der Wurzel eines PKI Baumes für CV-Zertifikate steht. Dieses wird auch Sicherheitsanker genannt und dient dem Import von CV-Zertifikaten der zweiten Ebene.

5.3.21.1 MF / PuK.RCA.CS.E256

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie steht. Er wird zur Prüfung von CV-Zertifikaten der zweiten Ebene von Karten der Generation 2 unter Nutzung elliptischer Kryptographie benötigt.

☒ **Card-G2-A_2583 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**

Das Objekt PuK.RCA.CS.E256 MUSS die in Tab_gSMC-K_ObjSys_024 dargestellten Werte besitzen.

Tabelle 47: Tab_gSMC-K_ObjSys_024 Initialisierte Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches Signaturprüfobjekt	
Für Echtkarten MÜSSEN die vier folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die vier folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	E 256 Root-CA-Kennung (5 Bytes) Erweiterung (3 Bytes)	
CHAT	<ul style="list-style-type: none"> OID_{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 07D8' 	siehe Hinweis (54)
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß [gemSpec_CVC_Root#5.4.2]	
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP#4.5]	
Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		
oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
lifeCycleStatus	„Operational state (activated)“	
accessRulesPublic SignatureVerificationObject	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE → AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublic AuthenticationObject	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE → ALWAYS EXTERNAL AUTHENTICATE → ALWAYS GENERAL AUTHENTICATE → ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (55)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (52) Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten sind: PSO Verify Certificate, TERMINATE

Hinweis (53) Während gemäß den Tabellen in [gemSpec_COS#H.4] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten auf ,0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ,1' gesetzt.

Hinweis (54) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.10.

☒ Card-G2-A_3262 K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Bei der Personalisierung von PuK.RCA.CS.E256 für Testkarten MÜSSEN die in Tab_gSMC-K_ObjSys_191 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Wenn die restlichen Attribute von PuK.RCS.CS.E256 mit Wildcard oder Attribute-NotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_gSMC-K_ObjSys_024 personalisiert werden.

Tabelle 48: Tab_gSMC-K_ObjSys_191 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Attribute	Wert	Bemerkung
<i>publicKey</i>	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-CVC-CA	personalisieren gemäß [gemSpec_TK#3.1.2]
<i>keyIdentifier</i>	E 256 Root-CA-Kennung (5 Bytes) Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels	
CHAT	OID _{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 07D8'	
<i>expirationDate</i>	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels	



5.3.22 Asymmetrische Kartenadministration

Die hier beschriebene optionale Variante der Administration der gSMC-K betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-K.

Die Administration einer gSMC-K erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels asymmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels symmetrischer Verfahren werden in 5.3.23 beschrieben.

Voraussetzung für den Aufbau mittels asymmetrischer Verfahren ist, dass sowohl die zu administrierende Karte, als auch das administrierende System über ein asymmetrisches Schlüsselpaar verfügen. Sei (PrK.ICC, PuK.ICC) das Schlüsselpaar der Smart Card und (PrK.Admin, PuK.Admin) das Schlüsselpaar des administrierenden Systems, dann ist es erforderlich, dass die Smart Card PuK.Admin kennt und das administrierende System PuK.ICC kennt.

Während die Schlüsselpaare auf Smart Cards typischerweise kartenindividuell sind, so ist es denkbar, dass mit einem Schlüsselpaar eines administrierenden Systems genau eine, oder mehrere oder alle Smart Cards administriert werden. Das Sicherheitskonzept des administrierenden Systems erscheint die geeignete Stelle zu sein um eine Variante auszuwählen.

5.3.22.1 MF / PuK.RCA.ADMINCMS.CS.E256

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie für die asymmetrische CMS-Authentisierung steht. PuK.RCA.ADMINCMS.CS.E256 wird für den Import weiterer Schlüssel für die elliptische Kryptographie benötigt.

☒ **Card-G2-A_2998 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab_gSMC-K_ObjSys_085 dargestellten Attribute besitzen.

Tabelle 49: Tab_gSMC-K_ObjSys_085 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches Signaturprüfobjekt, ELC 256	
Für Echtkarten MÜSSEN die beiden folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
CHAT	OID _{flags} = oid_cvc_fl_cms flagList = 'FF BFFF FFFF FFFF'	siehe Hinweis (57)
expirationDate	Identisch zu „expirationDate“ von PuK.RCA.CS.E256	
Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	'0000 0000 0000 0013'	
lifeCycleStatus	„Operational state (activated)“	
publicKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Domain-parameter = brainpoolP256r1	wird personalisiert
oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
accessRulesPublicSignatureVerificationObject.	Für alle Life Cycle State und in SE#1 gilt: DELETE --> AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublicAuthenticationObject.	Für alle Life Cycle State und in SE#1 gilt: DELETE --> ALWAYS GENERAL AUTHENTICATE → ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
PSO Verify Certificate	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (58)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (55) Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten sind: PSO Verify Certificate, TERMINATE

Hinweis (56) Während gemäß den Tabellen in [gemSpec_COS#H.4] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ,0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ,1' gesetzt.

Hinweis (57) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

☒ **Card-G2-A_3403 K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

Bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 MÜSSEN die in Tab_gSMC-K_ObjSys_108 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Wenn die restlichen Attribute von PuK.RCA.ADMINCMS.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_gSMC-K_ObjSys_085 personalisiert werden.

Tabelle 50: Tab_gSMC-K_ObjSys_108 Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
<i>publicKey</i>	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Admin-CVC-Root	
<i>publicKey</i> Option_Erstellung_von_Testkarten	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-Admin-CVC-Root	
CHAT	<ul style="list-style-type: none"> ▪ OIDflags = oid_cvc_fl_cms ▪ flagList = 'FF BFFF FFFF FFFF' 	
expirationDate Option_Erstellung_von_Testkarten	Identisch zu „expirationDate“ des personalisierten PuK.RCA.CS.E256	



5.3.23 Symmetrische Kartenadministration

Die hier beschriebene optionale Variante der Administration einer gSMC-K betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-K.

Die Administration einer gSMC-K erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels symmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels asymmetrischer Verfahren werden in 5.3.22 beschrieben.

Voraussetzung für den Aufbau mittels symmetrischer Verfahren ist, dass sowohl die zu administrierende Karte, als auch das administrierende System über denselben symmetrischen Schlüssel verfügen. .

Wenn die symmetrischen Schlüssel (SK.CMS und SK.CUP) für die Authentifizierung des Kartenadministrationssystems genutzt werden, dann MÜSSEN sie kartenindividuell personalisiert werden, so dass mit einem Schlüssel eines administrierenden Systems genau eine gSMC-K administriert werden kann.

Bei der Personalisierung sind nur die Schlüssel zu personalisieren, die tatsächlich benötigt werden.

5.3.23.1 MF /. SK.CMS.AES128

SK.CMS.AES128 (optional) ist der geheime AES-Schlüssel für die Durchführung des Konnektor/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel. Die nachfolgende Tabelle Tab_gSMC-K_ObjSys_030 zeigt die Eigenschaften des Schlüssels.

☒ **Card-G2-A_2588 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128**

Das Objekt SK.CMS.AES128 MUSS die in Tab_gSMC-K_ObjSys_030 dargestellten Werte besitzen.

Tabelle 51: Tab_gSMC-K_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES128

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'14' = 20	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
accessRulesSessionkeys	irrelevant	
Zugriffsregeln		
Zugriffsart	Zugriffsbedingung	Bemerkung

MUTUAL AUTHENTICATE	OR OR PWD(PIN.AK) PWD(PIN.NK) PWD(PIN.SAK)	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (60)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (58) Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GET SECURITY STATUS KEY, INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE, TERMINATE.

Hinweis (59) Das Kommando ist nur vom Inhaber des CMS- bzw. CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

Card-G2-A_3404 K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES128 die in Tab_gSMC-K_ObjSys_110 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 52: Tab_gSMC-K_ObjSys_110 Attribute von MF / SK.CMS.AES128

Attribute	Wert	Bemerkung
encKey	Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4]	
macKey	Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4]	



5.3.23.2 MF / SK.CMS.AES256

SK.CMS.AES256 ist der geheime AES-Schlüssel für die Durchführung des Konnektor/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel. Die nachfolgende Tabelle Tab_gSMC-K_ObjSys_031 zeigt die Eigenschaften des Schlüssels.

Card-G2-A_2589 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256

Das Objekt SK.CMS.AES256 MUSS die in Tab_gSMC-K_ObjSys_031 dargestellten Werte besitzen.

Tabelle 53: Tab_gSMC-K_ObjSys_031 Initialisierte Attribute von MF / SK.CMS.AES256

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	'18' = 24	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
accessRulesSessionkeys	irrelevant	
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	



Hinweis (60) Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GET SECURITY STATUS KEY, INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE, TERMINATE.

☒ **Card-G2-A_3405 K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES256 die in Tab_gSMC-K_ObjSys_111 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 54: Tab_gSMC-K_ObjSys_111 Attribute von MF / SK.CMS.AES256

Attribute	Wert	Bemerkung
encKey	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	
macKey	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	



5.3.23.3 MF / SK.CUP.AES128

Dieser AES-Schlüssel mit 128 bit Schlüssellänge wird benötigt, um dem CUPS administrative Zugriffe auf die gSMC-K bezüglich der Zertifikate zu erlauben.

☒ **Card-G2-A_3206 K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128**

SK.CUP.AES128 MUSS die in Tab_gSMC-K_ObjSys_154 dargestellten Initialisierten Attribute besitzen.

Tabelle 55: Tab_gSMC-K_ObjSys_154 Initialisierte Attribute von MF / SK.CUP.AES128

Attribute	Wert	Bemerkung
Objektyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'03' = 3	
lifeCycleStatus	„Operational state (activated)“	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
accessRulesSession-keys	irrelevant	
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	



☒ Card-G2-A_3447 K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CUP.AES128 die in Tab_gSMC-K_ObjSys_155 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 56: Tab_gSMC-K_ObjSys_155 Personalisierte Attribute von MF / SK.CUP.AES128

Attribute	Wert	Bemerkung
encKey	Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4]	
macKey	Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4]	



5.3.23.4 MF / SK.CUP.AES256

Dieser AES-Schlüssel mit 256 bit Schlüssellänge wird benötigt, um dem CUPS administrative Zugriffe auf die gSMC-K bezüglich der Zertifikate zu erlauben.

☒ Card-G2-A_3448 K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256

SK.CUP.AES256 MUSS die in Tab_gSMC-K_ObjSys_156 dargestellten Initialisierten Attribute besitzen.

Tabelle 57: Tab_gSMC-K_ObjSys_156 Initialisierte Attribute von MF / SK.CUP.AES256

Attribute	Wert	Bemerkung
Objektyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	'04' = 4	
lifeCycleStatus	„Operational state (activated)“	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
accessRulesSession-keys	irrelevant	
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	



☒ Card-G2-A_3449 K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CUP.AES256 die in Tab_gSMC-K_ObjSys_157 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 58: Tab_gSMC-K_ObjSys_157 Personalisierte Attribute von MF / SK.CUP.AES256

Attribute	Wert	Bemerkung
encKey	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	
macKey	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	



5.4 MF / DF.AK

Die Anwendung DF.AK enthält kryptographische Objekte des Anwendungskonnektors.

Der in dieser Anwendung enthaltene Schlüssel PrK.AK.AUT.R2048 unterstützt den Aufbau eines TLS-Kanals zwischen dem Anwendungskonnektor und dem Primärsystem. Daneben enthält die Anwendung das Zertifikat EF.C.AK.AUT.R2048, das den zugehörigen öffentlichen Schlüssel PuK.AK.AUT.R2048 enthält. Es wird als nicht erforderlich angesehen, dass die Anwendung auch Zertifikate höherer Ebenen enthält.

Mit dem Schlüssel PrK.AK.CA_PS.R2048 können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden.

Für die genannten Schlüssel sind die Nachfolger PrK.AK.AUT2.R2048 und PrK.AK.AUT.XXXX bzw. PrK.AK.CA_PS2.R2048 und PrK.AK.CA_PS.XXXX in der Anwendung enthalten, mit jeweils XXXX \in {R3072, E256, E384}. Als Nachfolger für EF.C.AK.AUT.R2048 dient die Datei EF.C.AK.AUT2.XXXX.

☒ **Card-G2-A_2592 K_Initialisierung: Initialisierte Attribute von MF / DF.AK**

Das Objekt DF.AK MUSS die in Tab_gSMC-K_ObjSys_032 dargestellten Werte besitzen.

Tabelle 59: Tab_gSMC-K_ObjSys_032 Initialisierte Attribute von MF / DF.AK

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
<i>applicationIdentifier</i>	'D276 0001 4402'	
<i>fileIdentifier</i>	herstellerspezifisch	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	PWD(PIN.Pers)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (63)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)



Hinweis (61) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (62) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.4 im Allgemeinen irrelevant.5.4

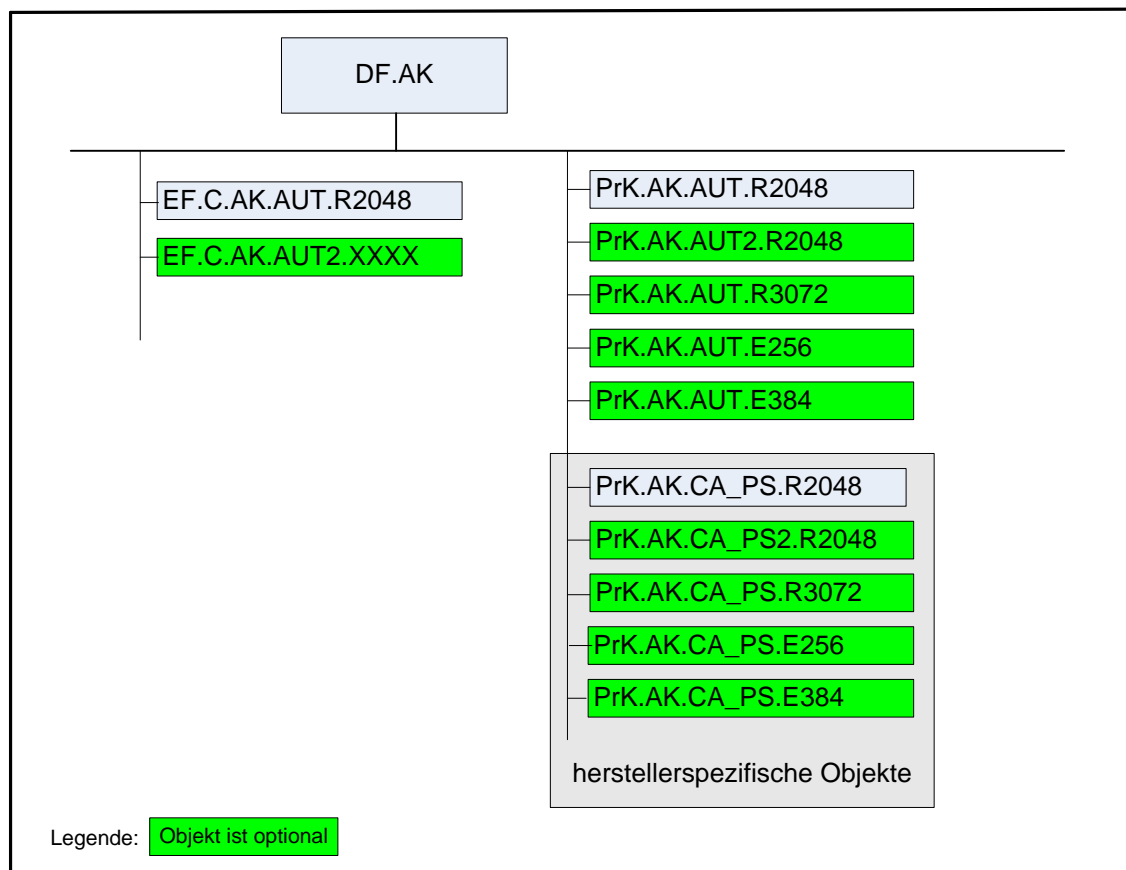


Abbildung 2: Abb_gSMC-K_ObjSys_002 Dateistruktur der Anwendung DF.AK

5.4.1 MF /DF.AK/ EF.C.AK.AUT.R2048

Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.AK.AUT.2048 zu PrK.AK.AUT.R2048 (siehe Kapitel 5.4.2) aufzunehmen.

☒ **Card-G2-A_2595 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048**

Das Objekt EF.C.AK.AUT.R2048 MUSS die in Tab_gSMC-K_ObjSys_034 dargestellten Werte besitzen.

Tabelle 60: Tab_gSMC-K_ObjSys_034 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C5 03'	
<i>shortFileIdentifier</i>	'03' = 3	
<i>numberOfOctet</i>	'08 02' Oktett = 2.050	
<i>positionLogicalEndOfFile</i>	Wildcard	wird personalisiert

<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (65)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (65)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (63)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (63)



Hinweis (63) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (64) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

Card-G2-A_3450 K_Personalisierung: Personalisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048

Bei der Personalisierung von EF.C.AK.AUT.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_158 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 61: Tab_gSMC-K_ObjSys_158 Attribute von MF / DF.AK / EF.C.AK.AUT.R2048

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette	
<i>body</i>	C.AK.AUT.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.AK.AUT.R2048	



5.4.2 MF / DF.AK / PrK.AK.AUT.R2048

Dieser Schlüssel ermöglicht den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem. Der öffentliche Teil zu diesem privaten Schlüssel ist in EF.C.AK.AUT.R2048 enthalten (siehe Kapitel 5.4.1).

Aus Sicht des Primärsystems handelt der Anwendungskonnektor beim Aufbau der TLS-Verbindung als Server. Gemäß [TLS#8.1.1] wird dabei für bestimmte CipherSuites wäh-

rend der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2.2 durchgeführt

☒ **Card-G2-A_2599 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048**

Das Objekt PrK.AK.AUT.R2048 MUSS die in Tab_gSMC-K_ObjSys_036 dargestellten Werte besitzen.

Tabelle 62: Tab_gSMC-K_ObjSys_036 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt RSA 2048	
keyIdentifier	'03' = 3	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	rsaDecipherOaep, rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, signPSS	siehe Hinweis (69) Hinweis (70)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsart		Bemerkung
DEACTIVATE	AUT_CMS OR AUT_CUP	
ACTIVATE	ALWAYS AUT_CMS OR AUT_CUP	herstellerspezifisch ist eine der beiden Varianten erlaubt
GENERATE ASYMMETRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	Siehe Hinweis (68)
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	PWD(PIN.AK)	
PSO Decipher	PWD(PIN.AK)	
DELETE	PWD(PIN.AK)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE	AUT_CMS OR AUT_CUP	
DEACTIVATE	NEVER AUT_CMS OR AUT_CUP	herstellerspezifisch ist eine der beiden Varianten erlaubt
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (65) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (66) Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt

Hinweis (67) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

Hinweis (68) Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.

Hinweis (69) Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

☒ **Card-G2-A_3406 K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048**

Bei der Personalisierung von PrK.AK.AUT.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_113 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 63: Tab_gSMC-K_ObjSys_113 Attribute von MF / DF.AK / PrK.AK.AUT.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.4.3 MF /DF.AK/ EF.C.AK.AUT2.XXXX

Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.AK.AUT.XXXX zu PrK.AK.AUT.XXXX (XXXX aus der Menge {R2048, R3072, E256, E384}) nach Ablauf der Nutzungszeit des Schlüssels PrK.AK.AUT.R2048 aufzunehmen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3451 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT2.XXXX**

Das Objekt EF.C.AK.AUT2.XXXX MUSS bei Ausgabe der Karte mit den in Tab_gSMC-K_ObjSys_159 gezeigten Eigenschaften angelegt werden.

Tabelle 64: Tab_gSMC-K_ObjSys_159 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT2.XXXX

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C5 04'	
<i>shortFileIdentifier</i>	'04' = 4	
<i>numberOfOctet</i>	'08 02' Oktett = 2.050	
<i>positionLogicalEndOfFile</i>	'0'	

<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird später nachgeladen
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (72)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (72)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (63)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (63)



Hinweis (70) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (71) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

5.4.4 MF / DF.AK / PrK.AK.AUT2.R2048

Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT2.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Card-G2-A_2597 K_externe Welt: Erstellung des zu PrK.AK.AUT2.R2048 gehörenden Zertifikats

Nach Auslesen des öffentlichen Schlüssels mit Generate Asymmetric Key Pair MUSS das dazugehörige Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden.

Card-G2-A_3452 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048

Das Objekt PrK.AK.AUT2.R2048 MUSS die in Tab_gSMC-K_ObjSys_187 dargestellten Werte besitzen.

Tabelle 65: Tab_gSMC-K_ObjSys_187 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt RSA 2048	
keyIdentifier	'04' = 4	
privateKey	Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	rsaDecipherOaep, rsaDecipherPKCS1_V1_5, signPKCS1_V1_5, signPSS	siehe Hinweis (69) Hinweis (70)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.AK.AUT.R2048	



5.4.5 MF / DF.AK / PrK.AK.AUT.R3072

Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3253 K_externe Welt: Erstellung der zu PrK.AK.AUT.R3072 gehörenden Zertifikate**

Nach Auslesen des öffentlichen Schlüssels mit GENERATE ASYMMETRIC KEY PAIR MUSS das dazugehörige Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden. ☒

☒ **Card-G2-A_3254 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072**

Das Objekt PrK.AK.AUT.R3072 MUSS die in Tab_gSMC-K_ObjSys_160 dargestellten Werte besitzen.

Tabelle 66: Tab_gSMC-K_ObjSys_160 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt R3072	
keyIdentifier	05' = 5	
privateKey	Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	

<i>listAlgorithmIdentifier</i>	rsaDecipherOaep, rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, signPSS	siehe Hinweis (69) Hinweis (70)
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.AK.AUT.R2048	



5.4.6 MF / DF.AK / PrK.AK.AUT.E256

Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3255 K_externe Welt: Erstellung der zu PrK.AK.AUT.E256 gehörenden Zertifikate**

Nach Auslesen des öffentlichen Schlüssels mit GENERATE ASYMMETRIC KEY PAIR MUSS das dazugehörige Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden. ☒

☒ **Card-G2-A_3256 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E256**

Das Objekt PrK.AK.AUT.E256 MUSS die in Tab_gSMC-K_ObjSys_161 dargestellten Werte besitzen.

Tabelle 67: Tab_gSMC-K_ObjSys_161 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E256

Attribute	Wert	Bemerkung
Objektyp	privates ELC Schlüsselobjekt E256	
<i>keyIdentifier</i>	'07' = 7	
<i>privateElcKey</i>	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	elcSharedSecretCalculation, signECDSA	siehe Hinweis (69) Hinweis (70)
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.AK.AUT.R2048	



5.4.7 MF / DF.AK / PrK.AK.AUT.E384

Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3257 K_externe Welt: Erstellung der zu PrK.AK.AUT.E384 gehörenden Zertifikate**

Nach Auslesen des öffentlichen Schlüssels mit GENERATE ASYMMETRIC KEY PAIR MUSS das dazugehörige Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden. ☒

☒ **Card-G2-A_3258 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384**

Das Objekt PrK.AK.AUT.E384 MUSS die in Tab_gSMC-K_ObjSys_162 dargestellten Werte besitzen.

Tabelle 68: Tab_gSMC-K_ObjSys_162 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Schlüsselobjekt E384	
keyIdentifier	'06' = 6	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	elcSharedSecretCalculation, signECDSA	siehe Hinweis (69) Hinweis (70)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.AK.AUT.R2048	

☒

5.4.8 MF / DF.AK / PrK.AK.CA_PS.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Client-Systemen signiert werden. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2600 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048**

Das Objekt PrK.AK.CA_PS.R2048 MUSS die in Tab_gSMC-K_ObjSys_037 dargestellten Werte besitzen.

Tabelle 69: Tab_gSMC-K_ObjSys_037 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'08' = 8	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='84' oder P1='80'	PWD(PIN.AK)	Siehe Hinweis (74)
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	PWD(PIN.AK)	
TERMINATE	PWD(PIN.AK)	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (63)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (72) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (73) Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt

☒ **Card-G2-A_3407 K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048**

Bei der Personalisierung von PrK.AK.CA_PS.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_114 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 70: Tab_gSMC-K_ObjSys_114 Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.4.9 MF / DF.AK / PrK.AK.CA_PS2.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ Card-G2-A_3408 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS2.R2048

Das Objekt PrK.AK.CA_PS2.R2048 MUSS die in Tab_gSMC-K_ObjSys_180 dargestellten Werte besitzen.

Tabelle 71: Tab_gSMC-K_ObjSys_180 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
<i>keyIdentifier</i>	'09' = 9	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.AK.CA_PS.R2048	



5.4.10 MF / DF.AK / PrK.AK.CA_PS.R3072

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zuge-

hörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2601 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R3072**

Das Objekt PrK.AK.CA_PS.R3072 MUSS die in Tab_gSMC-K_ObjSys_038 dargestellten Werte besitzen.

Tabelle 72: Tab_gSMC-K_ObjSys_038 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R3072

Attribute	Wert	Bemerkung
Objektyp	privates RSA Schlüsselobjekt	
keyIdentifier	'0D' = 13	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.AK.CA_PS.R2048	



5.4.11 MF / DF.AK / PrK.AK.CA_PS.E256

Dieser private Schlüssel für die Kryptographie mit ELC dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmateri als gewählt wird, wird zu einem späteren Zeitpunkt getroffen.. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3409 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E256**

Das Objekt PrK.AK.CA_PS.E256 MUSS die in Tab_gSMC-K_ObjSys_181 dargestellten Werte besitzen.

Tabelle 73: Tab_gSMC-K_ObjSys_181 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E256

Attribute	Wert	Bemerkung
Objektyp	privates ELC Schlüsselobjekt	
keyIdentifier	'10' = 16	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asym-

		metric Key Pair erzeugt
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] {signECDSA }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.AK.CA_PS.R2048	



Hinweis (74) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.4.12 MF / DF.AK / PrK.AK.CA_PS.E384

Dieser private Schlüssel für die Kryptographie mit ELC dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2602 K_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E384**

Das Objekt PrK.AK.CA_PS.E384 MUSS die in Tab_gSMC-K_ObjSys_039 dargestellten Werte besitzen.

Tabelle 74: Tab_gSMC-K_ObjSys_039 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Schlüsselobjekt	
<i>keyIdentifier</i>	'11' = 17	
<i>privateElcKey</i>	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] {signECDSA }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		

accessRules	identisch zu PrK.AK.CA_PS.R2048	
-------------	---------------------------------	--



Hinweis (75) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.5 MF / DF.NK

Die Anwendung DF.NK enthält kryptographische Objekte des Netzkonnektors.

Der in dieser Anwendung enthaltene Schlüssel PrK.NK.VPN (in der jeweils aktuellen Ausprägung) unterstützt den Aufbau einer VPN-Verbindung zum VPN-Konzentrator.

Diese Anwendung enthält neben den vorgenannten privaten Schlüsseln pro privatem Schlüssel ein Zertifikat mit dem öffentlichen Schlüssel zum jeweiligen privaten Schlüssel. Es wird als nicht erforderlich angesehen, dass die Anwendung auch Zertifikate höherer Ebenen enthält.

☒ Card-G2-A_2605 K_Initialisierung: Initialisierte Attribute von MF / DF.NK

Das Objekt DF.NK MUSS die in Tab_gSMC-K_ObjSys_040 dargestellten Werte besitzen.

Tabelle 75: Tab_gSMC-K_ObjSys_040 Initialisierte Attribute von MF / DF.NK

Attribute	Wert	Bemerkung
Objektyp	Ordner	
applicationIdentifier	'D276 0001 4403'	
fileIdentifier	'AA00'	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	PWD(PIN.Pers)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (76) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (77) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.5 im Allgemeinen irrelevant.

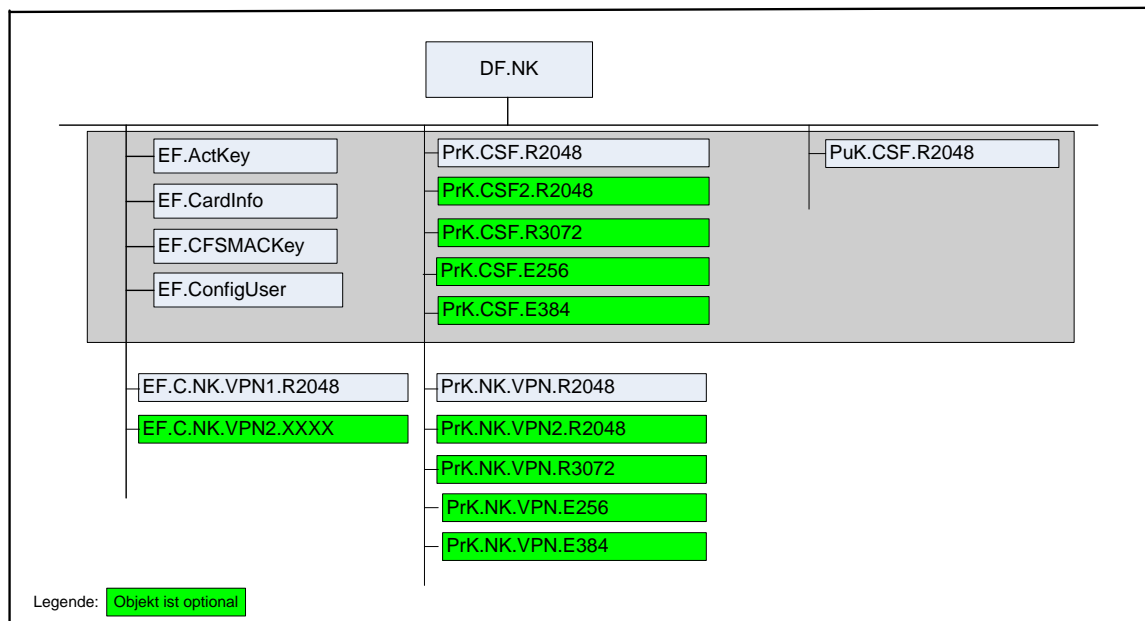


Abbildung 3: Abb_gSMC-K_ObjSys_003 Dateistruktur der Anwendung DF.NK

5.5.1 MF / DF.NK / EF.ActKey

Diese Datei ist in der Lage, Informationen über den aktuell zu verwendenden Schlüssel zu speichern. Inhalt und Verwendung dieser Datei sind herstellerspezifisch.

Card-G2-A_2606 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ActKey

Das Objekt EF.ActKey MUSS die in Tab_gSMC-K_ObjSys_041 dargestellten Werte besitzen.

Tabelle 76: Tab_gSMC-K_ObjSys_041 Initialisierte Attribute von MF / DF.NK / EF.ActKey

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'FE 05'	
shortFileIdentifier	–	
numberOfOctet	'000B' Oktett = 11 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung

READ BINARY	PWD(PIN.NK)	siehe Hinweis (80)
ERASE BINARY	PWD(PIN.NK)	siehe Hinweis (80)
SET LOGICAL EOF		
UPDATE BINARY		
WRITE BINARY		
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (78) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (79) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

5.5.2 MF / DF.NK / EF.CardInfo

Diese Datei ist in der Lage Kartenparameter des Netzkonnektors zu speichern. Inhalt und Verwendung dieser Datei ist herstellerspezifisch.

☒ **Card-G2-A_2607 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CardInfo**

Das Objekt EF.CardInfo MUSS die in Tab_gSMC-K_ObjSys_042 dargestellten Werte besitzen.

Tabelle 77: Tab_gSMC-K_ObjSys_042 Initialisierte Attribute von MF / DF.NK / EF.CardInfo

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'A2 00'	
shortFileIdentifier	–	
numberOfOctet	'000A' Oktett = 10 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY	PWD(PIN.NK)	
SET LOGICAL EOF		
UPDATE BINARY		
WRITE BINARY		
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (80) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (81)

5.5.3 MF / DF.NK / EF.CFSMACKey

Diese Datei ist in der Lage Informationen über das Dateisystem des Netzkonnektors zu speichern. Inhalt und Verwendung dieser Datei ist herstellerspezifisch.

Card-G2-A_2608 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey

Das Objekt EF.CFSMACKey MUSS die in Tab_gSMC-K_ObjSys_043 dargestellten Werte besitzen.

Tabelle 78: Tab_gSMC-K_ObjSys_043 Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'A1 07'	
shortFileIdentifier	–	
numberOfOctet	'0034' Oktett = 52 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	PWD(PIN.NK)	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.NK)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)

Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (82) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (83)

5.5.4 MF / DF.NK / EF.ConfigUser

Diese Datei ist in der Lage Konfigurationsinformationen zu speichern. Inhalt und Verwendung dieser Datei ist herstellerspezifisch.

☒ **Card-G2-A_2609 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ConfigUser**

Das Objekt EF.ConfigUser MUSS die in Tab_gSMC-K_ObjSys_044 dargestellten Werte besitzen.

Tabelle 79: Tab_gSMC-K_ObjSys_044 Initialisierte Attribute von MF / DF.NK / EF.ConfigUser

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'A1 00'	
<i>shortFileIdentifier</i>	–	
<i>numberOfOctet</i>	'00C8' Oktett = 200 Oktett	
<i>positionLogicalEndOfFile</i>	'0'	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	PWD(PIN.NK)	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.NK)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (84) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (85)

5.5.5 MF /DF.NK/ EF.C.NK.VPN.R2048

Diese Zertifikatsdatei enthält das Zertifikat mit dem öffentlichen Schlüssel zu PrK.NK.VPN.R2048 (siehe Kapitel 5.5.6).

☒ **Card-G2-A_2612 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048**

Das Objekt EF.C.NK.VPN.R2048 MUSS die in Tab_gSMC-K_ObjSys_046 dargestellten Werte besitzen.

Tabelle 80: Tab_gSMC-K_ObjSys_046 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'C5 05'	
shortFileIdentifier	'05' = 5	
numberOfOctet	'08 02' Oktett = 2.050 Oktett	
positionLogicalEndOfFile	Wildcard	wird personalisiert
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (88)
READ BINARY	PWD(PIN.NK)	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (88)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (86) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (87) Das Kommando ist nur vom Inhaber des CMS- bzw. CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

☒ **Card-G2-A_3410 K_Personalisierung: Personalisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048**

Die Objekte EF.C.NK.VPN.R2048 MÜSSEN gemäß der in Tab_gSMC-K_ObjSys_121 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 81: Tab_gSMC-K_ObjSys_121 Attribute von MF / DF.NK / EF.C.NK.VPN.R2048

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette	
<i>body</i>	C.NK.VPN.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.NK.VPN.R2048	



5.5.6 MF / DF.NK / PrK.NK.VPN.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient der Verbindung des Netzkonnektors mit dem VPN-Gateway. Der zugehörige öffentliche Schlüssel PuK.NK.VPN.R2048 ist im Zertifikat EF.C.NK.VPN.R2048 enthalten.

☒ **Card-G2-A_3259 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048**

Das Objekt PrK.NK.VPN.R2048 MUSS die in Tab_gSMC-K_ObjSys_188 dargestellten Werte besitzen.

Tabelle 82: Tab_gSMC-K_ObjSys_188 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
<i>keyIdentifier</i>	'05' = 5	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
<i>keyAvailable</i>	Wildcard	
<i>listAlgorithmIdentifier</i>	rsaDecipherPKCS1_V1_5, signPKCS1_V1_5, rsaDecipherOaep signPSS	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DEACTIVATE	AUT_CMS OR AUT_CUP	Siehe Hinweis (90)

ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
GENERATE ASYMMETRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	Siehe Hinweis (90)
PSO CompDigSig	PWD(PIN.NK)	
PSO Decipher	PWD(PIN.NK)	
DELETE	PWD(PIN.NK) OR AUT_CMS OR AUT_CUP	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE	AUT_CMS OR AUT_CUP	
DEACTIVATE	NEVER	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (88) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (89) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

Card-G2-A_3411 K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048

Bei der Personalisierung von PrK.NK.VPN.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_163 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 83: Tab_gSMC-K_ObjSys_163 Attribute von MF / DF.NK / PrK.NK.VPN.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.5.7 MF /DF.NK/ EF.C.NK.VPN2.XXXX

Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.NK.VPN.XXXX zu PrK.NK.VPN.XXXX (XXXX aus der Menge {R2048, R3072, E256, E384}) nach Ablauf der Nutzungszeit des Schlüssels PrK.AK.AUT.R2048 aufzunehmen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3260 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN2.XXXX**

Das Objekt EF.C.NK.VPN2.XXXX MUSS bei Ausgabe der Karte mit den in Tab_gSMC-K_ObjSys_189 dargestellten Werte angelegt werden.

Tabelle 84: Tab_gSMC-K_ObjSys_189 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN2.XXXX

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'C5 06'	
shortFileIdentifier	'06' = 6	
numberOfOctet	'08 02' Oktett = 2.050 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird später nachgeladen
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (92)
READ BINARY	PWD(PIN.NK)	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (92)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)



Hinweis (90) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (91) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

5.5.8 MF / DF.NK / PrK.NK.VPN2.R2048

Dieser private Schlüssel für die Kryptographie mit RSA wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörnde öffentliche Schlüssel PuK.NK.VPN2.R2048 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.

☒ **Card-G2-A_3412 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048**

Das Objekt PrK.NK.VPN2.R2048 MUSS die in Tab_gSMC-K_ObjSys_164 dargestellten Werte besitzen.

Tabelle 85: Tab_gSMC-K_ObjSys_164 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'06' = 6	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	rsaDecipherPKCS1_V1_5, rsaDecipherOaep signPKCS1_V1_5, signPSS	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.NK.VPN.R2048	



5.5.9 MF / DF.NK / PrK.NK.VPN.R3072

Dieser private Schlüssel für die Kryptographie mit RSA wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörnde öffentliche Schlüssel PuK.NK.VPN2.R3072 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.

☒ **Card-G2-A_3413 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072**

Das Objekt PrK.NK.VPN.R3072 MUSS die in Tab_gSMC-K_ObjSys_190 dargestellten Werte besitzen.

Tabelle 86: Tab_gSMC-K_ObjSys_190 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 3072	
keyIdentifier	'07' = 7	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	rsaDecipherPKCS1_V1_5, rsaDecipherOaep signPKCS1_V1_5, signPSS	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.NK.VPN.R2048	



5.5.10 MF / DF.NK / PrK.NK.VPN.E256

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel PuK.NK.VPN2.E256 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.

☒ **Card-G2-A_3414 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E256**

Das Objekt PrK.NK.VPN.E256 MUSS die in Tab_gSMC-K_ObjSys_165 dargestellten Werte besitzen.

Tabelle 87: Tab_gSMC-K_ObjSys_165 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'0A' = 10	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt

<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	elcSharedSecretCalculation, signECDSA	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.NK.VPN.R2048	



5.5.11 MF / DF.NK / PrK.NK.VPN.E384

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel PuK.NK.VPN2.E384 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.

☒ **Card-G2-A_3415 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384**

Das Objekt PrK.NK.VPN.E384 MUSS die in Tab_gSMC-K_ObjSys_166 dargestellten Werte besitzen.

Tabelle 88: Tab_gSMC-K_ObjSys_166 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 384	
<i>keyIdentifier</i>	'08' = 8	
<i>privateElcKey</i>	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	elcSharedSecretCalculation, signECDSA	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.NK.VPN.R2048	



5.5.12 MF / DF.NK / PrK.CFS.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Der zugehörige öffentliche Schlüssel ist PuK.CFS.R2048 (siehe Kapitel 5.5.13). Er lässt sich auch mittels

des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2617 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048**

Das Objekt PrK.CFS.R2048 MUSS die in Tab_gSMC-K_ObjSys_049 dargestellten Werte besitzen.

Tabelle 89: Tab_gSMC-K_ObjSys_049 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048

Attribute	Wert	Bemerkung
Objektyp	privates RSA-Schlüsselobjekt	
keyIdentifier	'09' = 9	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='84' oder P1='80'	PWD(PIN.NK)	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	PWD(PIN.NK)	
PSO Decipher	PWD(PIN.NK)	
PSO Transcipher	PWD(PIN.NK)	
TERMINATE	PWD(PIN.NK)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (78)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (92) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

☒ **Card-G2-A_3416 K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.CFS.R2048**

Bei der Personalisierung von PrK.CFS.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_123 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 90: Tab_gSMC-K_ObjSys_123 Attribute von MF / DF.NK / PrK.CFS.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.5.13 MF / DF.NK / PuK.CFS.R2048

Dieses Objekt enthält den öffentlichen Schlüssel für die Kryptographie mit RSA zu PrK.CFS.R2048 (siehe Kapitel 5.5.12). Der öffentliche Schlüssel dient der Verschlüsselung von Daten.

☒ **Card-G2-A_2623 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048**

Das Objekt PuK.CFS.R2048 MUSS die in Tab_gSMC-K_ObjSys_055 dargestellten Werte besitzen.

Tabelle 91: Tab_gSMC-K_ObjSys_055 Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048

Attribute	Wert	Bemerkung
Objektyp	öffentliches RSA Verschlüsselungsobjekt	
keyIdentifier	'00000000000000000000000019'	
publicKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
oid	Id-rsaEncipherOaep	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Encipher	ALWAYS	
TERMINATE	PWD(PIN.NK)	siehe Hinweis (95)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (3)
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (93) Kommandos, die gemäß [gemSpec_COS#8.6.4.3] mit einem öffentlichen Verschlüsselungsobjekt arbeiten sind: PSO Encipher, TERMINATE

Hinweis (94) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.10.

☒ Card-G2-A_3417 K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PuK.CFS.R2048

Bei der Personalisierung von PuK.CFS.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_130 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 92: Tab_gSMC-K_ObjSys_130 Attribute von MF / DF.NK / PuK.CFS.R2048

Attribute	Wert	Bemerkung
<i>publicKey</i>	Moduluslänge 2048 Bit	



5.5.14 MF / DF.NK / PrK.CFS2.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel PuK.CFS2.R2048 lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) aus diesem Objekt auslesen.

☒ Card-G2-A_3418 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048

Das Objekt PrK.CFS2.R2048 MUSS die in Tab_gSMC-K_ObjSys_182 dargestellten Werte besitzen.

Tabelle 93: Tab_gSMC-K_ObjSys_182 Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
<i>keyIdentifier</i>	'0B' = 11	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	

<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.CFS.R2048	



5.5.15 MF / DF.NK / PrK.CFS.R3072

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel PuK.CFS2.R3072 lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) aus diesem Objekt auslesen.

☒ **Card-G2-A_3419 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072**

Das Objekt PrK.CFS.R3072 MUSS die in Tab_gSMC-K_ObjSys_050 dargestellten Werte besitzen.

Tabelle 94: Tab_gSMC-K_ObjSys_050 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 3072	
<i>keyIdentifier</i>	'13' = 19	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] { signPSS, rsaDecipherOaep, rsaDecipherPKCS1_V1_5 signPKCS1_V1_5, }	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.CFS.R2048	



5.5.16 MF / DF.NK / PrK.CFS.E256

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel PuK.CFS2.E256 lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec_COS#14.9.3.4]) aus diesem Objekt auslesen.

☒ **Card-G2-A_3420 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256**

Das Objekt PrK.CFS.E256 MUSS die in Tab_gSMC-K_ObjSys_183 dargestellten Werte besitzen.

Tabelle 95: Tab_gSMC-K_ObjSys_183 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'0C' = 12	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcSharedSecretCalculation, signECDSA}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
accessRules	identisch zu PrK.CFS.R2048	



5.5.17 MF / DF.NK / PrK.CFS.E384

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Der zugehörige öffentliche Schlüssel PuK.CFS2.E384 lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec_COS#14.9.3.4]) aus diesem Objekt auslesen.

☒ **Card-G2-A_3421 K_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384**

Das Objekt PrK.CFS.E384 MUSS die in Tab_gSMC-K_ObjSys_051 dargestellten Werte besitzen.

Tabelle 96: Tab_gSMC-K_ObjSys_051 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 384	
keyIdentifier	'14' = 20	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcSharedSecretCalculation, signECDSA}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
accessRules	identisch zu PrK.CFS.R2048	



5.6 MF / DF.SAK

Die Anwendung DF.SAK enthält kryptographische Objekte der Signaturanwendungskomponente.

Die in dieser Anwendung enthaltenen Schlüssel PrK.SAK.AUT unterstützen den Aufbau eines TLS-Kanals zwischen der SAK und einem Extended Trusted Viewer sowie der SAK zu einem Kartenterminal.

Diese Anwendung enthält für die Kryptographie mit RSA bzw. elliptischen Kurven neben den entsprechenden Schlüsseln korrespondierende Zertifikate, die die zugehörigen öffentlichen Schlüssel PuK.SAK.AUT.XXXX enthalten. Es wird als nicht erforderlich angesehen, dass die Anwendung auch Zertifikate höherer Ebenen enthält.

Mit dem Schlüsselpaar PrK.SAK.SIG.XXXX (mit XXXX aus der Menge {R2048, R3072, E256, E384}) und PuK.SAK.SIG.XXXX (mit XXXX aus der Menge {R2048, R3072, E256, E384}) wird die Erstellung einer Signatur, bzw. Überprüfung einer Signatur für den Integritätsschutz von Konfigurationsdaten der SAK ermöglicht.

Kommunikation mit Karten der Generation 2

Der in dieser Anwendung enthaltene Schlüssel PrK.SAK.AUTD_CVC.E256 (alternativ PrK.SAK.AUTD_CVC.E384) für die Kryptographie mit elliptischen Kurven unterstützt den Aufbau eines Trusted Channels zwischen der Signaturanwendungskomponente einerseits und der sicheren Signaturerstellungseinheit andererseits.

Diese Anwendung enthält für die Kryptographie mit elliptischen Kurven neben dem vorgenannten Schlüssel PrK.SAK.AUTD_CVC.E256 (alternativ PrK.SAK.AUTD_CVC.E384) ein Zertifikat C.SAK.AUTD_CVC.E256 (optional C.SAK.AUTD_CVC.E384), welches den öffentlichen Schlüssel zu PrK.SAK.AUTD_CVC.E256 (optional PrK.SAK.AUTD_CVC.E384) enthält. Zur Prüfung des Zertifikates C.SAK.AUTD_CVC.E256 (optional C.SAK.AUTD_CVC.E384) wird der öffentliche Schlüssel aus C.CA_SAK.CS.E256 (siehe Kapitel 5.3.7) (optional C.CA_SAK.CS.E384, siehe Kapitel 5.3.9) benötigt.

☒ **Card-G2-A_2626 K_Initialisierung: Vorhandensein von DF.SAK**

Die Anwendung DF.SAK MUSS auf einer gSMC-K vorhanden sein. ☒

☒ **Card-G2-A_2627 K_Initialisierung: Konfiguration von DF.SAK**

Die Anwendung DF.SAK MUSS gemäß den Angaben dieses Unterkapitels konfiguriert sein. ☒

☒ **Card-G2-A_2628 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK**

Das Objekt DF.SAK MUSS die in Tab_gSMC-K_ObjSys_058 dargestellten Werte besitzen.

Tabelle 97: Tab_gSMC-K_ObjSys_058 Initialisierte Attribute von MF / DF.SAK

Attribute	Wert	Bemerkung
Objektyp	Ordner	
<i>applicationIdentifier</i>	'D276 0001 4404'	
<i>fileIdentifier</i>	herstellerspezifisch	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM,	ALWAYS	
LOAD APPLICATION	PWD(PIN.Pers)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)



Hinweis (95) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (96) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.6 im Allgemeinen irrelevant.

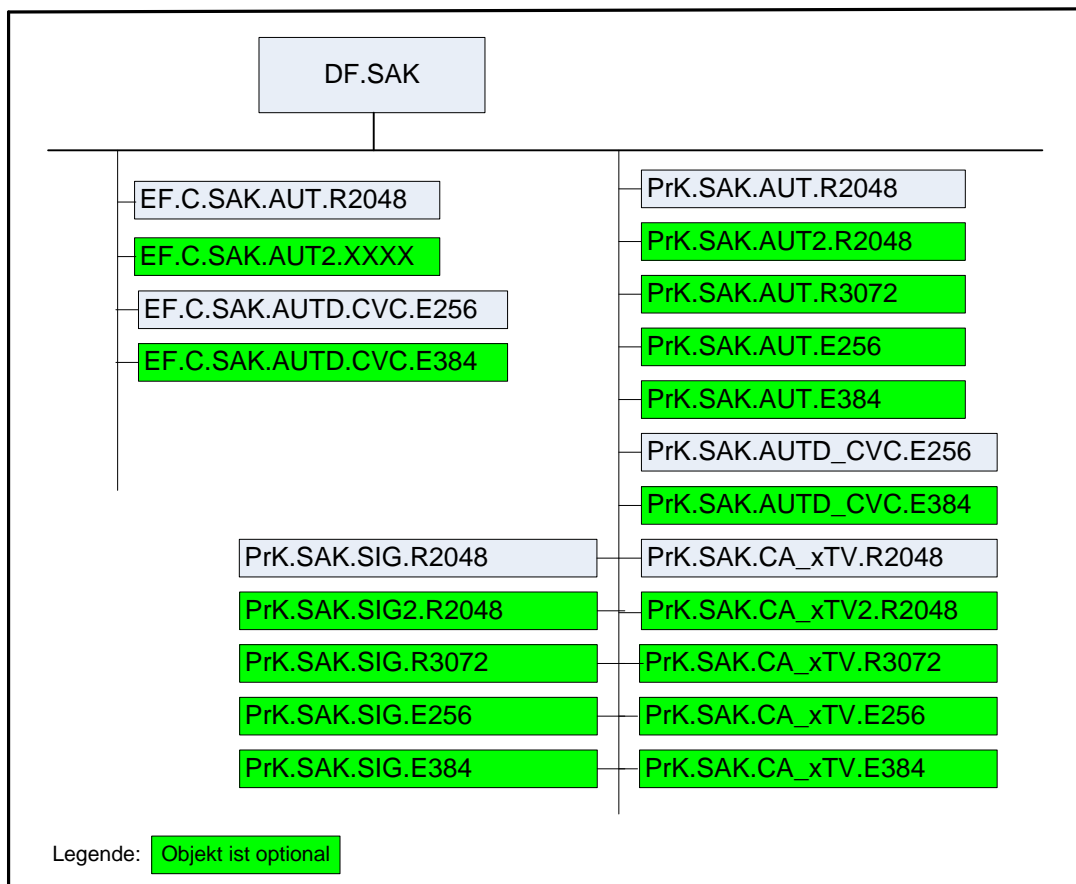


Abbildung 4: Abb_gSMC-K_ObjSys_004 Objektstruktur der Anwendung DF.SAK

5.6.1 MF / DF.SAK / EF.C.SAK.AUT.R2048

Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel zu PrK.SAK.AUT.R2048 (siehe Kapitel 5.6.2) aufzunehmen.

☒ **Card-G2-A_3422 K Initialisierung: Initialisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT.R2048**

Das Objekt EF.C.SAK.AUT.R2048 MUSS die in Tab_gSMC-K_ObjSys_167 dargestellten Werte besitzen.

Tabelle 98: Tab_gSMC-K_ObjSys_167 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C5 06'	
<i>shortFileIdentifier</i>	'06' = 6	
<i>numberOfOctet</i>	'08 02' Oktett = 2050 Oktett	
<i>positionLogicalEndOfFile</i>	WildCard	wird personalisiert
<i>flagTransactionMo-</i>	True	

de		
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (99)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (99)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (97) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (98) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

☒ **Card-G2-A_3423 K_Personalisierung: Personalisierte Attribute von MF/DF.SAK / EF.C.SAK.AUT.R2048**

Bei der Personalisierung von EF.C.SAK.AUT.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_133 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 99: Tab_gSMC-K_ObjSys_133 Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.SAK.AUT.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.SAK.AUT.R2048	



5.6.2 MF / DF.SAK / PrK.SAK.AUT.R2048

Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT.R2048 gehört.

☒ **Card-G2-A_2635 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048**

Das Objekt PrK.SAK.AUT.R2048 MUSS die in Tab_gSMC-K_ObjSys_168 dargestellten Werte besitzen.

Tabelle 100: Tab_gSMC-K_ObjSys_168 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'06' = 6	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	Alle Werte aus der Menge sign9796_2_DS2, signPKCS1_V1_5, signPSS}	siehe Hinweis (102)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DEACTIVATE	AUT_CMS OR AUT_CUP	
ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
GENERATE ASYMMETRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	Siehe Hinweis (101)
PSO COMPUTE DIGITALSIGNATURE	PWD(PIN.SAK)	
DELETE	PWD(PIN.SAK) OR AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE	AUT_CMS OR AUT_CUP	
DEACTIVATE	NEVER	herstellerspezifisch ist eine der beiden Varianten erlaubt
	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (99) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (100) Das Kommando ist nur vom Inhaber des CMS- /CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

Hinweis (101) Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.

Hinweis (102) Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

☒ **Card-G2-A_3424 K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048**

Bei der Personalisierung von PrK.SAK.AUT.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_169 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 101: Tab_gSMC-K_ObjSys_169 Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.6.3 MF / DF.SAK / EF.C.SAK.AUT2.XXXX

Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.SAK.AUT2.XXXX zu PrK.SAK.AUT2.XXXX (XXXX aus der Menge {R2048, R3072, E256, E384}) nach Ablauf der Nutzungszeit des Schlüssels PrK.SAK.AUT.R2048 aufzunehmen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_2631 K_Initialisierung: Initialisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT2.XXXX**

Das Objekt EF.C.SAK.AUT2.XXXX MUSS bei Ausgabe der Karte mit den in Tab_gSMC-K_ObjSys_060 dargestellten Werten angelegt werden.

Tabelle 102: Tab_gSMC-K_ObjSys_060 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT2.XXXX

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C5 07'	
<i>shortFileIdentifier</i>	'07' = 7	
<i>numberOfOctet</i>	'08 02' Oktett = 2.050 Oktett	
<i>positionLogicalEndOfFile</i>	'0'	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird später nachgeladen
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung

DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (105)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (105)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (103) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (104) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

5.6.4 MF / DF.SAK / PrK.SAK.AUT2.R2048

Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Card-G2-A_3425 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048

Das Objekt PrK.SAK.AUT2.R2048 MUSS die in Tab_gSMC-K_ObjSys_170 dargestellten Werte besitzen.

Tabelle 103: Tab_gSMC-K_ObjSys_170 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'07' = 7	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	Alle Werte aus der Menge {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	siehe Hinweis (107)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.AUT.R2048	



Hinweis (105) Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.

Hinweis (106) Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

5.6.5 MF / DF.SAK / PrK.SAK.AUT.R3072

Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3426 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072**

Das Objekt PrK.SAK.AUT.R3072 MUSS die in Tab_gSMC-K_ObjSys_171 dargestellten Werte besitzen.

Tabelle 104: Tab_gSMC-K_ObjSys_171 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 3072	
keyIdentifier	08' = 8	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	Alle Werte aus der Menge {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	siehe Hinweis (109)
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.AUT.R2048	



Hinweis (107) Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.

Hinweis (108) Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

5.6.6 MF / DF.SAK / PrK.SAK.AUT.E256

Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

☒ **Card-G2-A_3427 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E256**

Das Objekt PrK.SAK.AUT.E256 MUSS die in Tab_gSMC-K_ObjSys_172 dargestellten Werte besitzen.

Tabelle 105: Tab_gSMC-K_ObjSys_172 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifizier	'05' = 5	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifizier	signECDSA	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.AUT.R2048	



5.6.7 MF / DF.SAK / PrK.SAK.AUT.E384

Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.

Card-G2-A_3428 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384

Das Objekt PrK.SAK.AUT.E384 MUSS die in Tab_gSMC-K_ObjSys_173 dargestellten Werte besitzen.

Tabelle 106: Tab_gSMC-K_ObjSys_173 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 384	
keyIdentifizier	'09' = 9	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifizier	signECDSA	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		

<i>accessRules</i>	identisch zu PrK.SAK.AUT.R2048	
--------------------	--------------------------------	--



5.6.8 MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256

EF.C.SAK.AUTD_CVC.E256 enthält ein CV-Zertifikat gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.SAK.AUTD_CVC.E256 enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_SAK.CS.E256 (siehe Kapitel 5.3.8) prüfen.

☒ Card-G2-A_2638 K_Personalisierung: CHR von C.SAK.AUTD_CVC.E256

Für die CHR des Zertifikates MUSS gelten: CHR = '00 0A' || ICCSN, wobei die IC-CSN denselben Wert besitzen MUSS wie das Wertfeld *body* aus Card-G2-A_2567).



☒ Card-G2-A_2639 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256

Das Objekt EF.C.SAK.AUTD_CVC.E256 MUSS die in Tab_gSMC-K_ObjSys_064 dargestellten Werte besitzen.

Tabelle 107: Tab_gSMC-K_ObjSys_064 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 0A'	
<i>shortFileIdentifier</i>	'0A' = 10	
<i>numberOfOctet</i>	'011F' Oktett = 287 Oktett	
<i>positionLogicalEndOfFile</i>	Wildcard	wird personalisiert
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	undefiniert	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (111)
READ BINARY	ALWAYS	
SET LOGICAL EOF	AUT_CMS OR AUT_CUP	siehe Hinweis (111)
WRITE BINARY		
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)



Hinweis (109) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis (110) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

☒ Card-G2-A_3429 K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256

Bei der Personalisierung von EF.C.SAK.AUTD_CVC.E256 MÜSSEN die in Tab_gSMC-K_ObjSys_135 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 108: Tab_gSMC-K_ObjSys_135 Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	'00DE' Oktett = 222 Oktett	
<i>body</i>	C.SAK.AUTD_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.SAK.AUTD_CVC.E256	



5.6.9 MF / DF.SAK / PrK.SAK.AUTD_CVC.E256

PrK.SAK.AUTD_CVC.E256 wird im Rahmen von asymmetrischen Authentisierungsprotokollen für die Kryptographie mit elliptischen Kurven verwendet. Der zugehörige öffentliche Schlüssel PuK.SAK.AUTD_CVC.E256 ist in C.SAK.AUTD_CVC.E256 (siehe Kapitel 5.6.8) enthalten.

☒ Card-G2-A_2643 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256

Die Objekte PrK.SAK.AUTD_CVC.E256 MÜSSEN die in Tab_gSMC-K_ObjSys_067 dargestellten Werte besitzen.

Tabelle 109: Tab_gSMC-K_ObjSys_067 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt ELC 256	
<i>keyIdentifier</i>	'0A' = 10	
<i>privateElcKey</i>	<i>domainparameter = brainpoolP256r1</i>	
<i>privateElcKey</i>	<i>keyData = AttributNotSet</i>	<i>wird personalisiert</i>
<i>keyAvailable</i>	WildCard	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge { elcSessionkey4TC }	
<i>accessRulesSessionkeys</i>	Für alle logischen LCS Werte gilt Zugriffsart = PSO	

	→ Zugriffsbedingung = AUT(flagTI.52)	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE DEACTIVATE	AUT_CMS OR AUT_CUP	
GENERATE ASYM- METRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	siehe Hinweis (114)
GENERATE ASYM- METRIC KEY PAIR P1='81'	PWD(PIN.SAK)	
GENERAL AUTHENTI- CATE	ALWAYS	siehe Hinweis (113)
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (114)
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	NEVER	



Hinweis (111) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (112) Diese Rolle ist einem HBA zugewiesen

Hinweis (113) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10.

Card-G2-A_3430 K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256

Die Objekte PrK.SAK.AUTD_CVC.E256 MÜSSEN die in Tab_gSMC-K_ObjSys_137 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 110: Tab_gSMC-K_ObjSys_137 Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
privateElcKey	keyData = eine ganze Zahl im Intervall [1, domain-Parameter.n – 1]	



5.6.10 MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384

EF.C.SAK.AUTD_CVC.E384 enthält ein CV-Zertifikat gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.SAK.AUTD_CVC.E384 enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_SAK.CS.E384 (siehe Kapitel 5.3.9 prüfen.

☒ **Card-G2-A_2640 K_Personalisierung: CHR von C.SAK.AUTD_CVC.E384**

Für die CHR des Zertifikates MUSS gelten: CHR = '00 0F' || ICCSN, wobei die IC-CSN denselben Wert besitzen MUSS wie das Wertfeld *body* aus Card-G2-A_2567).



☒ **Card-G2-A_2641 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384**

Das Objekt EF.C.SAK.AUTD_CVC.E384 MUSS die in Tab_gSMC-K_ObjSys_065 dargestellten Werte besitzen.

Tabelle 111: Tab_gSMC-K_ObjSys_065 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 0F'	
<i>shortFileIdentifier</i>	'0F' = 15	
<i>numberOfOctet</i>	'011F' Oktett = 287 Oktett	
<i>positionLogicalEndOfFile</i>	'0'	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	undefiniert	wird später nachgeladen
Zugriffsregeln		
<i>accessRules</i>	identisch zu EF.C.SAK.AUTD_CVC.E256	siehe Hinweis (97)



5.6.11 MF / DF.SAK / PrK.SAK.AUTD_CVC.E384

PrK.SAK.AUTD_CVC.E384 wird im Rahmen von asymmetrischen Authentisierungsprotokollen für die Kryptographie mit elliptischen Kurven verwendet. Der zugehörige öffentliche Schlüssel PuK.SAK.AUTD_CVC.E384 ist in C.SAK.AUTD_CVC.E384 (siehe Kapitel 5.6.10) enthalten.

☒ **Card-G2-A_2644 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E384**

Das Objekt PrK.SAK.AUTD_CVC.E384 MUSS die in Tab_gSMC-K_ObjSys_068 dargestellten Werte besitzen.

Tabelle 112: Tab_gSMC-K_ObjSys_068 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E384

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt ELC 384	
keyIdentifizier	'0F' = 15	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifizier	alle Werte aus der Menge {elcSessionkey4TC}	
accessRulesSessionkeys	identisch zu PrK.SAK.AUTD_CVC.E256	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.AUTD_CVC.E256	



5.6.12 MF / DF.SAK / PrK.SAK.CA_xTV.R2048

Dieser private CA-Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers. Mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Der zugehörige öffentliche Schlüssel lässt sich auch mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2645 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048**

Das Objekt PrK.SAK.CA_xTV.R2048 MUSS die in Tab_gSMC-K_ObjSys_069 dargestellten Werte besitzen.

Tabelle 113: Tab_gSMC-K_ObjSys_069 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifizier	'0B' = 11	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifizier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM-	PWD(PIN.SAK)	

METRIC KEY PAIR P1='84' oder P1='80'		
GENERATE ASYM- METRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	PWD(PIN.SAK)	
TERMINATE	PWD(PIN.SAK)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (114) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (115) Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt

Card-G2-A_3431 K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048

Bei der Personalisierung von PrK.SAK.CA_xTV.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_139 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 114: Tab_gSMC-K_ObjSys_139 Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.6.13 MF / DF.SAK / PrK.SAK.CA_xTV2.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellereigenen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3432 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV2.R2048**

Das Objekt PrK.SAK.CA_xTV2.R2048 MUSS die in Tab_gSMC-K_ObjSys_174 dargestellten Werte besitzen.

Tabelle 115: Tab_gSMC-K_ObjSys_174 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'19' = 25	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.CA_xTV.R2048	



5.6.14 MF / DF.SAK / PrK.SAK.CA_xTV.R3072

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden.. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2646 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R3072**

Das Objekt PrK.SAK.CA_xTV.R3072 MUSS die in Tab_gSMC-K_ObjSys_070 dargestellten Werte besitzen.

Tabelle 116: Tab_gSMC-K_ObjSys_070 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 3072	
keyIdentifier	'0C' = 12	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	

<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.SAK.CA_xTV.R2048	



5.6.15 MF / DF.SAK / PrK.SAK.CA_xTV.E256

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_3433 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E256**

Das Objekt PrK.SAK.CA_xTV.E256 MUSS die in Tab_gSMC-K_ObjSys_184 dargestellten Werte besitzen.

Tabelle 117: Tab_gSMC-K_ObjSys_184 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
<i>keyIdentifier</i>	'0E' = 14	
<i>privateElcKey</i>	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
<i>privateElcKey</i>	keyData = AttributNotSet	
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] {signECDSA}	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.SAK.CA_xTV.R2048	



Hinweis (116) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.6.16 MF / DF.SAK / PrK.SAK.CA_xTV.E384

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2647 K Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E384**

Das Objekt PrK.SAK.CA_xTV.E384 MUSS die in Tab_gSMC-K_ObjSys_071 dargestellten Werte besitzen.

Tabelle 118: Tab_gSMC-K_ObjSys_071 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E384

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 384	
keyIdentifier	'0D' = 13	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {signECDSA}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.CA_xTV.R2048	



Hinweis (117) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.6.17 MF / DF.SAK / PrK.SAK.SIG.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient dazu Konfigurationsdaten der SAK zu signieren mit dem Ziel die Integrität der Daten zu schützen. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2648 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048**

Das Objekt PrK.SAK.SIG.R2048 MUSS die in Tab_gSMC-K_ObjSys_072 dargestellten Werte besitzen.

Tabelle 119: Tab_gSMC-K_ObjSys_072 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'14' = 20	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='84' oder P1='80'	PWD(PIN.SAK)	
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
PSO CompDigSig	PWD(PIN.SAK)	
TERMINATE	PWD(PIN.SAK)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (97)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	



Hinweis (118) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis (119) Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt

☒ **Card-G2-A_3434 K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048**

Bei der Personalisierung von PrK.SAK.SIG.R2048 MÜSSEN die in Tab_gSMC-K_ObjSys_142 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 120: Tab_gSMC-K_ObjSys_142 Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	



5.6.18 MF / DF.SAK / PrK.SAK.SIG2.R2048

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls dazu, Konfigurationsdaten der SAK zu signieren mit dem Ziel, die Integrität der Daten zu schützen. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.SIG.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec_COS#14.9.3.4]) auslesen.

Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.

☒ **Card-G2-A_3435 K Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048**

Das Objekt PrK.SAK.SIG2.R2048 MUSS die in Tab_gSMC-K_ObjSys_185 dargestellten Werte besitzen.

Tabelle 121: Tab_gSMC-K_ObjSys_185 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
<i>keyIdentifier</i>	'17' = 23	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
<i>keyAvailable</i>	False	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPSS}	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln		
<i>accessRules</i>	identisch zu PrK.SAK.SIG.R2048	



5.6.19 MF / DF.SAK / PrK.SAK.SIG.R3072

Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls dazu, Konfigurationsdaten der SAK zu signieren mit dem Ziel, die Integrität der Daten zu schützen. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.SIG.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu

einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec_COS#14.9.3.4]) auslesen.

Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.

☒ **Card-G2-A_2649 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072**

Das Objekt PrK.SAK.SIG.R3072 MUSS die in Tab_gSMC-K_ObjSys_073 dargestellten Werte besitzen.

Tabelle 122: Tab_gSMC-K_ObjSys_073 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 3072	
keyIdentifier	'15' = 21	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {sign9796_2_DS2, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SAK.SIG.R2048	



5.6.20 MF / DF.SAK / PrK.SAK.SIG.E256

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls dazu, Konfigurationsdaten der SAK zu signieren mit dem Ziel, die Integrität der Daten zu schützen. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.SIG.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec_COS#14.9.3.4]) auslesen.

Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.

☒ **Card-G2-A_3436 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256**

Das Objekt PrK.SAK.SIG.E256 MUSS die in Tab_gSMC-K_ObjSys_186 dargestellten Werte besitzen.

Tabelle 123: Tab_gSMC-K_ObjSys_186 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'18' = 24	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {signECDSA }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
accessRules	identisch zu PrK.SAK.SIG.R2048	



5.6.21 MF / DF.SAK / PrK.SAK.SIG.E384

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient dazu Konfigurationsdaten der SAK zu signieren mit dem Ziel die Integrität der Daten zu schützen. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.

Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec_COS#14.9.3.4]) auslesen.

☒ **Card-G2-A_2650 K_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384**

Das Objekt PrK.SAK.SIG.E384 MUSS die in Tab_gSMC-K_ObjSys_074 dargestellten Werte besitzen.

Tabelle 124: Tab_gSMC-K_ObjSys_074 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 384	
keyIdentifier	'16' = 22	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {signECDSA }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
accessRules	identisch zu PrK.SAK.SIG.R2048	



Hinweis (120) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

5.7 MF / DF.Sicherheitsanker

Die Anwendung DF.Sicherheitsanker enthält Zertifikate, die im Rahmen der Prüfung von TSL- oder TCL-Listen und QES-Zertifikaten relevant sind.

Hinweis (121) Aktuell werden in diesem Ordner Root Zertifikate C.TSL.CA gespeichert. Diese selbstsignierten Zertifikate enthalten einen öffentlichen Schlüssel zur Prüfung der Signer Zertifikate C.TSL.SIG und C.TCL.SIG. Die öffentlichen Schlüssel der letztgenannten Signaturzertifikate dienen dazu, Signaturen von TSL bzw. TCL Listen zu prüfen.

☒ Card-G2-A_2653 K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker

Das Objekt DF.Sicherheitsanker MUSS die in Tab_gSMC-K_ObjSys_075 dargestellten Werte besitzen.

Tabelle 125: Tab_gSMC-K_ObjSys_075 Initialisierte Attribute von MF / DF.Sicherheitsanker

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
<i>applicationIdentifier</i>	'D276 0001 4405'	
<i>fileIdentifier</i>	herstellerspezifisch	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	PWD(PIN.Pers)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)



Hinweis (122) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (123) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.7 im Allgemeinen irrelevant.

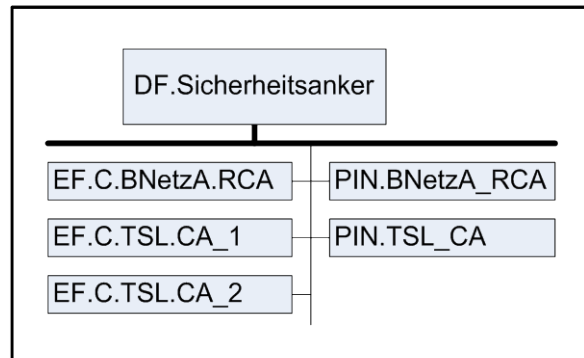


Abbildung 5: Abb_gSMC-K_ObjSys_005 Dateistruktur der Anwendung DF.Sicherheitsanker

5.7.1 MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.BnetzA.RCA. Dieser öffentliche Schlüssel dient der Verifikation des Zertifikates C.BnetzA.RCA, welches ein selbstsigniertes Wurzelzertifikat der Bundesnetzagentur ist. Falls der Fehlbedienungszähler *retryCounter* von PIN.BNetzA_RCA den Wert null besitzt, dann sind weitere Änderungen des Dateiinhaltes unmöglich.

☒ **Card-G2-A_2654 K Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA**

Das Objekt EF.C.BNetzA.RCA MUSS die in Tab_gSMC-K_ObjSys_076 dargestellten Werte besitzen.

Tabelle 126: Tab_gSMC-K_ObjSys_076 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'C6 10'	
shortFileIdentifier	'10' = 16	
numberOfOctet	'08 02' Oktett = 2.050 Oktett	
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden. Für Option_Erstellung_von_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden.		
body	'	

	Aktuelles Root-Zertifikat der BNetzA (C.BNetzA.RCA) gemäß [gemSpec_PKI#8.5.2]	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.BnetzA_RCA)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)



Hinweis (124) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

☒ **Card-G2-A_3582 K_Personalisierung: Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten**

Bei der Personalisierung von EF.C.BNetzA.RCA für Testkarten MUSS das in Tab_gSMC-K_ObjSys_214 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 127: Tab_gSMC-K_ObjSys_214 Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten

Attribute	Wert	Bemerkung
body	Root-Zertifikat der Pseudo-QES-Root gemäß [gemSpec_PKI#8.5.2]	



5.7.2 MF / DF.Sicherheitsanker / EF.C.TSL.CA_1

Genau wie EF.C.TSL.CA_2 in Kapitel 5.7.3 enthält diese Datei ein Zertifikat mit dem öffentlichen Schlüssel PuK.TSL.CA_1. Dieser öffentliche Schlüssel dient der Verifikation des Zertifikates C.TSL.SIG. Bei C.TSL.CA_1 handelt es sich um ein CA-Zertifikat. Falls der Fehlbedienungszyklus *retryCounter* von PIN.TSL_CA_1 den Wert null besitzt, dann sind weitere Änderungen des Dateiinhaltes unmöglich.

☒ **Card-G2-A_2655 K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_1**

Das Objekt EF.C.TSL.CA_1 MUSS die in Tab_gSMC-K_ObjSys_077 dargestellten Werte besitzen.

Tabelle 128: Tab_gSMC-K_ObjSys_077 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_1

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'C6 01'	
shortFileIdentifier	'01' = 1	
numberOfOctet	'08 02' Oktett = 2050 Oktett	
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden.		
Für Option_Erstellung_von_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden.		
body	C.TSL.CA_1 gemäß [gemSpec_PKI#5.13.3]	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.TSL_CA)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)



Hinweis (125) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

☒ **Card-G2-A_3583 K_Personalisierung: Personalisierte Attribute von MF / EF.C.TSL.CA_1 für Testkarten**

Bei der Personalisierung von EF.C.TSL.CA_1 für Testkarten MUSS das in Tab_gSMC-K_ObjSys_215 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 129: Tab_gSMC-K_ObjSys_215 Personalisierte Attribute von MF / EF.C.TSL.CA_1 für Testkarten

Attribute	Wert	Bemerkung
<i>body</i>	Zertifikat der Test-TSL.CA gemäß gemSpec_PKI[gemSpec_PKI#5.13.3]	



5.7.3 MF / DF.Sicherheitsanker / EF.C.TSL.CA_2

Genau wie EF.C.TSL.CA_1 in Kapitel 5.7.2 enthält diese Datei ein Zertifikat mit dem öffentlichen Schlüssel PuK.TSL.CA_2. Dieser öffentliche Schlüssel dient der Verifikation des Zertifikates C.TSL.SIG. Bei C.TSL.CA_2 handelt es sich um ein CA-Zertifikat. Falls der Fehlbedienungsähler *retryCounter* von PIN.TSL_CA_2 den Wert null besitzt, dann sind weitere Änderungen des Dateiinhaltes unmöglich.

☒ **Card-G2-A_2656 K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_2**

Das Objekt EF.C.TSL.CA_2 MUSS die in Tab_gSMC-K_ObjSys_078 dargestellten Werte besitzen.

Tabelle 130: Tab_gSMC-K_ObjSys_078 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_2

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C6 02'	
<i>shortFileIdentifier</i>	'02' = 2	
<i>numberOfOctet</i>	'08 02' Oktett = 2.050 Oktett	
<i>positionLogicalEndOfFile</i>	'0'	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF	PWD(PIN.TSL_CA)	

UPDATE BINARY WRITE BINARY		
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)



Hinweis (126) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

5.7.4 MF/DF.Sicherheitsanker / PIN.BNetzA_RCA

Dieses Passwortobjekt wird zur Freischaltung des Kommandos UPDATE BINARY für die Datei EF.C.BNetzA.RCA (siehe Kapitel 5.7.1) verwendet.

☒ **Card-G2-A_2658 K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA**

Das Objekt PIN.BNetzA_RCA MUSS die in Tab_gSMC-K_ObjSys_080 dargestellten Werte besitzen.

Tabelle 131: Tab_gSMC-K_ObjSys_080 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA

Attribute	Wert	Bemerkung
Objektyp	Passwortobjekt	
<i>pwdIdentifier</i>	'00' = 0	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	12	
<i>maximumLength</i>	12	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	
<i>PUK</i>	kein Inhalt	keine PUK
<i>pukUsage</i>	0	keine PUK
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (129)

	herstellerspezifisch	siehe [Card-G2-A_2659]
CHANGE RD, P1=0	ALWAYS	siehe Hinweis (130)
GET PIN STATUS	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)



Hinweis (127) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE

Hinweis (128) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.

Hinweis (129) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

☒ Card-G2-A_2659 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.BNetzA_RCA

Wenn für PIN.BnetzA_RCA als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.BnetzA_RCA nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerepezifisch umzusetzen. ☒

☒ Card-G2-A_3438 K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA

Wenn der Wert des Attributes *transportStatus* Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.BNetzA_RCA die in Tab_gSMC-K_ObjSys_146 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 132: Tab_gSMC-K_ObjSys_146 Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA

Attribute	Wert	Bemerkung
secret	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
<i>transportStatus</i>	Transport-PIN	wird gegebenenfalls personalisiert, siehe Hinweis (131)



Hinweis (130) Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

5.7.5 MF/DF.Sicherheitsanker / PIN.TSL_CA

Dieses Passwortobjekt wird zur Freischaltung des Kommandos UPDATE BINARY für die Datei EF.C.TSL.CA_1 (siehe Kapitel 5.7.2) und EF.C.TSL.CA_2 (siehe Kapitel 5.7.3) verwendet.

☒ Card-G2-A_2660 K_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA

Das Objekt PIN.TSL_CA MUSS die in Tab_gSMC-K_ObjSys_081 dargestellten Werte besitzen.

Tabelle 133: Tab_gSMC-K_ObjSys_081 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA

Attribute	Wert	Bemerkung
Objektyp	Passwortobjekt	
pwdIdentifier	'01' = 1	
secret	undefiniert	wird personalisiert
minimumLength	12	
maximumLength	12	
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
flagEnabled	True	
startSsec	unendlich	
PUK	kein Inhalt	keine PUK
pukUsage	0	keine PUK
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (133)
	herstellerspezifisch	siehe Hinweis (133)
CHANGE RD, P1=0	ALWAYS	siehe Hinweis (134)
GET PIN STATUS	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (124)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	siehe Hinweis (124)
------	----------------------	---------------------



Hinweis (131) Kommandos, die gemäß [gemSpec_COS]] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE

Hinweis (132) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.

Hinweis (133) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

☒ Card-G2-A_2661 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.TSL_CA

Wenn für PIN.TSL_CA als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.TSL_CA nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen. ☒

☒ Card-G2-A_3439 K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA

Wenn der Wert des Attributes *transportStatus* ransport-PIN ist, MÜSSEN bei der Personalisierung von PIN.TSL_CA die in Tab_gSMC-K_ObjSys_147 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 134: Tab_gSMC-K_ObjSys_147 Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
<i>transportStatus</i>	Transport-PIN	wird gegebenenfalls personalisiert, siehe Hinweis (135)



Hinweis (134) Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

5.8 Zusätzliche Applikationen und Dateien

Da eine gSMC-K innerhalb der TI nicht als eigenständige Komponente verwendet wird, sondern lediglich als Teilkomponente innerhalb eines Konnektors, ist es möglich, dass ein bestimmter Konnektor für den Betrieb weitere Objekte auf einer gSMC-K erwartet. Die Anforderungen in diesem Kapitel sind dazu gedacht, einem Konnektorhersteller in gewissem Rahmen eine Planungssicherheit zu geben, was die Installation weiterer Applikationen und Dateien anbelangt.

☒ **Card-G2-A_2662 K_Initialisierung: Zahl der Ordner in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker**

Für jeden Ordner, sofern vorhanden, aus der Menge {MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker} gilt:

- a) Es MUSS möglich sein, im Ordner bis zu vier Dateien anzulegen.
- b) Für jede Datei gilt:
 1. Es MUSS möglich sein, dass die Datei durch bis zu zwei individuelle Zugriffsregel geschützt wird.
 2. Jede dieser Zugriffsregeln MUSS gemäß [gemSpec_COS] kodierbar sein und MUSS insbesondere den Punkt [gemSpec_COS#N007.170] beachten.
 3. Die Zugriffsregeln einer Datei DÜRFEN bei einer Kodierung gemäß [ISO7816-4] Kapitel 5.4.3.2 zusammen NICHT mehr als 128 Oktette beanspruchen. ☒

☒ **Card-G2-A_2663 K_gSMC-K: Anlegen von EF.GeneralPurpose in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker**

Es MUSS möglich sein

- a) in mindestens einem Ordner aus der Menge {MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker}, sofern dieser vorhanden ist
- b) die in Tab_gSMC-K_ObjSys_082 spezifizierte Datei anzulegen. ☒

Hinweis (135) Card-G2-A_2662 stellt sicher, dass für die Zugriffsregeln immer eine gewisse Menge an Speicherplatz vorhanden ist. Das gilt z.B. auch, wenn das COS die Zugriffsregeln analog zu [ISO7816-4] Kapitel 5.4.3.3 in einem EF.ARR speichert.

Hinweis (136) Card-G2-A_2663 stellt sicher, dass eine gewisse Menge an freiem Speicherplatz zur Verfügung steht. Dabei fordert Card-G2-A_2663 a, dass in jedem vorhandenen Ordner der hier geforderte Speicherplatz auch exklusiv zur Verfügung steht. Demgegenüber stellt Card-G2-A_2663 b eine Forderung nach der Mindestmenge an gesamten freien Speicher dar.

5.9 EF.GeneralPurpose (kann nach Ausgabe der gSMC-K nachgeladen werden)

☒ **Card-G2-A_2664 Attribute der nachladbaren Datei EF.GeneralPurpose**

Falls das Objekt EF.GeneralPurpose auf die gSMC-K nachgeladen wird, MUSS es die in Tab_gSMC-K_ObjSys_082 dargestellten Werte besitzen.

Tabelle 135: Tab_gSMC-K_ObjSys_082 Attribute der nachladbaren Datei EF.GeneralPurpose

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'10 00'	
shortFileIdentifier	–	

<i>numberOfOctet</i>	'2000' Oktett = 8.192 Oktett	
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	'XX...YY'	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	ALWAYS	
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	



Hinweis (137) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

5.10 Laden einer neuen Anwendung oder Anlegen eines EFs oder Sperren von Schlüsseln nach Ausgabe der gSMC-K

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien EF.DIR und EF.Version) nach der Ausgabe der gSMC-K von einem Card Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CMS optional. Die Inhalte des Kapitels 14 in [gemSpec_COS] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe der gSMC-K durchgeführt werden.

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AK	Anwendungskonnektor
APDU	Application Protocol Data Unit
ATR	Answer to Reset
CA	Certification Authority
CHAT	Certificate Holder Authorisation Template Liste von Rechten, die ein Zertifikatsinhaber besitzt
CMS	Card Management System
COS	Card Operating System, Kartenbetriebssystem
CUP	Certificate Update
C2C	Card to Card
DF	Dedicated File
EF	Elementary File
ELC	Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven
GDO	Global Data Object
HBA	Heilberufsausweis
MF	Master File
NK	Netzkonnektor
RCA	Root Certification Authority
SAK	Signaturanwendungskomponente
TPM	Trusted Platform Module
TSL	Trust-service Status List
VPN	Virtual Private Network

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

Abbildung 1: Abb_gSMC-K_ObjSys_001 Dateistruktur einer gSMC-K auf oberster Ebene	22
Abbildung 2: Abb_gSMC-K_ObjSys_002 Dateistruktur der Anwendung DF.AK	80
Abbildung 3: Abb_gSMC-K_ObjSys_003 Dateistruktur der Anwendung DF.NK	93
Abbildung 4: Abb_gSMC-K_ObjSys_004 Objektstruktur der Anwendung DF.SAK	111
Abbildung 5: Abb_gSMC-K_ObjSys_005 Dateistruktur der Anwendung DF.Sicherheitsanker	132

A4 – Tabellenverzeichnis

Tabelle 1: Tab_gSMC-K_ObjSys_001 Liste der Komponenten, aus deren Sicht Anforderungen betrachtet werden	11
Tabelle 2: Tab_gSMC-K_ObjSys_002 ATR-Kodierung	20
Tabelle 3: Tab_gSMC-K_ObjSys_004 - Initialisierte Attribute von MF	23
Tabelle 4: Tab_gSMC-K_ObjSys_005 - Initialisierte Attribute von MF / EF.ATR	23
Tabelle 5: Tab_gSMC-K_ObjSys_009 Initialisierte Attribute von MF / EF.DIR	24
Tabelle 6: Tab_gSMC-K_ObjSys_010 Initialisierte Attribute von MF / EF.EnvironmentSettings	26
Tabelle 7: Tab_gSMC-K_ObjSys_090 Attribute von MF / EF.EnvironmentSettings	26
Tabelle 8: Tab_gSMC-K_ObjSys_011 Initialisierte Attribute von MF / EF.GDO	27
Tabelle 9: Tab_gSMC-K_ObjSys_177 Personalisierte Attribute von MF / EF.GDO	28
Tabelle 10: Tab_gSMC-K_ObjSys_150 Initialisierte Attribute von MF / EF.KeyInfo	28
Tabelle 11: Tab_gSMC-K_ObjSys_012 Initialisierte Attribute von MF / EF.Version2	29
Tabelle 12: Tab_gSMC-K_ObjSys_007 Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E256	30
Tabelle 13: Tab_gSMC-K_ObjSys_087 Attribute von MF / EF.C.CA_SAK.CS.E256	31
Tabelle 14: Tab_gSMC-K_ObjSys_008 Initialisierte Attribute von MF / EF.C.CA_SAK.CS.E384	32
Tabelle 15: Tab_gSMC-K_ObjSys_176 Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048	32
Tabelle 16: Tab_gSMC-K_ObjSys_148 Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten	33
Tabelle 17: Tab_gSMC-K_ObjSys_084 Initialisierte Attribute von MF / EF.C.RCA.CS.E256	34
Tabelle 18: Tab_gSMC-K_ObjSys_149 Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten	35

Tabelle 19: Tab_gSMC-K_ObjSys_192 Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256.....	35
Tabelle 20: Tab_gSMC-K_ObjSys_193 Personalisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256.....	36
Tabelle 21: Tab_gSMC-K_ObjSys_194 Initialisierte Attribute von MF / EF.C.SMC.AUT_CVC.E384.....	37
Tabelle 22: Tab_gSMC-K_ObjSys_013 Initialisierte Attribute von MF / PIN.AK	38
Tabelle 23: Tab_gSMC-K_ObjSys_094 Attribute von MF / PIN.AK.....	39
Tabelle 24: Tab_gSMC-K_ObjSys_014 Initialisierte Attribute von MF / PIN.NK.....	39
Tabelle 25: Tab_gSMC-K_ObjSys_095 Attribute von MF / PIN.NK.....	41
Tabelle 26: Tab_gSMC-K_ObjSys_015 Initialisierte Attribute von MF / PIN.Pers.....	41
Tabelle 27: Tab_gSMC-K_ObjSys_096 Attribute von MF / PIN.Pers	42
Tabelle 28: Tab_gSMC-K_ObjSys_016 Initialisierte Attribute von MF / PIN.SAK.....	43
Tabelle 29: Tab_gSMC-K_ObjSys_097 Attribute von MF / PIN.SAK.....	44
Tabelle 30: Tab_gSMC-K_ObjSys_195 Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E256.....	44
Tabelle 31: Tab_gSMC-K_ObjSys_196 Personalisierte Attribute von MF / PrK.SMC.AUT_CVC.E256.....	46
Tabelle 32: Tab_gSMC-K_ObjSys_197 Initialisierte Attribute von MF / PrK.SMC.AUT_CVC.E384.....	46
Tabelle 33: Tab_gSMC-K_ObjSys_017 Initialisierte Attribute von MF / PrK.KONN.AUT.R2048.....	48
Tabelle 34: Tab_gSMC-K_ObjSys_098 Attribute von MF / PrK.KONN.AUT.R2048	49
Tabelle 35: Tab_gSMC-K_ObjSys_152 Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048.....	49
Tabelle 36: Tab_gSMC-K_ObjSys_018 Initialisierte Attribute von MF / PrK.KONN.AUT.R3072.....	50
Tabelle 37: Tab_gSMC-K_ObjSys_178 Initialisierte Attribute von MF / PrK.KONN.AUT.E256.....	51
Tabelle 38: Tab_gSMC-K_ObjSys_019 Initialisierte Attribute von MF / PrK.KONN.AUT.E384	52
Tabelle 39: Tab_gSMC-K_ObjSys_020 Initialisierte Attribute von MF / PrK.GP.R2048...64	64
Tabelle 40: Tab_gSMC-K_ObjSys_101 Attribute von MF / PrK.GP.R2048	65
Tabelle 41: Tab_gSMC-K_ObjSys_027 Initialisierte Attribute von MF / PuK.GP.R2048..66	66
Tabelle 42: Tab_gSMC-K_ObjSys_104 Attribute von MF / PuK.GP.R2048	66
Tabelle 43: Tab_gSMC-K_ObjSys_153 Initialisierte Attribute von MF / PrK.GP2.R2048.67	67
Tabelle 44: Tab_gSMC-K_ObjSys_021 Initialisierte Attribute von MF / PrK.GP.R3072...67	67
Tabelle 45: Tab_gSMC-K_ObjSys_179 Initialisierte Attribute von MF / PrK.GP.E256.....68	68
Tabelle 46: Tab_gSMC-K_ObjSys_022 Initialisierte Attribute von MF / PrK.GP.E384.....69	69

Tabelle 47: Tab_gSMC-K_ObjSys_024 Initialisierte Attribute von MF / PuK.RCA.CS.E256	70
Tabelle 48: Tab_gSMC-K_ObjSys_191 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	71
Tabelle 49: Tab_gSMC-K_ObjSys_085 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	72
Tabelle 50: Tab_gSMC-K_ObjSys_108 Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	73
Tabelle 51: Tab_gSMC-K_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES128	74
Tabelle 52: Tab_gSMC-K_ObjSys_110 Attribute von MF / SK.CMS.AES128	75
Tabelle 53: Tab_gSMC-K_ObjSys_031 Initialisierte Attribute von MF / SK.CMS.AES256	75
Tabelle 54: Tab_gSMC-K_ObjSys_111 Attribute von MF / SK.CMS.AES256	76
Tabelle 55: Tab_gSMC-K_ObjSys_154 Initialisierte Attribute von MF / SK.CUP.AES128	77
Tabelle 56: Tab_gSMC-K_ObjSys_155 Personalisierte Attribute von MF / SK.CUP.AES128	77
Tabelle 57: Tab_gSMC-K_ObjSys_156 Initialisierte Attribute von MF / SK.CUP.AES256	78
Tabelle 58: Tab_gSMC-K_ObjSys_157 Personalisierte Attribute von MF / SK.CUP.AES256	78
Tabelle 59: Tab_gSMC-K_ObjSys_032 Initialisierte Attribute von MF / DF.AK	79
Tabelle 60: Tab_gSMC-K_ObjSys_034 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	80
Tabelle 61: Tab_gSMC-K_ObjSys_158 Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	81
Tabelle 62: Tab_gSMC-K_ObjSys_036 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048	82
Tabelle 63: Tab_gSMC-K_ObjSys_113 Attribute von MF / DF.AK / PrK.AK.AUT.R2048	83
Tabelle 64: Tab_gSMC-K_ObjSys_159 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT2.XXXX	83
Tabelle 65: Tab_gSMC-K_ObjSys_187 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048	85
Tabelle 66: Tab_gSMC-K_ObjSys_160 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072	85
Tabelle 67: Tab_gSMC-K_ObjSys_161 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E256	86
Tabelle 68: Tab_gSMC-K_ObjSys_162 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384	87

Tabelle 69: Tab_gSMC-K_ObjSys_037 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048.....	88
Tabelle 70: Tab_gSMC-K_ObjSys_114 Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048	89
Tabelle 71: Tab_gSMC-K_ObjSys_180 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS2.R2048.....	89
Tabelle 72: Tab_gSMC-K_ObjSys_038 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R3072.....	90
Tabelle 73: Tab_gSMC-K_ObjSys_181 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E256.....	90
Tabelle 74: Tab_gSMC-K_ObjSys_039 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.E384.....	91
Tabelle 75: Tab_gSMC-K_ObjSys_040 Initialisierte Attribute von MF / DF.NK	92
Tabelle 76: Tab_gSMC-K_ObjSys_041 Initialisierte Attribute von MF / DF.NK / EF.ActKey	93
Tabelle 77: Tab_gSMC-K_ObjSys_042 Initialisierte Attribute von MF / DF.NK / EF.CardInfo	94
Tabelle 78: Tab_gSMC-K_ObjSys_043 Initialisierte Attribute von MF / DF.NK / EF.CFSMACKKey.....	95
Tabelle 79: Tab_gSMC-K_ObjSys_044 Initialisierte Attribute von MF / DF.NK / EF.ConfigUser	96
Tabelle 80: Tab_gSMC-K_ObjSys_046 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048.....	97
Tabelle 81: Tab_gSMC-K_ObjSys_121 Attribute von MF / DF.NK / EF.C.NK.VPN.R2048	98
Tabelle 82: Tab_gSMC-K_ObjSys_188 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048.....	98
Tabelle 83: Tab_gSMC-K_ObjSys_163 Attribute von MF / DF.NK / PrK.NK.VPN.R2048	99
Tabelle 84: Tab_gSMC-K_ObjSys_189 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN2.XXXX.....	100
Tabelle 85: Tab_gSMC-K_ObjSys_164 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048.....	101
Tabelle 86: Tab_gSMC-K_ObjSys_190 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072.....	102
Tabelle 87: Tab_gSMC-K_ObjSys_165 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E256.....	102
Tabelle 88: Tab_gSMC-K_ObjSys_166 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384.....	103
Tabelle 89: Tab_gSMC-K_ObjSys_049 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048.....	104
Tabelle 90: Tab_gSMC-K_ObjSys_123 Attribute von MF / DF.NK / PrK.CFS.R2048....	105

Tabelle 91: Tab_gSMC-K_ObjSys_055 Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048	105
Tabelle 92: Tab_gSMC-K_ObjSys_130 Attribute von MF / DF.NK / PuK.CFS.R2048 ...	106
Tabelle 93: Tab_gSMC-K_ObjSys_182 Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048	106
Tabelle 94: Tab_gSMC-K_ObjSys_050 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072	107
Tabelle 95: Tab_gSMC-K_ObjSys_183 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256	108
Tabelle 96: Tab_gSMC-K_ObjSys_051 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384	109
Tabelle 97: Tab_gSMC-K_ObjSys_058 Initialisierte Attribute von MF / DF.SAK	110
Tabelle 98: Tab_gSMC-K_ObjSys_167 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048	111
Tabelle 99: Tab_gSMC-K_ObjSys_133 Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048	112
Tabelle 100: Tab_gSMC-K_ObjSys_168 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	113
Tabelle 101: Tab_gSMC-K_ObjSys_169 Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	114
Tabelle 102: Tab_gSMC-K_ObjSys_060 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT2.XXXX	114
Tabelle 103: Tab_gSMC-K_ObjSys_170 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048	115
Tabelle 104: Tab_gSMC-K_ObjSys_171 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072	116
Tabelle 105: Tab_gSMC-K_ObjSys_172 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E256	117
Tabelle 106: Tab_gSMC-K_ObjSys_173 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384	117
Tabelle 107: Tab_gSMC-K_ObjSys_064 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	118
Tabelle 108: Tab_gSMC-K_ObjSys_135 Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	119
Tabelle 109: Tab_gSMC-K_ObjSys_067 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	119
Tabelle 110: Tab_gSMC-K_ObjSys_137 Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	120
Tabelle 111: Tab_gSMC-K_ObjSys_065 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E384	121
Tabelle 112: Tab_gSMC-K_ObjSys_068 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E384	122

Tabelle 113: Tab_gSMC-K_ObjSys_069 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048.....	122
Tabelle 114: Tab_gSMC-K_ObjSys_139 Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048.....	123
Tabelle 115: Tab_gSMC-K_ObjSys_174 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV2.R2048.....	124
Tabelle 116: Tab_gSMC-K_ObjSys_070 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R3072.....	124
Tabelle 117: Tab_gSMC-K_ObjSys_184 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E256.....	125
Tabelle 118: Tab_gSMC-K_ObjSys_071 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.E384.....	126
Tabelle 119: Tab_gSMC-K_ObjSys_072 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048.....	127
Tabelle 120: Tab_gSMC-K_ObjSys_142 Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048.....	128
Tabelle 121: Tab_gSMC-K_ObjSys_185 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048.....	128
Tabelle 122: Tab_gSMC-K_ObjSys_073 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072.....	129
Tabelle 123: Tab_gSMC-K_ObjSys_186 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256.....	129
Tabelle 124: Tab_gSMC-K_ObjSys_074 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384.....	130
Tabelle 125: Tab_gSMC-K_ObjSys_075 Initialisierte Attribute von MF / DF.Sicherheitsanker.....	131
Tabelle 126: Tab_gSMC-K_ObjSys_076 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA.....	132
Tabelle 127: Tab_gSMC-K_ObjSys_214 Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten.....	133
Tabelle 128: Tab_gSMC-K_ObjSys_077 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_1.....	134
Tabelle 129: Tab_gSMC-K_ObjSys_215 Personalisierte Attribute von MF / EF.C.TSL.CA_1 für Testkarten.....	135
Tabelle 130: Tab_gSMC-K_ObjSys_078 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA_2.....	135
Tabelle 131: Tab_gSMC-K_ObjSys_080 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA.....	136
Tabelle 132: Tab_gSMC-K_ObjSys_146 Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA_RCA.....	137
Tabelle 133: Tab_gSMC-K_ObjSys_081 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA.....	138

Tabelle 134: Tab_gSMC-K_ObjSys_147 Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA	139
--	-----

Tabelle 135: Tab_gSMC-K_ObjSys_082 Attribute der nachladbaren Datei EF.GeneralPurpose	140
---	-----

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastuktur. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionen sind in den von der gematik veröffentlichten Produkttypsteckbriefen enthalten, in denen die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS) - Elektrische Schnittstelle
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_PINPUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smart-cards der Telematikinfrastuktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastuktur
[gemSpec_CVC_Root]	gematik: Spezifikation CVC - Root
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_TK]	gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2
[gemSpec_SMC_OPT]	gematik: Spezifikation der Security Module Card (SMC) – Gemeinsame optische Merkmale

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Beschluss 190]	Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DIN_EN_1867]	EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers DIN EN 1867:1997 Maschinenlesbare Karten – Anwendungen im Gesundheitswesen – Nummerierungssystem und Registrierungsverfahren für Kartenausgeber-schlüssel
[ISO3166-1]	ISO/IEC 3166-1: Codes for the representations of names of countries
[ISO7816-3]	ISO/IEC 7816-3: Smart Card Standard: Part 3: Electronic Signals and Transmission Protocols
[ISO7816-4]	ISO/IEC 7816-4: 2005 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ISO8825-1]	ISO/IEC 8825-1: 1995 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
[SD5]	ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19 Register of IC manufacturers
[PKCS#1v2.1]	PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 2002-06-14
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[TLS]	The Transport Layer Security (TLS) Protocol, Version 1.1, RFC 4346