gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation der Security Module Card SMC-B

Objektsystem

Version:	3.0.0
Revision:	\main\rel_online\1
Stand:	19.09.2012
Status:	freigegeben
Klassifizierung	öffentlich
Referenzierung:	[gemSpec_SMC-B_ObjSys]

Dokumentinformationen

Änderungen zur Vorversion

Dies ist die Erstversion des Dokumentes für Generation 2. Sie basiert auf dem Dokument „Spezifikation des elektronischen Heilberufsausweises Teil III: SMC - Anwendungen und Funktionen“ in der Version 2.3.2 vom 05.08.2009 unter Berücksichtigung der zugehörigen SRQs.

Inhaltliche Änderungen gegenüber Vorversionen sind NICHT farblich markiert, da das Dokument komplett überarbeitet wurde.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.3.2	05.08.09		Die Version 2.3.2 der „Spezifikation des elektronischen Heilberufsausweises, Teil 3: SMC – Anwendungen und Funktionen“ für die Generation 1 ist Grundlage der vorliegenden Spezifikation. Die Dokumentenhistorie der Version 2.3.2 ist nicht in dieses Dokument übernommen worden; sie kann bei Bedarf dort eingesehen werden.	gematik
	05.06.12		zur Abstimmung freigegeben	PL P71
3.0.0. RC	24.08.12		zur Freigabe empfohlen	PL P71
3.0.0	19.09.12		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an das Objektsystem der Sicherheitsmodulkarte SMC-B. Es beinhaltet die Definition der Anforderungen an die Objektstruktur, die Beschreibung der Kartenschnittstelle der Sicherheitsmodulkarte SMC-B für Institutionen im Gesundheitswesen und die.

Das Dokument berücksichtigt dabei:

- die DIN-Spezifikation für Chipkarten mit digitaler Signatur
- die ESIGN-Spezifikation für elektronische Signaturen
- die zugehörenden ISO-Standards (speziell ISO/IEC 7816, Teile 1-4, 6, 8, 9 und 15)
- andere Quellen (z. B. Anforderungen der Trustcenter)

Dieses Dokument spezifiziert Anwendungen der Sicherheitsmodulkarte SMC-B unter den folgenden, rein kartenorientierten Gesichtspunkten:

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

Somit stellt dieses Dokument auf unterster technischer Ebene eine Reihe von Datencontainern bereit. Zudem werden hier die Sicherheitsmechanismen für diese Datencontainer festgelegt, d. h. es wird festgelegt, welchen Instanzen es unter welchen Voraussetzungen möglich ist, auf Inhalte der Container zuzugreifen. Die Semantik und die Syntax der Inhalte in Datencontainern ist dagegen nicht Gegenstand dieses Dokumentes (siehe dazu auch Kapitel 1.4).

1.2 Zielgruppe

Das Dokument richtet sich an

- Hersteller, welche die hier spezifizierten Anwendungen für ein bestimmtes Chipkartenbetriebssystem umsetzen,
- Kartenherausgeber, die anhand der hier spezifizierten Anwendungen die elektrische Personalisierung einer Sicherheitsmodulkarte SMC-B planen,
- Hersteller von Systemen, welche unmittelbar mit der Chipkarte kommunizieren.

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.

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

Die Basiskommandos, die Grundfunktionen des Betriebssystems sowie die grundlegenden Sicherheitsfunktionen und -algorithmen (hard facts) für alle Karten des Gesundheitswesens (eGK, HBA, SMC-B, gSMC-K, gSMC-KT) werden in der Spezifikation des Card Operating System (COS) detailliert beschrieben [gemSpec_COS]. Die Spezifikation [gemSpec_COS] ist Grundlage der Entwicklung der Kommandostrukturen und Funktionen für die Chipkartenbetriebssysteme.

Die optische Gestaltung für alle SMCs und damit auch für die SMC-B wird in dem Dokument „Gemeinsame optische Merkmale der SMC“ [gemSpec_SMC_OPT] wird festgelegt.

1.5 Methodik

1.5.1 Nomenklatur

´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, …).

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

AUT_CMS	Symmetrische Schlüssel: Falls SK.CMS.AES256 nicht vorhanden ist: [AUT(SK.CMS.AES128) AND SmMac(SK.CMS.AES128)] AND SmCmdEnc AND SmRspEnc
	Symmetrische Schlüssel: Falls SK.CMS.AES256 vorhanden ist: {[AUT(SK.CMS.AES128) AND SmMac(SK.CMS.AES128)] OR [AUT(SK.CMS.AES256) AND SmMac(SK.CMS.AES256)]} AND SmCmdEnc AND SmRspEnc
	Asymmetrische Schlüsselpaare mit PuK.CMS_SMC-B.AUT_CVC.E256 oder PuK.CMS_SMC-B.AUT_CVC.E384 SmMac(cvc_FlagList_CMS, flag=08) AND SmCmdEnc AND SmRspEnc

Anmerkung. Bei Kommandos ohne Daten, z.B. ERASE, entfällt die Verpflichtung zur Verschlüsselung (SmCmdEnc, SmRspEnc).

1.5.2 Verwendung von Schüsselworten

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_xxxx - <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

Abwandlungen von „**MUSS**“ zu „**MÜSSEN**“ etc. sind der Grammatik geschuldet. Da im Beispielsatz „*Eine leere Liste DARF NICHT ein Element besitzen*.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „*Eine leere Liste DARF KEIN Element besitzen*.“ verwendet.

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 Komponente zu betrachten. Die normativen Abschnitte tragen deshalb eine Kennzeichnung, aus wessen Sichtweise die Anforderung primär betrachtet wird.

Tabelle 1: Tab_SMC-B_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt

Komponente	Beschreibung
K_Personalisierung	Instanz, die eine Chipkarte im Rahmen einer Produktion individualisiert
K_Terminal	eHealth-Kartenterminal
K_COS	Betriebssystem einer Smart Card

2 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 Begriffe "Vorbereitungsphase" und "Nutzungsphase" werden in [gemSpec_COS#4] definiert.

3 Anwendungsübergreifende Festlegungen

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

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

3.1 Attributstabellen

⌦ **Card-G2-A_2134 (N700.100) K_Personalisierung: Änderung von Zugriffsregeln**

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

⌦ **Card-G2-A_2135 (N700.200) K_Personalisierung: Verwendung von SE**

Der Terminus „alle SE“ bedeutet, dass Objekte sich in SE#1 wie angegeben verwenden lassen MÜSSEN. Diese Objekte KÖNNEN in anderen SE verwendet werden und MÜSSEN dort dieselben Eigenschaften wie in SE#1 besitzen. ⌫

3.1.1 Attribute eines Ordners

⌦ **Card-G2-A_2136 (N700.300) K_Personalisierung: 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 NICHT mittels eines *fileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.1] selektierbar sein, 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. ⌫

3.1.2 Attribute einer Datei (EF)

⌦ **Card-G2-A_2137 (N700.400) K_Personalisierung: 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_2668 (N700.430) K_Personalisierung Wert von „positionLogicalEndOfFile“

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

3.2 Zugriffsregeln für besondere Kommandos

Gemäß [gemSpec_COS] gilt:

Card-G2-A_2669 (N700.450) K_Personalisierung: Zugriffsregeln für besondere Kommandos

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

3.3 Mindestanzahl logischer Kanäle

Card-G2-A_2196 (N700.500) K_Personalisierung: Anzahl logischer Kanäle

Für die Anzahl logischer Kanäle, die von einer SMC-B zu unterstützen ist, gilt:

a) Die maximale Anzahl logischer Kanäle MUSS gemäß [ISO7816-4#Tab.88] in den Historical Bytes des ATR angezeigt werden.

b) Die SMC-B 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.⌫

Jeder Kanal besitzt seinen eigenen unabhängigen Sicherheitsstatus, d.h. eine externe Authentisierung der Rollenkennung in einem logischen Kanal setzt keinen Sicherheitszustand in irgendeinem anderen Kanal.

3.4 Kryptobox

Card-G2-A_2871 (N700.550) COS: Kryptobox

Im COS einer SMC-B MUSS die Option_Kryptobox vorhanden sein.⌫

3.5 Zusätzliche Schnittstellen

3.5.1 Kontaktlose Schnittstelle

Card-G2-A_2138 (N700.600) 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 SMC-B NICHT genutzt werden.⌫

3.5.2 USB-Schnittstelle (optional)

⌦ **Card-G2-A_2872 (N700.900) COS: Vorhandensein einer USB-Schnittstelle**

Im COS einer SMC-B KANN die Option_USB_Schnittstelle

a) vorhanden sein, oder

b) fehlen.⌫

4 Spezifikation grundlegender Applikationen

Zu den grundlegenden Applikationen der Sicherheitsmodulkarte SMC-B zählen:

- das Wurzelverzeichnis der SMC, auch Root oder Master File (MF) genannt,
- die Sicherheitsmodulanwendung DF.SMA (Security Module Application),
- die Krypto-Anwendung DF.ESIGN
- die Kartenterminalanwendung DF.KT

4.1 Attribute des Objektsystems

Das Objektsystem der SMC-B enthält gemäß [gemSpec_COS#9.1] folgende Attribute:

⌦ **Card-G2-A_2139 (N701.000) K_Personalisierung: Wert des Attributes *root***

Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_SMC-B_ObjSys_002 sein. ⌫

⌦ **Card-G2-A_2140 (N701.100) K_Personalisierung: Wert des Attributes answer-ToReset**

Der Wert des Attributes *answerToReset* MUSS gemäß Kapitel 4.1.1 sein.⌫

⌦ **Card-G2-A_2141 (N701.200) K_Personalisierung: Wert des Attributes iccsn8**

Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein. ⌫

⌦ **Card-G2-A_2142 (N701.300) K_Personalisierung: Inhalt persistentPublicKey-List**

Das Attribut *persistentPublicKeyList* MUSS die Schlüssel PuK.RCA.CS.R2048 und PuK.RCA.CS.E256 enthalten. ⌫

4.1.1 ATR-Kodierung und technische Eigenschaften

⌦ **Card-G2-A_2670 (N701.310) ATR-Kodierung**

Für die SMC-B MÜSSEN dieselben Konventionen für die technischen Eigenschaften, ATR und Übertragungsprotokolle wie für den HBA gelten, siehe [gemSpec_COS#11.2] für die elektrische Schnittstelle und Kapitel 4.1.1 in [gemSpec_HBA_ObjSys] für die ATR-Kodierung. ⌫

4.2 Allgemeine Struktur

Card-G2-A_2143 (N701.320) K_Personalisierung: Kompatibilität zu G1-Karten

Die SMC-B der Generation 2 MUSS rückwärtskompatibel zu den Karten der Generation 1 sein. Deshalb MUSS sie bezüglich der CV-Zertifikate sowohl Zertifikate und Schlüssel für das RSA-Verfahren mit einer Schlüssellänge von 2048 bit (Generation 1) als auch Zertifikate und Schlüssel für die Verfahren mit elliptischen Kurven mit einer Schlüssellänge von 256 bit (Generation 2) enthalten.⌫

Card-G2-A_2144 (N701.340) K_Personalisierung: Container und Schlüssel für eine längere Laufzeit des SMC-B im Feld (optional)

Um eine langfristige Nutzbarkeit der Karten der Generation 2 zu ermöglichen, KÖNNEN optional sowohl für RSA als auch für elliptische Kurven Container für Zertifikate und Schlüssel für die nächste Stufe der Schlüssellängen (3072 bit für RSA und 384 bit für elliptische Kurven) vorgesehen werden. ⌫

Card-G2-A_2145 (N701.360) K_Personalisierung: Füllung der optionalen Container für Zertifikate und Schlüssel

Wenn die Container für Zertifikate und Schlüssel für die nächste Stufe der Schlüssellängen (3072 bit für RSA und 384 bit für elliptische Kurven) angelegt werden, dann MÜSSEN sie gemäß dieser Spezifikation befüllt werden.⌫

Abbildung 1 zeigt die allgemeine Struktur der SMC-B.

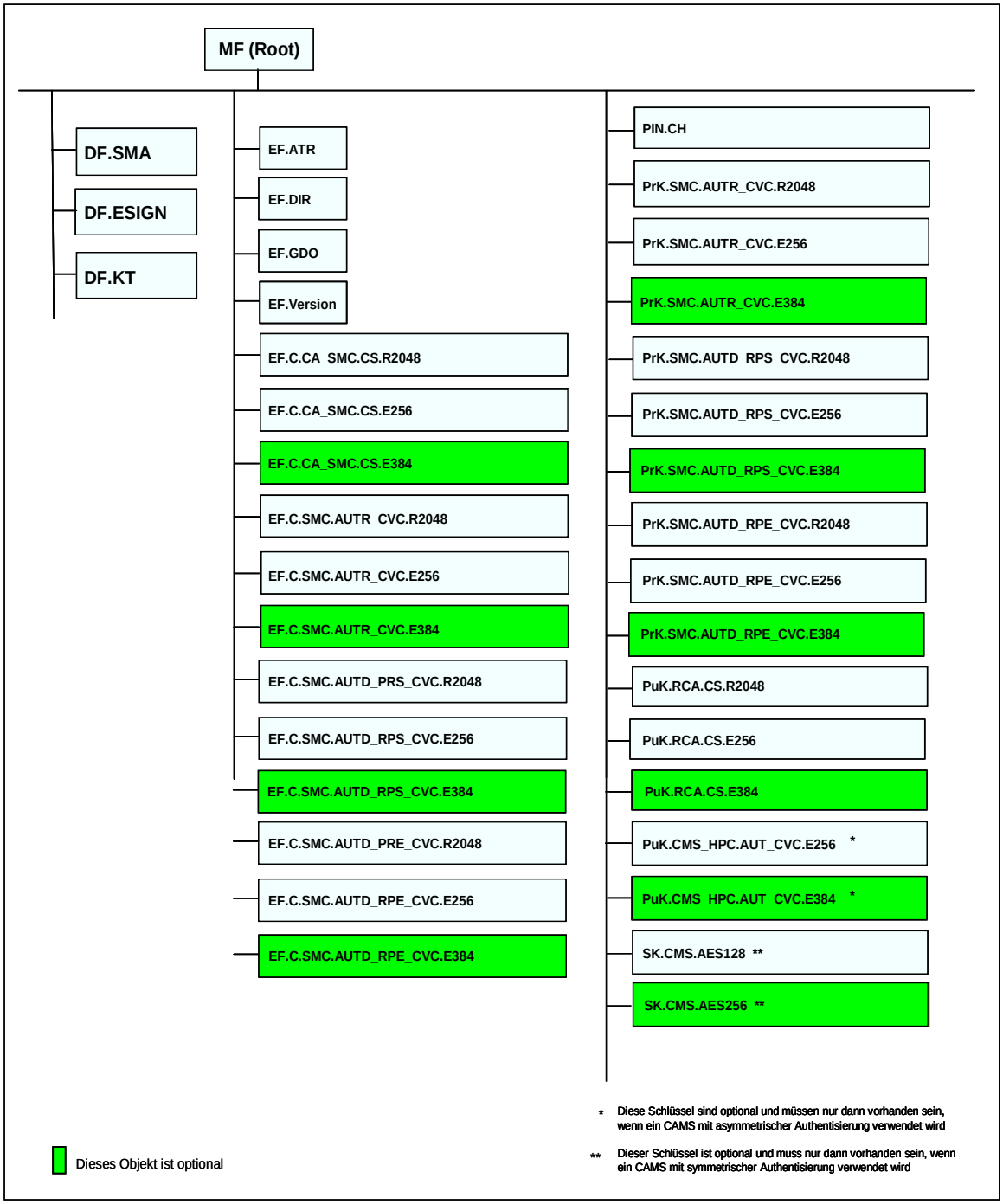

Abbildung 1: Abb_SMC-B_ObjSys_001 Allgemeine Struktur der SMC-B

Eine kryptografische Informationsanwendung (DF.CIA.ESIGN) ist nicht erforderlich, da eine SMC-B stationär gesteckt bleibt und die Anwendung der zuständigen Software bekannt ist.

4.3 Root, die Wurzelapplikation MF

Das MF der SMC-B ist ein “Application Dedicated File” (siehe [gemSpec_COS#8.3.1.3]) mit den in Tab_SMC-B_ObjSys_002 gezeigten Eigenschaften.

⌦ **Card-G2-A_2146 (N701.400) K_Personalisierung: Attribute von MF**

MF MUSS die in Tab_SMC-B_ObjSys_002 dargestellten Werte besitzen.

Tabelle 2: Tab_SMC-B_ObjSys_002 Attribute von MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	‘D27600014606’	
FID	´3F 00´	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
FINGERPRINT	SmMac(cvc_FlagList_TI, flag=49)	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 3:
SELECT	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 2: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT, TERMINATE

Hinweis 3: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.1 MF / EF.ATR

Die transparente Datei EF.ATR enthält Informationen zur maximalen Größe der APDU sowie zur Identifizierung des Betriebssystems.

⌦ **Card-G2-A_2147 (N701.500) K_Personalisierung: Attribute von MF / EF.ATR**

EF.ATR MUSS die in Tab_SMC-B_ObjSys_003 dargestellten Werte besitzen.

Tabelle 3: Tab_SMC-B_ObjSys_003 Attribute von MF / EF.ATR

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 01´	siehe Hinweis 5:
shortFileIdentifier	´1D´= 29	
numberOfOctet	herstellerspezifisch	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	siehe unten
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	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 4: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

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

Für das Attribut body gelten folgende Festlegungen:

⌦ **Card-G2-A_2148 (N701.600) K_Personalisierung: Datenobjekte in EF.ATR**

Der Oktettstring body MUSS DER-TLV codierte Datenobjekte (DO) enthalten, welche lückenlos hintereinander konkateniert werden MÜSSEN.⌫

Card-G2-A_2149 (N701.700) K_Personalisierung: DO_BufferSize in EF.ATR

In body MUSS an erster Stelle genau ein DO_BufferSize mit folgenden Eigenschaften enthalten sein:

a) Tag = ´E0´.

b) DO_BufferSize MUSS genau vier DO mit einem Tag ´02´ enthalten. Der Tag ´02´ bezeichnet einen Integer Wert, der gemäß [ISO8825-1]#8.3] codiert werden MUSS.

c) Das erste DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine ungesicherte Kommando APDU nicht überschreiten SOLL.

d) Das zweite DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine ungesicherte Antwort nicht überschreiten SOLL.

e) Das dritte DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine gesicherte Kommando APDU nicht überschreiten SOLL.

f) Das vierte DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine gesicherte Antwort nicht überschreiten SOLL. ⌫

Card-G2-A_2150 (N701.800) K_Personalisierung: DO_CardData in EF.ATR

In body MUSS an zweiter Stelle genau ein DO_CardData mit folgenden Eigenschaften enthalten sein:

a) Tag = ´66´.

b) Das Wertfeld von DO_CardData MUSS genau ein DO_PreIssuingData mit folgenden Eigenschaften enthalten:

1. Tag = ´46´.
2. Das erste Oktett des Wertfeldes MUSS die Chiphersteller ID gemäß [SD5] enthalten.
3. Die Oktette zwei bis sechs MÜSSEN die Kartenhersteller–ID enthalten. Anträge unter http://www.sit.fraunhofer.de/ bzw. http://141.12.72.35/_karten_ident/SIT/pdfs/ICCM_Antrag_2006.pdf.
4. Weitere Oktette sind herstellerspezifisch zu codieren und SOLLEN eine Betriebssystemversion eineindeutig referenzieren.

c) Das Wertfeld von DO_CardData MUSS genau ein DO_Card Capabilities mit folgenden Eigenschaften enthalten:

1. Tag = ´47´(Kodierung gemäß Card-G2-A_2153)

c) Das Wertfeld von DO_CardData KANN weitere DER-TLV codierte Datenobjekte enthalten. ⌫

⌦ **Card-G2-A_2152 (N701.900) K_Personalisierung: Weitere Datenobjekte in EF.ATR**

In body KÖNNEN weitere DER-TLV codierte Datenobjekte enthalten sein. ⌫

⌦ **Card-G2-A_2153 (N702.000) K_Personalisierung: Wert of DO Card Capabilities (Tag '47')**

DO Card Capabilities (Tag '47') MUSS die in Tab_SMC-B_ObjSys_004 dargestellten Attribute besitzen.

Tabelle 4: Tab_SMC-B_ObjSys_004 Wert of DO Card Capabilities (Tag '47')

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung des 1. Byte ('x6')
1	-	-	-	-	-	-	-	DF-Auswahl mit vollem DF-Namen
-	x	-	-	-	-	-	-	DF-Auswahl mit partiellem DF-Namen (nicht festgelegt)
-	-	x	-	-	-	-	-	DF- Auswahl mit Pfad (nicht festgelegt)
-	-	-	1	-	-	-	-	DF- Auswahl mit File Identifier
-	-	-	-	0	-	-	-	Implizite DF-Auswahl (nicht unterstützt)
-	-	-	-	-	1	-	-	Unterstützung der Short File Identifier
-	-	-	-	-	-	1	-	Unterstützung von Rekordnummern
-	-	-	-	-	-	-	0	Record Identifier (nicht unterstützt)
b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung de 2. Byte ('21')
0	-	-	-	-	-	-	-	EFs mit TLV-Struktur (nicht unterstützt)
-	0	1	-	-	-	-	-	Verhalten der Schreibfunktionen (proprietär)
-	-	-	0	-	-	-	-	Wert 'FF' als 1. Byte von BER-TLV Tagfeldern unzulässig
-	-	-	-	0	0	0	1	Größe der Dateneinheiten in Vierbit-Einheiten (als Zweierpotenz, d.h. '01' = 2 Vierbit-Einheiten = 1 Byte)
b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung des 3. Byte ('Dx')
1	-	-	-	-	-	-	-	Unterstützung von Command Chaining, siehe Anmerkung 1
-	1	-	-	-	-	-	-	Extended Lc und Le-Felder
-	-	0	-	-	-	-	-	b6 ist RFU (b6 = 0 empfohlen)
-	-	-	1	0	-	-	-	Zuweisung der Nummern logischer Kanäle durch die Karte
					y	z	t	
-	-	-	-	-	x	x	x	Maximale Anzahl logischer Kanäle, siehe Anmerkung 2

⌫

4.3.2 MF / EF.DIR

Die Datei EF.DIR enthält eine Liste mit Anwendungs-Templates gemäß [ISO/IEC 7816-4]. Diese Liste wird dann angepasst, wenn sich die Applikationsstruktur durch Löschen oder Anlegen von Anwendungen verändert.

Card-G2-A_2154 (N702.100) K_Personalisierung: Attribute von MF / EF.DIR

EF.DIR MUSS die in Tab_SMC-B_ObjSys_005 dargestellten Werte besitzen.

Tabelle 5: Tab_SMC-B_ObjSys_005 Attribute von MF / EF.DIR

Attribute	Wert	Bemerkung
Objekttyp	linear variables Elementary File	
fileIdentifier	´2F 00´	siehe Hinweis 7:
shortFileIdentifier	´1E´= 30	siehe Hinweis 7:
numberOfOctet	´0085´ Oktett = 133 Oktett	
maxNumRecords	7 Rekord	
maxRecordLength	19 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList Rekord 1 Rekord 2 Rekord 3 Rekord 4 Rekord 5	 ´61-L_{61}-(‘4F 06 D27600014606 || …)’ ´61-L_{61}-(4F 06 D27600014607 || …)´ ´61-L_{61}-(4F 0A A000000167 455349474E || …)´ ´61-L_{61}- (4F 06 D27600014400 || …)´ nicht vorhanden, MUSS mittels APPEND RECORD für eine neue Anwendung nachgeladen werden Ergänzungen zum DO ’61 siehe Card-G2-A_2155	 AID.MF AID.SMA AID.ESIGN AID.KT
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
APPEND RECORD	AUT_CMS	siehe Hinweis 8:
DELETE	AUT_CMS	siehe Hinweis 8:
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT_CMS	siehe Hinweis 8:
SELECT	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 6: Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD, TERMINATE

Hinweis 7: Die Werte von fileIdentifier und shortFileIdentifier sind in ISO/IEC 7816-4 festgelegt.

Hinweis 8: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

⌦ **Card-G2-A_2155 (N701.150) K_Personalisierung: DO ’61’ in EF.DIR**

Im EF.DIR MUSS jeder Rekord ein DO’61’ enthalten.

a) In jedem DO’61’ MUSS ein DO’4F’ mit der AID gemäß Tab_SMC-B_ObjSys_005 enthalten sein.

b) In jedem DO’61’ MUSS ein DO’50’ enthalten sein, das die Implementierung der korrespondierenden Anwendung identifiziert.

c) Der Rekord, welcher das MF beschreibt MUSS zusätzlich ein DO’53’ enthalten, das die Implementierung des COS identifiziert. ⌫

Die Inhalte von DO’53’ und aller DO’50’ werden von der gematik herstellerspezifisch festgelegt.

4.3.3 MF / EF.GDO

In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte enthält. Die Kennnummer basiert auf [Beschluss190].

⌦ **Card-G2-A_2156 (N701.200) K_Personalisierung: Attribute von MF / EF.GDO**

EF.GDO MUSS die in Tab_SMC-B_ObjSys_006 dargestellten Werte besitzen.

Tabelle 6: Tab_SMC-B_ObjSys_006 Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 02´	
shortFileIdentifier	´02´= 2	
numberOfOctet	´000C´ Oktett = 12 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	

body	´5A0AXX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	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 9: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Das Attribut body enthält die Seriennummer der Karte. Dabei gilt:

⌦ **Card-G2-A_2157 (N701.300) K_Personalisierung: DO_ICCSN in EF.GDO**

In body MUSS genau ein DER-TLV codiertes Datenobjekt DO_ICCSN mit folgenden Eigenschaften enthalten sein:

a) Tag = ´5A´ und Längenfeld = ´0A´.

b) Für das Wertfeld MUSS gelten:

1. Das erste Oktett MUSS den Major Industry Identifier (MII) mit dem Wert ´80´ enthalten, welcher eine Gesundheitskarte kennzeichnet (siehe [DIN_EN_1867]).
2. Die nächsten drei Nibble MÜSSEN den Country Code Deutschlands mit dem Wert ´276´enthalten (siehe [ISO3166-1]).
3. Die nächsten fünf Nibble MÜSSEN den Issuer Identifier enthalten.
4. Die restlichen fünf Oktette MÜSSEN BCD codiert eine Seriennummer enthalten. ⌫

Hinweis 10: Die Kennung eines Kartenherausgebers (Issuer Identifier) erlaubt, in Verbindung mit dem Ländercode, eine weltweit eineindeutige Identifizierung des Kartenherausgebers. In Verbindung mit der Seriennummer ist es deshalb möglich, eine Karte weltweit eineindeutig zu referenzieren.

Hinweis 11: Die Kennung des Kartenherausgebers entsprechend [DIN_EN_1867] wird in Deutschland im Auftrag des DIN durch GS1 Germany GmbH, Köln (www.gs1-germany.de)

vergeben. Der Kartenherausgeber ist gewöhnlich der rechtmäßige Eigentümer der ausgegebenen Karte.

4.3.4 A MF / EF.Version

Diese Datei enthält pro Rekord die Versionsnummer einer "Schnittstelle". Dabei werden folgende "Schnittstellen", besser gesagt folgende Ebenen unterschieden:

- Betriebssystem: Die "Schnittstelle" des Betriebssystems wird in [gemSpec_COS] spezifiziert. Dabei werden der grundsätzliche Funktionsumfang und der Aufbau der Nachrichten von und zur SMC-B festgelegt.
- Objektsystem: Die Konfiguration des Objektsystems wird in diesem Dokument spezifiziert. Damit wird für die fachliche Ebene festgelegt, wo Daten abgelegt sind und welche Zugriffsrechte die SMC-B durchsetzt.

⌦ **Card-G2-A_2158 (N701.400) K_Personalisierung: Attribute von MF / EF.Version**

EF.Version MUSS die in Tab_SMC-B_ObjSys_007 dargestellten Werte besitzen.

Tabelle 7: Tab_SMC-B_ObjSys_007 Attribute von MF / EF.Version

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´2F 10´	
shortFileIdentifier	´10´= 16	
Number of Bytes	´0014´ Oktett = 20 Oktett	
maxNumRecords	4 Rekord	
maxRecordLength	5 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList Rekord 1 Rekord 2 Rekord 3 Rekord 4	 ´XX…YY´ ´XX…YY´ ´XX…YY´ ´XX…YY	Der Rekordinhalt wird im Produkttypsteckbrief der SMC-B festgelegt.
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ RECORD SEARCH RECORD	ALWAYS	

UPDATE RECORD	AUT_CMS	siehe Hinweis 13:
SELECT	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 12: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD, TERMINATE

Hinweis 13: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.5 MF / EF.C.CA_SMC.CS.R2048

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit RSA gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SMC.CS.R2048 einer CA enthält.

⌦ **Card-G2-A_2159 (N701.500) K_Personalisierung: Attribute von MF / EF.C.CA_SMC.CS.R2048**

EF.C.CA_SMC.CS.R2048 MUSS die in Tab_SMC-B_ObjSys_008 dargestellten Werte besitzen.

Tabelle 8: Tab_SMC-B_ObjSys_008 Attribute von MF / EF.C.CA_SMC.CS.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 04´	
shortFileIdentifier	´04´= 4	
numberOfOctet	´014B´ Oktett = 331 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
body	´7F21 820146 XX…YY´	wird personalisiert

Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 15:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 15:
SELECT	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 14: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 15: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.6 MF / EF.C.CA_SMC.CS.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SMC.CS.E256 einer CA enthält.

⌦ **Card-G2-A_2160 (N701.600) K_Personalisierung: Attribute MF / EF.C.CA_SMC.CS.E256**

EF.C.CA_SMC.CS.E256 MUSS die in Tab_SMC-B_ObjSys_009 dargestellten Werte besitzen.

Tabelle 9: Tab_SMC-B_ObjSys_009 Attribute MF / EF.C.CA_SMC.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 07´	
shortFileIdentifier	´07´= 7	
numberOfOctet	´00DC´ Oktett = 220 Oktett	
flagTransactionMode	False	
flagChecksum	False	

lifeCycleStatus	„Operational state (activated)“	
body	´7F21 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 17:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 17:
SELECT	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 16: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 17: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.7 MF / EF.C.CA_SMC.CS.E384 (optional)

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SMC.CS.E384 einer CA enthält.

⌦ **Card-G2-A_2161 (N701.700) K_Personalisierung: Attribute MF / EF.C.CA_SMC.CS.E384**

EF.C.CA_SMC.CS.E384 MUSS die in Tab_SMC-B_ObjSys_010 dargestellten Werte besitzen.

Tabelle 10: Tab_SMC-B_ObjSys_010 Attribute MF / EF.C.CA_SMC.CS.E384

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 0D´	
shortFileIdentifier	´0D´= 13	
numberOfOctet	´011D´ Oktett = 285 Oktett	

flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7F21 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 19:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 19:
SELECT	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 18: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 19: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.8 MF / EF.C.SMC.AUTR_CVC.R2048

EF.C.SMC.AUTR_CVC.R2048 enthält das CV-Zertifikat der SMC-B für die Kryptographie mit RSA für rollenbasierte C2C-Authentisierung zwischen SMC-B und eGK. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTR_CVC.R2048 ist im Kapitel 4.3.18 definiert.

⌦ **Card-G2-A_2162 (N701.800) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTR_CVC.R2048**

EF.C.SMC.AUTR_CVC.R2048 MUSS die in Tab_SMC-B_ObjSys_011 dargestellten Werte besitzen.

Tabelle 11: (Tab_SMC-B_ObjSys_011) Attribute von MF / EF.C.SMC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 03´	
shortFileIdentifier	´03´= 3	
numberOfOctet	´0155´ Oktett = 341 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 21:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 21:
SELECT	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 20: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 21: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.9 MF / EF.C.SMC.AUTR_CVC.E256

EF.C.SMC.AUTR_CVC.E256 enthält das CV-Zertifikat der SMC-B für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen SMC-B und eGK. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTR_CVC.E256 ist im Kapitel 4.3.19 definiert.

⌦ **Card-G2-A_2163 (N701.900) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTR_CVC.E256**

EF.C.SMC.AUTR_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_012 dargestellten Werte besitzen.

Tabelle 12: (Tab_SMC-B_ObjSys_012) Attribute von MF / EF.C.SMC.AUTR_CVC.E256

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 06´	
shortFileIdentifier	´06´= 6	
numberOfOctet	´00DE´ Oktett = 222 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	Xx …xxx	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 23:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 23:
SELECT	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 22: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 23: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.10 MF / EF.C.SMC.AUTR_CVC.E384 (optional)

EF.C.SMC.AUTR_CVC.E384 enthält das CV-Zertifikat der SMC-B für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen SMC-B und eGK. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTR_CVC.E384 ist im Kapitel 4.3.20 definiert.

⌦ **Card-G2-A_2164 (N702.000) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTR_CVC.E384**

EF.C.SMC.AUTR_CVC.E384 MUSS die in Tab_SMC-B_ObjSys_013 dargestellten Werte besitzen.

Tabelle 13: (Tab_SMC-B_ObjSys_013) Attribute von MF / EF.C.SMC.AUTR_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 0C´	
shortFileIdentifier	´0C´= 12	
numberOfOctet	´011F´ Oktett = 287 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
Body	Xx … xx´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 25:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 25:
SELECT	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 24: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 25: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.11 MF / EF.C.SMC.AUTD_RPS_CVC.R2048

EF.C.SMC.AUTD_RPS_CVC.R2048 enthält das CV-Zertifikat einer SMC-B für die Kryptographie mit RSA für funktionsbasierte C2C-Authentisierungsprozesse zur Übertragung einer eingegebenen PIN an einen HBA oder einen RFID-Token, siehe Anmerkung. Dieses Zertifikat kann ohne PIN-Authentisierung genutzt werden. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPS_CVC.R2048 ist im Kapitel 4.3.21 definiert.

ANMERKUNG – Sowohl die Präsentation des RFID-Tokens, als auch die PIN-Eingabe für einen RFID-Token erfolgt lokal voraussichtlich an demselben Authentisierungsterminal, nutzt aber den Modus für entfernte PIN-Übertragung, um die Daten an der Luftschnittstelle abzusichern.

⌦ **Card-G2-A_2165 (N702.100) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.R2048**

EF.C.SMC.AUTD_RPS_CVC.R2048 MUSS die in Tab_SMC-B_ObjSys_014 dargestellten Werte besitzen.

Tabelle 14: Tab_SMC-B_ObjSys_014 Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 11´	
shortFileIdentifier	´11´= 17	
numberOfOctet	´0155´ Oktett = 341 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7F21 820150 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 27:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 27:
SELECT	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 26: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 27: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.12 MF / EF.C.SMC.AUTD_RPS_CVC.E256

EF.C.SMC.AUTD_RPS_CVC.E256 enthält das CV-Zertifikat einer SMC-B für die Kryptographie mit elliptischen Kurven für funktionsbasierte C2C-Authentisierungsprozesse zur Übertragung einer eingegebenen PIN an einen HBA oder einen RFID-Token, siehe Anmerkung. Dieses Zertifikat kann ohne PIN-Authentisierung genutzt werden. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPS_CVC.E256 ist im Kapitel 4.3.22 definiert.

ANMERKUNG – Sowohl die Präsentation des RFID-Tokens als auch die PIN-Eingabe für ein RFID-Token erfolgt lokal voraussichtlich an demselben Authentisierungsterminal, nutzt aber den Modus für entfernte PIN-Übertragung, um die Daten an der Luftschnittstelle abzusichern.

⌦ **Card-G2-A_2166 (N702.200) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256**

EF.C.SMC.AUTD_RPS_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_015 dargestellten Werte besitzen.

Tabelle 15: Tab_SMC-B_ObjSys_015 Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 0A´	
shortFileIdentifier	´0A´= 10	
numberOfOctet	´00DE´ Oktett = 222 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7F21 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		

Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 29:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMSc	siehe Hinweis 29:
SELECT	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 28: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 29: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.13 MF / EF.C.SMC.AUTD_RPS_CVC.E384 (optional)

EF.C.SMC.AUTD_RPS_CVC.E384 enthält das CV-Zertifikat einer SMC-B für die Kryptographie mit elliptischen Kurven für funktionsbasierte C2C-Authentisierungsprozesse zur Übertragung einer eingegebenen PIN an einen HBA oder einen RFID-Token, siehe Anmerkung. Dieses Zertifikat kann ohne PIN-Authentisierung genutzt werden. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPS_CVC.E384 ist im Kapitel 4.3.23 definiert.

ANMERKUNG – Sowohl die Präsentation des RFID-Tokens, als auch die PIN-Eingabe für einen RFID-Token erfolgt lokal voraussichtlich an demselben Authentisierungsterminal, nutzt aber den Modus für entfernte PIN-Übertragung, um die Daten an der Luftschnittstelle abzusichern.

⌦ **Card-G2-A_2167 (N702.300) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E384**

EF.C.SMC.AUTD_RPS_CVC.E384 MUSS die in Tab_SMC-B_ObjSys_016 dargestellten Werte besitzen.

Tabelle 16: Tab_SMC-B_ObjSys_016 Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 0F´	

shortFileIdentifier	´0F´= 15	
numberOfOctet	´011F´ Oktett = 287 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7F21 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 31:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 31:
SELECT	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 30: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 31: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.14 MF / EF.C.SMC.AUTD_RPE_CVC.R2048

EF.C.SMC.AUTD_RPE_CVC.R2048 enthält das CV-Zertifikat für die Kryptographie mit RSA für die C2C-Geräteauthentisierung zwischen SMC-B und einer SMC-B als entfernter PIN-Empfänger. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPE_CVC.R2048 ist im Kapitel 4.3.24 definiert.

⌦ **Card-G2-A_2168 (N702.400) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.R2048**

EF.C.SMC.AUTD_RPE_CVC.R2048 MUSS die in Tab_SMC-B_ObjSys_017 dargestellten Werte besitzen.

Tabelle 17: Tab_SMC-B_ObjSys_017 Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 05´	
shortFileIdentifier	´05´= 5	
numberOfOctet	´0155´ Oktett = 341 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body		wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 33:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 33:
SELECT	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 32: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 33: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.15 MF / EF.C.SMC.AUTD_RPE_CVC.E256

EF.C.SMC.AUTD_RPE_CVC.E256 enthält das CV-Zertifikat für die Kryptographie mit elliptischen Kurven für die C2C-Geräteauthentisierung zwischen einer lokal vorhandenen SMC-B und einer SMC-B als entferntem PIN-Empfänger. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPE_CVC.E256 ist im Kapitel 4.3.25 definiert.

⌦ **Card-G2-A_2169 (N702.500) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256**

EF.C.SMC.AUTD_RPE_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_018 dargestellten Werte besitzen.

Tabelle 18: (Tab_SMC-B_ObjSys_018) Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 09´	
shortFileIdentifier	´09´= 9	
numberOfOctet	´00DE´ Oktett = 222 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	Xx … xxx	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 35:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 35:
SELECT	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 34: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 35: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.16 MF / EF.C.SMC.AUTD_RPE_CVC.E384 (optional)

EF.C.SMC.AUTD_RPE_CVC.E384 enthält das CV-Zertifikat für die Kryptographie mit elliptischen Kurven für die C2C-Geräteauthentisierung zwischen einer lokal vorhandenen SMC-B und einer SMC-B als entferntem PIN-Empfänger. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPE_CVC.E384 ist im Kapitel 4.3.26 definiert.

⌦ **Card-G2-A_2170 (N702.600) K_Personalisierung: Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E384**

EF.C.SMC.AUTD_RPE_CVC.E384 MUSS die in Tab_SMC-B_ObjSys_019 dargestellten Werte besitzen.

Tabelle 19: Tab_SMC-B_ObjSys_019 Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 0E´	
shortFileIdentifier	´0E´= 14	
numberOfOctet	´011F´ Oktett = 287 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	Xx … xx	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 37:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 37:
SELECT	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 36: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 37: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.17 MF / PIN.SMC

Dieses Passwortobjekt wird zur Freischaltung von Schlüsseln und Inhalten der SMC-B verwendet.

⌧ **Card-G2-A_2171 (N702.700) K_Personalisierung: Attribute von MF / PIN.SMC**

PIN.SMC MUSS die in Tab_SMC-B_ObjSys_020 dargestellten Werte besitzen.

Tabelle 20: Tab_SMC-B_ObjSys_020 Attribute von MF / PIN.SMC

Attribute	Wert	Bemerkung
Objekttyp	Reguläres Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	
MaximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword, Transport-PIN}	
flagEnabled	True	
startSsec	unendlich	
PUK	…	wird personalisiert
pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	ALWAYS	
VERIFY	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 38: 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

⌦ **Card-G2-A_2172 (N702.800) K_Personalisierung: Länge der PUK für der SMC-B**

Bei der Personalisierung MUSS eine PUK mit acht Ziffern gewählt werden. ⌫

4.3.18 MF / PrK.SMC.AUTR_CVC.R2048

PrK.SMC.AUTR_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für die C2C-Authentisierung zwischen SMC-B/eGK. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTR_CVC.R2048 ist in C.SMC.AUTR_CVC.R2048 (siehe Kapitel 4.3.8) enthalten.

⌦ **Card-G2-A_2173 (N702.820) K_Personalisierung: Freischaltung der SMC-B einer Institution mit Ausnahme eines Krankenhauses (PrK.SMC.AUTR_CVC.R2048)**

Der private Schlüssel PrK.SMC.AUTR_CVC.R2048 der SMC-B einer Institution mit Ausnahme eines Krankenhauses DARF NICHT durch einen HBA freigeschaltet werden können, der ein anderes Profil (einen anderen Hex-Wert) als die SMC-B selbst aufweist. ⌫

⌦ **Card-G2-A_2174 (N702.840) K_Personalisierung: Verpflichtende Regeln für die Freischaltung der SMC-B eines Krankenhauses (PrK.SMC.AUTR_CVC.R2048)**

Der private Schlüssel PrK.SMC.AUTR_CVC.R2048 der SMC-B eines Krankenhauses MUSS außer durch Eingabe der PIN.SMC auch durch das Profil 2 (den Hex-Wert ’00 5D29 FAAA 8000’) freigeschaltet werden. ⌫

⌦ **Card-G2-A_2175 (N702.860) K_Personalisierung: Optionale Regeln für die Freischaltung der SMC-B eines Krankenhauses (PrK.SMC.AUTR_CVC.R2048)**

Der private Schlüssel PrK.SMC.AUTR_CVC.R2048 der SMC-B eines Krankenhauses KANN außer durch das Profil 2 (den Hex-Wert ’00 5D29 FAAA 8000’) auch durch einen HBA mit Profil 3 (Hex-Wert ´00 5C42 FAA8 8000´), Profil 4 (Hex-Wert ´00 4C42 FAAA 8000´) oder Profil 5 (Hex-Wert ´00 5C00 02A8 0000´) freigeschaltet werden. Es liegt im Ermessen des jeweiligen Krankenhauses, entweder alle oder

nur einen Teil der zusätzlichen Profile (Hex-Werte) zur Freischaltung der SMC-B zuzulassen. ⌫

⌦ **Card-G2-A_2176 (N702.900) K_Personalisierung: Attribute von MF / PrK.SMC.AUTR_CVC.R2048**

PrK.SMC.AUTR_CVC.R2048 MUSS die in Tab_SMC-B_ObjSys_021 dargestellten Werte besitzen.

Tabelle 21: Tab_SMC-B_ObjSys_021 Attribute von MF / PrK.SMC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´10´ = 16	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge {rsaRoleAuthentication, rsaSessionkey4SM, rsaSessionkey4TC}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 42:
INTERNAL AUTH.	SMC-B in einer Institution außer einem Krankenhaus PWD(PIN.SMC) OR AUT(‘D27600004000’ || ‘xx’) OR AUT(‘yy.....yy’)	siehe Hinweis 40:
INTERNAL AUTH.	SMC-B in einem Krankenhaus PWD(PIN.SMC): OR AUT(‘D27600004000’ || '02') OR beliebige Elemente aus der Menge {‘D27600004000’ || '03', ‘D27600004000’ || '04' ‘D27600004000’ || '05'} OR AUT(‘00 5D29 FAAA 8000’) OR beliebige Elemente aus der Menge {´00 5C42 FAA8 8000´, ´00 4C42 FAAA 8000’, ´00 5C00 02A8 0000´}	siehe Hinweis 41:
TERMINATE	AUT_CMS	siehe Hinweis 42:

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 39: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 40: SMC-B in einer Institution außer einem Krankenhaus: Authentisierung mit PIN.SMC oder Rollenauthentisierung mit einem HBA oder SMC mit zugehörigem persönlichen Profil 'xx', z.B. Profil 2 (Generation 1) oder einem Hex-Wert 'yy.....yy', der der Flagliste eines entsprechenden HBA oder einer entsprechenden SMC entspricht (Generation 2), siehe Anhang H von [gemSpec_COS]. xx' muss auf der SMC-B und der freischaltenden Karte identisch sein, d.h. z.B., dass die SMC-B einer Arztpraxis nur von einem HBA mit Profil 2 (bzw. entsprechenden Hex-Wert) freigeschaltet werden darf.

Hinweis 41: SMC-B in einem Krankenhaus: Die SMC eines Krankenhauses besitzt dieselben Zugriffsrechte auf eine eGK wie die SMC einer Arzt- oder Zahnarztpraxis. Während die SMC einer Praxis jedoch ausschließlich (ungeachtet der Eingabe von PIN.SMC) durch den HPC eines Arztes oder Zahnarztes autorisiert werden kann, sind möglicherweise die Profile mehrerer Berufsgruppen berechtigt, die SMC in einem Krankenhaus zu autorisieren. Die aufgeführten Profile stellen die maximal zugelassenen Profile dar. Die zuständige Institution kann daraus eine Untermenge festlegen, die zur Autorisierung einer bestimmten SMC berechtigt ist.

Hinweis 42: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

Der öffentliche Schlüssel, der zu PrK.SMC.AUTR_CVC.R2048 (mit Profil des CVC-Inhabers), gehört, ist in C.SMC.AUTR_CVC.R2048 enthalten.

4.3.19 MF / PrK.SMC.AUTR_CVC.E256

PrK.SMC.AUTR_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/eGK. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTR_CVC.E256 ist in C.SMC.AUTR_CVC.E256 (siehe Kapitel 4.3.9) enthalten.

⌦ **Card-G2-A_2177 (N702.920) K_Personalisierung: Freischaltung der SMC-B einer Institution mit Ausnahme eines Krankenhauses (PrK.SMC.AUTR_CVC.E256)**

Der private Schlüssel PrK.SMC.AUTR_CVC.E256 der SMC-B einer Institution mit Ausnahme eines Krankenhauses DARF NICHT durch einen HBA freigeschaltet werden können, der ein anderes Profil (einen anderen Hex-Wert) als die SMC-B selbst aufweist. ⌫

⌦ **Card-G2-A_2178 (N702.940) _Personalisierung: Verpflichtende Regeln für die Freischaltung der SMC-B eines Krankenhauses (PrK.SMC.AUTR_CVC.E256)**

Der private Schlüssel PrK.SMC.AUTR_CVC.E256 der SMC-B eines Krankenhauses MUSS außer durch Eingabe der PIN.SMC auch durch das Profil 2 (den Hex-Wert '00 5D29 FAAA 8000') freigeschaltet werden. ⌫

⌦ **Card-G2-A_2179 (N702.960) _Personalisierung: Optionale Regeln für die Freischaltung der SMC-B eines Krankenhauses (PrK.SMC.AUTR_CVC.E256)**

Der private Schlüssel PrK.SMC.AUTR_CVC.E256 der SMC-B eines Krankenhauses KANN außer durch das Profil 2 (den Hex-Wert '00 5D29 FAAA 8000') auch durch einen HBA mit Profil 3 (Hex-Wert ´00 5C42 FAA8 8000´), Profil 4 (Hex-Wert ´00 4C42 FAAA 8000´) und Profil 5 (Hex-Wert ´00 5C00 02A8 0000´) freigeschaltet werden. Es liegt im Ermessen des jeweiligen Krankenhauses, entweder alle oder nur einen Teil der zusätzlichen Profile (Hex-Werte) zur Freischaltung der SMC-B zuzulassen. ⌫

⌦ **Card-G2-A_2180 (N703.000) K_Personalisierung: Attribute von MF / PrK.SMC.AUTR_CVC.E256**

PrK.SMC.AUTR_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_022 dargestellten Werte besitzen.

Tabelle 22: Tab_SMC-B_ObjSys_022 Attribute von MF / PrK.SMC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´06´ = 6	
privateKey	Domainparameter = brainpoolP256r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge {elcRoleAuthentication, elcSessionkey4SM, elcSessionkey4TC}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 46:
INTERNAL AUTH.	SMC-B in einer Institutionen außer einem Krankenhaus	siehe Hinweis 44:

	PWD(PIN.SMC) OR AUT(‘D27600004000’ || ‘xx’) OR AUT(‘yy.....yy’)	
INTERNAL AUTH.	SMC-B in einem Krankenhaus PWD(PIN.SMC): OR AUT(‘D27600004000’ || '02') OR beliebige Elemente aus der Menge {‘D27600004000’ || '03', ‘D27600004000’ || '04' ‘D27600004000’ || '05'} OR AUT(’00 5D29 FAAA 8000’) OR beliebige Elemente aus der Menge {´00 5C42 FAA8 8000´, ´00 4C42 FAAA 8000’, ´00 5C00 02A8 0000´}	Siehe Hinweis 45:
TERMINATE	AUT_CMS	siehe Hinweis 46:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 43: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 44: SMC-B in einer Institution außer einem Krankenhaus: Authentisierung mit PIN.SMC oder Rollenauthentisierung mit einem HBA oder SMC mit zugehörigem persönlichen Profil ’xx’, z.B. Profil 2 (Generation 1) oder einem Hex-Wert ‘yy…..yy’, der der Flagliste eines entsprechenden HBA oder einer entsprechenden SMC entspricht (Generation 2), siehe Anhang H von [gemSpec_COS]. ’xx’ muss auf der SMC-B und dem freischaltenden HBA identisch sein, d.h. z.B., dass die SMC-B einer Arztpraxis nur von einem HBA mit Profil 2 (bzw. entsprechenden Hex-Wert) freigeschaltet werden darf.

Hinweis 45: SMC-B in einem Krankenhaus: Die SMC eines Krankenhauses besitzt dieselben Zugriffsrechte auf eine eGK wie die SMC einer Arzt- oder Zahnarztpraxis. Während die SMC einer Praxis jedoch ausschließlich (ungeachtet der Eingabe von PIN.SMC) durch den HPC eines Arztes oder Zahnarztes autorisiert werden kann, sind möglicherweise die Profile mehrerer Berufsgruppen berechtigt, die SMC in einem Krankenhaus zu autorisieren. Die aufgeführten Profile stellen die maximal zugelassenen Profile dar. Die zuständige Institution

kann daraus eine Untermenge festlegen, die zur Autorisierung einer bestimmten SMC berechtigt ist..

Hinweis 46: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.20 MF / PrK.SMC.AUTR_CVC.E384 (optional)

PrK.SMC.AUTR_CVC.E384 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/eGK. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTR_CVC.E384 ist in C.SMC.AUTR_CVC.E384 (siehe Kapitel 4.3.10) enthalten.

⌦ **Card-G2-A_2181 (N703.020) Personalisierung: Freischaltung der SMC-B einer Institution mit Ausnahme eines Krankenhauses (PrK.SMC.AUTR_CVC.E384)**

Der private Schlüssel PrK.SMC.AUTR_CVC.E384 der SMC-B einer Institution mit Ausnahme eines Krankenhauses DARF NICHT durch einen HBA freigeschaltet werden können, der ein anderes Profil (einen anderen Hex-Wert) als die SMC-B selbst aufweist. ⌫

⌦ **Card-G2-A_2182 (N703.040) K_Personalisierung: Verpflichtende Regeln für die Freischaltung der SMC-B eines Krankenhauses (PrK.SMC.AUTR_CVC.E384)**

Der private Schlüssel PrK.SMC.AUTR_CVC.E384 der SMC-B eines Krankenhauses MUSS außer durch Eingabe der PIN.SMC auch durch das Profil 2 (den Hex-Wert ’00 5D29 FAAA 8000’) freigeschaltet werden. ⌫

⌦ **Card-G2-A_2183 (N703.060) K_Personalisierung: Optionale Regeln für die Freischaltung der SMC-B eines Krankenhauses (PrK.SMC.AUTR_CVC.E384)**

Der private Schlüssel PrK.SMC.AUTR_CVC.E384 der SMC-B eines Krankenhauses KANN außer durch das Profil 2 (den Hex-Wert ’00 5D29 FAAA 8000’) auch durch einen HBA mit Profil 3 (Hex-Wert ´00 5C42 FAA8 8000´), Profil 4 (Hex-Wert ´00 4C42 FAAA 8000´) und Profil 5 (Hex-Wert ´00 5C00 02A8 0000´) freigeschaltet werden. Es liegt im Ermessen des jeweiligen Krankenhauses, entweder alle oder nur einen Teil der zusätzlichen Profile (Hex-Werte) zur Freischaltung der SMC-B zuzulassen. ⌫

⌦ **Card-G2-A_2184 (N703.100) K_Personalisierung: Attribute von MF / PrK.SMC.AUTR_CVC.E384**

PrK.SMC.AUTR_CVC.E384 MUSS die in Tab_SMC-B_ObjSys_023 dargestellten Werte besitzen.

Tabelle 23: Tab_SMC-B_ObjSys_023 Attribute von MF / PrK.SMC.AUTR_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´0C´ = 12	

privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge {elcRoleAuthentication, elcSessionkey4SM, elcSessionkey4TC}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 50:
INTERNAL AUTH.	SMC-B in einer Institutionen außer einem Krankenhaus PWD(PIN.SMC) OR AUT(‘D27600004000’ || ‘xx’) OR AUT(‘yy.....yy’)	siehe Hinweis 48:
INTERNAL AUTH.	SMC-B in einem Krankenhaus PWD(PIN.SMC): OR AUT(‘D27600004000’ || '02') OR beliebige Elemente aus der Menge {‘D27600004000’ || '03', ‘D27600004000’ || '04' ‘D27600004000’ || '05'} OR AUT(’00 5D29 FAAA 8000’) OR beliebige Elemente aus der Menge {´00 5C42 FAA8 8000´, ´00 4C42 FAAA 8000’, ´00 5C00 02A8 0000´}	siehe Hinweis 49:
TERMINATE	AUT_CMS	siehe Hinweis 50:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

*Hinweis 47: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE*

Hinweis 48: SMC-B in einer Institution außer einem Krankenhaus: Authentisierung mit PIN.SMC oder Rollenauthentisierung mit einem HBA oder SMC mit zugehörigem persönlichen Profil 'xx', z.B. Profil 2 (Generation 1) oder einem Hex-Wert 'yy.....yy' der der Flagliste eines entsprechenden HBA oder einer entsprechenden SMC entspricht (Generation 2), siehe Anhang H von [gemSpec_COS]. 'xx' muss auf der SMC-B und dem freischaltenden HBA identisch sein, d.h. z.B., dass die SMC-B einer Arztpraxis nur von einem HBA mit Profil 2 (bzw. entsprechenden Hex-Wert) freigeschaltet werden darf.

Hinweis 49: SMC-B in einem Krankenhaus: Die SMC eines Krankenhauses besitzt dieselben Zugriffsrechte auf eine eGK wie die SMC einer Arzt- oder Zahnarztpraxis. Während die SMC einer Praxis jedoch ausschließlich (ungeachtet der Eingabe von PIN.SMC) durch den HPC eines Arztes oder Zahnarztes autorisiert werden kann, sind möglicherweise die Profile mehrerer Berufsgruppen berechtigt, die SMC in einem Krankenhaus zu autorisieren. Die aufgeführten Profile stellen die maximal zugelassenen Profile dar. Die zuständige Institution kann daraus eine Untermenge festlegen, die zur Autorisierung einer bestimmten SMC berechtigt ist.

Hinweis 50: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.21 MF / PrK.SMC.AUTD_RPS_CVC.R2048

PrK.SMC.AUTD_RPS_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für die C2C-Authentisierung zwischen SMC-B/HBA, SMC-B/SMC-B oder SMC-B/RFID-Token in der Funktion des PIN-Senders. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPS_CVC.R2048 ist in C.SMC.AUTD_RPS_CVC.R2048 (siehe Kapitel 4.3.11) enthalten.

⌦ **Card-G2-A_2185 (N703.200) K_Personalisierung: Attribute von MF / PrK.SMC.AUTD_RPS_CVC.R2048**

PrK.SMC.AUTD_RPS_CVC.R2048 MUSS die in Tab_SMC-B_ObjSys_024 dargestellten Werte besitzen.

Tabelle 24: Tab_SMC-B_ObjSys_024 Attribute von MF / PrK.SMC.AUTD_RPS_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´11´ = 17	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge { rsaSessionkey4TC}	
lifeCycleStatus	„Operational state (activated)“	
accessRulesSessionkeys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=ALWAYS	

Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS AND SmCmdEnc	siehe Hinweis 53:
INTERNAL AUTH.	[SmMac(‘D27600004000’ || '35') OR [SmMac(‘D27600004000’ || '37')	siehe Hinweis 52:
TERMINATE	AUT_CMS	siehe Hinweis 53:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 51: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 52: Funktionale Geräteauthentisierung einer SMC (SSCD mit Profil 53) oder RFID-Token (PIN-Empfänger mit Profil 55).

Hinweis 53: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.22 MF / PrK.SMC.AUTD_RPS_CVC.E256

PrK.SMC.AUTD_RPS_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/HBA, SMC-B/SMC-B oder SMC-B/RFID-Token in der Funktion des PIN-Senders. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPS_CVC.E256 ist in C.SMC.AUTD_RPS_CVC.E256 (siehe Kapitel 4.3.12) enthalten.

⌦ **Card-G2-A_2186 (N703.300) K_Personalisierung: Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256**

PrK.SMC.AUTD_RPS_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_025 dargestellten Werte besitzen.

Tabelle 25: Tab_SMC-B_ObjSys_025 Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´0A´ = 10	
privateKey	Domainparameter = brainpoolP256r1	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge {elcSessionkey4TC}	
lifeCycleStatus	„Operational state (activated)“	
accessRulesSessionkeys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 56:
INTERNAL AUTH.	SmMac(cvc_FlagList_TI, flag=53) OR SmMac(cvc_FlagList_TI, flag=55)	siehe Hinweis 55:
TERMINATE	AUT_CMS	siehe Hinweis 56:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 54: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 55: Funktionale Geräteauthentisierung einer SMC (SSCD mit Flag=53) oder RFID-Token (PIN-Empfänger mit Flag=55), cvc:Flaglist_TI siehe Anhang H4 von [gemSpec_COS].

Hinweis 56: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.3.23 MF / PrK.SMC.AUTD_RPS_CVC.E384 (optional)

PrK.SMC.AUTD_RPS_CVC.E384 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/HBA, SMC-B/SMC-

B oder SMC-B/RFID-Token in der Funktion des PIN-Senders. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPS_CVC.E384 ist in C.SMC.AUTD_RPS_CVC.E384 (siehe Kapitel 4.3.13) enthalten.

⌦ **Card-G2-A_2187 (N703.400) K_Personalisierung: Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E384**

PrK.SMC.AUTD_RPS_CVC.E384 MUSS die in Tab_SMC-B_ObjSys_026 dargestellten Werte besitzen.

Tabelle 26: Tab_SMC-B_ObjSys_026 Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E384

Attribute	**Wert**	**Bemerkung**
Objekttyp	private ELC Authentisierungsobjekt	
keyIdentifier	´0F´ = 15	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge {elcSessionkey4TC,}	
lifeCycleStatus	„Operational state (activated)“	
accessRulesSessionkeys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 59:
INTERNAL AUTH.	SmMac(cvc_FlagList_TI, flag=53) OR SmMac(cvc_FlagList_TI, flag=55)	siehe Hinweis 58:
TERMINATE	AUT_CMS	siehe Hinweis 59:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 57: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE

ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 58: Funktionale Geräteauthentisierung einer SMC (SSCD mit Flag=53) oder RFID-Token (PIN-Empfänger mit Flag=55), cvc:Flaglist_TI siehe Anhang H4 von [gemSpec_COS]

Hinweis 59: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.24 MF / PrK.SMC.AUTD_RPE_CVC.R2048

PrK.SMC.AUTD_RPE_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für die C2C-Authentisierung zwischen SMC-B/SMC-B in der Funktion des PIN-Empfängers. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPE_CVC.R2048 ist in C.SMC.AUTD_RPE_CVC.R2048 (siehe Kapitel 4.3.14) enthalten.

⌧ **Card-G2-A_2188 (N703.500) K_Personalisierung: Attribute von MF / PrK.SMC.AUTD_RPE_CVC.R2048**

PrK.SMC.AUTD_RPE_CVC.R2048 MUSS die in Tab_SMC-B_ObjSys_027 dargestellten Werte besitzen.

Tabelle 27: Tab_SMC-B_ObjSys_027 Attribute von MF / PrK.SMC.AUTD_RPE_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	Profil 55 (PIN-Empfänger)
keyIdentifier	´05´ = 0	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge {rsaSessionkey4SM}	
accessRuleSessionkeys	irrelevant	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 61:
INTERNAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 61:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		

Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 60: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 61: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.25 MF / PrK.SMC.AUTD_RPE_CVC.E256

PrK.SMC.AUTD_RPE_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/SMC-B in der Funktion des PIN-Empfängers. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPE_CVC.E256 ist in C.SMC.AUTD_RPE_CVC.E256 (siehe Kapitel 4.3.15) enthalten.

⌦ **Card-G2-A_2189 (N703.600) K_Personalisierung: Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256**

PrK.SMC.AUTD_RPE_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_028 dargestellten Werte besitzen.

Tabelle 28: Tab_SMC-B_ObjSys_028 Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates ELC-Authentisierungsobjekt	Profil 55 (PIN-Empfänger)
keyIdentifier	´0A´ = 10	
privateKey	Domainparameter = brainpoolP256r1	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge { elcSessionkey4SM}	
accessRuleSessionkeys	irrelevant	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 63:

INTERNAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 63:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 62: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 63: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.26 MF / PrK.SMC.AUTD_RPE_CVC.E384 (optional)

PrK.SMC.AUTD_RPE_CVC.E384 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/SMC-B in der Funktion des PIN-Empfängers. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPE_CVC.E384 ist in C.SMC.AUTD_RPE_CVC.E384 (siehe Kapitel 4.3.16) enthalten.

⌦ **Card-G2-A_2190 (N703.700) K_Personalisierung: Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E384**

PrK.SMC.AUTD_RPE_CVC.E384 MUSS die in Tab_SMC-B_ObjSys_029 dargestellten Werte besitzen.

Tabelle 29: Tab_SMC-B_ObjSys_029 Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC-Authentisierungsobjekt	Profil 55 (PIN-Empfänger)
keyIdentifier	´0E´ = 14	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge { elcSessionkey4SM}	
accessRuleSession	irrelevant	

keys		
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 65:
INTERNAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 65:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 64: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 65: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.27 MF / PuK.RCA.CS.R2048

PuK.RCA.CS.R2048 ist der öffentliche Schlüssel der Root-CA des Gesundheitswesens für die Kryptographie mit RSA für die Prüfung von CVC-Zertifikaten, die von dieser herausgegeben werden.

⌦ **Card-G2-A_2191 (N703.800) K_Personalisierung: Attribute von MF / PuK.RCA.CS.R2048**

PuK.RCA.CS.R2048 MUSS die in Tab_SMC-B_ObjSys_030 dargestellten Werte besitzen.

Tabelle 30: Tab_SMC-B_ObjSys_030 Attribute von MF / PuK.RCA.CS.R2048

Attribute	Wert	Bemerkung
Objekttyp	öffentliches RSA Signaturprüfobjekt	

keyIdentifier	RSA 2048 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes)	wird personalisiert
publicKey	…, Moduluslänge 2048 Bit	wird personalisiert
oid	sigS_ISO9796-2Withrsa_sha256 ´2B240304020204´ = {1.3.36.3.4.2.2.4}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Verify Cert.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 67:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 66: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen RSA-Signaturprüfobjekt arbeiten, sind:
PSO Verify Certificate, TERMINATE

Hinweis 67: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.28 MF / PuK.RCA.CS.E256

PuK.RCA.CS.E256 ist der öffentliche Schlüssel der Root-CA des Gesundheitswesens für die Kryptographie mit elliptischen Kurven für die Prüfung von CVC-Zertifikaten, die von dieser herausgegeben werden.

⌦ **Card-G2-A_2192 (N703.900) K_Personalisierung: Attribute von MF / PuK.RCA.CS.E256**

PuK.RCA.CS.E256 MUSS die in Tab_SMC-B_ObjSys_031 dargestellten Werte besitzen.

Tabelle 31: Tab_SMC-B_ObjSys_031 Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Signaturprüfobjekt	
keyIdentifier	ELC 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes)	wird personalisiert
expirationDate		wird personalisiert
CHAT	• OIDflags = cvc_Flags_TI • flagList = ´FF 0000 0000 7FE6´	
publicKey	Domainparameter = brainpoolP256r1	wird personalisiert
oid	ecdsa-with-SHA256 ´2A8648CE3D040302´ = {1.2.840.10045.4.3.2}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Verify Cert.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 69:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 68: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen ELC-Signaturprüfobjekt arbeiten, sind:
PSO Verify Certificate, TERMINATE,

Hinweis 69: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.29 MF / PuK.RCA.CS.E384 (optional)

PuK.RCA.CS.E384 enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E384-Hierarchie steht. Er wird zur Prüfung von CV-Zertifikaten der zweiten Ebene unter Nutzung elliptischer Kryptographie benötigt.

Es ist nicht erforderlich, dass PuK.RCA.CS.E384 bei Ausgabe der Karte vorhanden ist; er wird im Feld bei Aktivierung der Schlüssellänge 384 bit über ein Cross-Zertifikat zu der

Root für 256 bit (zu der der öffentliche Schlüssel PuK.RCA.CS.E256 gehört, siehe Kapitel 4.3.28) in die Karte geladen.

⌦ **Card-G2-A_2671 (N704.000) K_Personalisierung: Attribute von PuK.RCA.CS.E384**

Die Attribute von PuK.RCA.CS.E384 MÜSSEN bis auf den keyIdentifier, den Domainparameter und die oid mit den Attributen von PuK.RCA.CS.E256 identisch sein.

Für die oid MUSS der Wert für ecdsa-with-SHA384 (´2A8648CE3D040303´ = {1.2.840.10045.4.3.3}) eingetragen werden.

Der keyIdentifier MUSS den Wert E 384 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes) aufweisen.

Für den Domainparameter gilt: Domainparameter = brainpoolP384r1⌫

4.3.30 MF / PuK.CMS_SMC-B.AUT_CVC.E256 (optional)

PuK.CMS_SMC-B.AUT_CVC.E256 (optional) ist der öffentliche Schlüssel für die Kryptographie mit elliptischen Kurven zur Durchführung des SMC-B/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.

⌦ **Card-G2-A_2193 (N704.100) K_Personalisierung: Attribute von MF / PuK.CMS_SMC-B.AUT_CVC.E256**

PuK.CMS_SMC-B.AUT_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_032 dargestellten Werte besitzen.

Tabelle 32: Tab_SMC-B_ObjSys_032 Attribute von MF / PuK.CMS_SMC-B.AUT_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Authentisierungsobjekt	
keyIdentifier	´XX…YY´, zwölf Oktette	wird personalisiert
expirationDate		wird personalisiert
CHAT	cvc_FlagList_CMS, flag=08 gesetzt	
publicKey	Domainparameter = brainpoolP256r1	wird personalisiert
oid	authS_gemSpec-COS-G2_ecc-with-sha256 ´2B2403050301´ = {1.3.36.3.5.3.1}	
Algorithm Identifier	elcSessionkey4SM	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

GENERAL AUTHENTICATE	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 71:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

*Hinweis 70: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen ELC-Authentisierungsobjekt arbeiten, sind:
INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE, TERMINATE,*

Hinweis 71: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.31 MF / PuK.CMS_SMC-B.AUT_CVC.E384 (optional)

PuK.CMS_SMC-B.AUT_CVC.E384 (optional) ist der öffentliche Schlüssel für die Kryptographie mit elliptischen Kurven, mit dem eine Authentisierung zwischen SMC-B und CMS mit der Einrichtung eines TC durchgeführt wird.

PuK.CMS_SMC-B.AUT_CVC.E384 wird verwendet, wenn ein CMS mit asymmetrischer Authentisierung mit elliptischen Kurven und der Schlüssellänge 384 bit genutzt werden soll. Es ist nicht erforderlich, dass der Schlüssel bei Ausgabe der Karte vorhanden ist; er wird im Feld bei Aktivierung der Schlüssellänge 384 bit über ein Cross-Zertifikat zu der Root für 256 bit (zu der der öffentliche Schlüssel PuK.CMS_SMC-B.AUT_CVC.E256 gehört, siehe Kapitel 4.3.30) in die Karte geladen.

⌦ Card-G2-A_2672 (N704.200) K_Personalisierung: Attribute von PuK.CMS_SMC-B.AUT_CVC.E384

Die Attribute von PuK.CMS_SMC-B.AUT_CVC.E384 MÜSSEN bis auf den keyIdentifier, den Domainparameter und die oid mit den Attributen von PuK.CMS_SMC-B.AUT_CVC.E256 identisch sein.

Für die oid MUSS der Wert für authS_gemSpec-COS-G2_ecc-with-sha384 (´2B2403050302' = {1.3.36.3.5.3.2}) eingetragen werden.

Für den Domainparameter gilt: Domainparameter = brainpoolP384r1.⌫

PuK.CMS_SMC-B.AUT_CVC.E384 muss genau dann in der Karte vorhanden sein, wenn ein CMS mit asymmetrischer Authentisierung mit elliptischen Kurven und der Schlüssel-

länge 384 bit verwendet wird. PuK.CMS_SMC-B.AUT_CVC.E384 ist ein globaler Schlüssel mit einem einheitlichen Key Identifier und einem CMS-spezifischen Schlüsselwert, der zudem vom Ausgabejahr der SMC abhängen kann. Das zugehörige CMS ist wahrscheinlich daran gebunden, jede einzelne Karte zu identifizieren, um den passenden Schlüssel zu verwenden. Der Key Identifier kommt als Schlüsselreferenz im Authentisierungsverfahren zwischen SMC-B und CMS zum Einsatz, während die CHAT in Zugriffsregeln verwendet wird.

4.3.32 MF / SK.CMS.AES128 (optional)

SK.CMS.AES128 (optional) ist der geheime Schlüssel für die Durchführung des SMC-B/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel. Die nachfolgende Tabelle Tab_SMC-B_ObjSys_033 zeigt die Eigenschaften des Schlüssels.

⌧ **Card-G2-A_2194 (N704.300) K_Personalisierung: Attribute von MF / SK.CMS.AES128**

SK.CMS.AES128 MUSS die in Tab_SMC-B_ObjSys_033 dargestellten Werte besitzen.

Tabelle 33: Tab_SMC-B_ObjSys_033 Attribute von MF / SK.CMS.AES128

Attribute	Wert	Bemerkung
Objekttyp	AES Authentisierungsobjekt	
keyIdentifier	´14´ = 20	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTUAL AUTHENTICATE	PWD(PIN.SMC) OR AUT(‘D27600004000’ || ‘xx’) OR AUT(‘yy.....yy’)	siehe Hinweis 73:
TERMINATE	AUT_CMS	siehe Hinweis 74:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	

andere	NEVER	

⌫

Hinweis 72: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE; TERMINATE

Hinweis 73: Authentisierung mit PIN.SMC oder Rollenauthentisierung mit einem HBA oder SMC mit zugehörigem persönlichen Profil 'xx', z.B. Profil 2 (Generation 1) oder einem Hex-Wert 'yy.....yy', der der Flagliste eines entsprechenden HBA oder einer entsprechenden SMC entspricht (Generation 2, siehe [gemSpec_COS])..

Hinweis 74: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.3.33 MF / SK.CMS.AES256 (optional)

SK.CMS.AES256 (optional) ist der geheime Schlüssel für die Durchführung des SMC-B / CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.

⌦ **Card-G2-A_2195 (N704.400) K_Personalisierung: Attribute von MF / SK.CMS.AES256**

SK.CMS.AES256 MUSS die in Tab_SMC-B_ObjSys_034 dargestellten Werte besitzen.

Tabelle 34: Tab_SMC-B_ObjSys_034 Attribute von MF / SK.CMS.AES256

Attribute	**Wert**	**Bemerkung**
Objekttyp	AES Authentisierungsobjekt	
keyIdentifier	´18´ = 24	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTUAL AUTHENTICATE	PWD(PIN.SMC) OR AUT('D27600004000' || 'xx') OR AUT('yy.....yy')	siehe Hinweis 76:
TERMINATE	AUT_CMS	siehe Hinweis 77:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 75: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE; TERMINATE

Hinweis 76: Authentisierung mit PIN.SMC oder Rollenauthentisierung mit einem HBA oder SMC mit zugehörigem persönlichen Profil 'xx', z.B. Profil 2 (Generation 1) oder einem Hex-Wert 'yy.....yy', der der Flagliste eines entsprechenden HBA oder einer entsprechenden SMC entspricht (Generation 2, siehe [gemSpec_COS]).

Hinweis 77: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.4 Die Sicherheitsmodul-Anwendung DF.SMA

4.4.1 Dateistruktur und Dateiinhalt

Die folgende Abbildung zeigt die Dateistruktur von DF.SMA für die SMC-B.

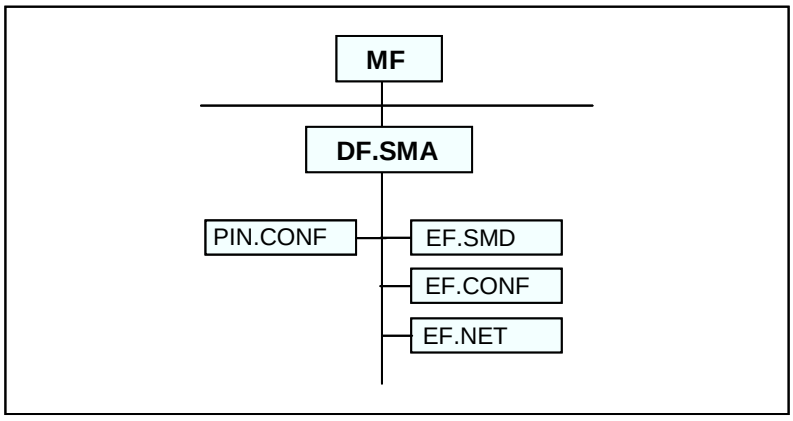

Abbildung 2: (Abb_SMC-B_ObjSys_002) Prinzipielle Struktur der Sicherheitsmodul-Anwendung der SMC-B

4.4.2 MF / DF.SMA (Security Module Application)

DF.SMA ist ein „Application Directory“ gemäß [gemSpec_COS#8.3.1.1], d.h. ist mittels Anwendungskennung selektierbar.

⌦ **Card-G2-A_2197 (N706.000) K_Personalisierung: Attribute von MF / DF.SMA**

DF.SMA MUSS die in Tab_SMC-B_ObjSys_035 dargestellten Werte besitzen.

Tabelle 35: Tab_SMC-B_ObjSys_035 Attribute von MF / DF.SMA

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	'D27600014607'	
fileIdentifier	–	Siehe Hinweis 79:
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
LOAD APPLICATION	AUT_CMS	siehe Hinweis 80:
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

⌫

Hinweis 78: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: LOAD APPLICATION, SELECT

Hinweis 79: Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS# 8.1.1]

Hinweis 80: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7.

4.4.2.1 MF / DF.SMA / EF.SMD

Die transparente Datei EF.SMD ist für die Speicherung von SMC-B-bezogenen Daten vorgesehen, z.B. von speziellen Konfigurationsdaten. Die Datei kann immer gelesen werden, aber eine Aktualisierung ist nur nach erfolgreicher Authentisierung zwischen der SMC-B und einem entsprechenden HBA oder SMC-B möglich. Die folgende Tabelle Tab_SMC-B_ObjSys_036 zeigt die Attribute und Zugriffsbedingungen der Datei EF.SMD. Alternativ zur Authentisierung mit einem HBA oder einer SMC-B kann für den aktu-alisierenden oder löschenden Zugriff die Authentisierung mit der PIN.SMC genutzt werden.

⌦ **Card-G2-A_2198 (N706.100) K_Personalisierung: Attribute von MF / DF.SMA / EF.SMD**

EF.SMD MUSS die in Tab_SMC-B_ObjSys_036 dargestellten Werte besitzen.

Tabelle 36: Tab_SMC-B_ObjSys_036 Attribute von MF / DF.SMA / EF.SMD

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	‘D0 01’	
shortFileIdentifier	‘01’ = 1	
numberOfOctet	´0400´ Oktett = 1024 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
Body		wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.SMC) OR AUT(‘D27600004000’ || ‘xx’) OR AUT(‘yy.....yy’)	Siehe Hinweis 82:
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 81: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 82: Authentisierung mit PIN.SMC oder Rollenauthentisierung mit einem HBA oder SMC mit zugehörigem persönlichen Profil ’xx’, z.B. Profil 2 (Generation 1) oder einem Hex-Wert ‘yy.....yy’, der der Flagliste eines entsprechenden HBA oder einer entsprechenden SMC entspricht (Generation 2, siehe [gemSpec_COS]).

4.4.2.2 MF / DF.SMA / EF.CONF

Die transparente Datei EF.CONF speichert Konfigurationsdaten für die Konnektorwartung. Dies kann beispielsweise beim Austausch des Konnektors genutzt werden, um Pairing-Informationen zu sichern und an den neuen Konnektor zu übertragen. Lesen, Aktualisieren und Löschen der Daten sind nur nach erfolgreicher Präsentation der PIN.CONF zugelassen.

⌦ **Card-G2-A_2199 (N706.200) K_Personalisierung: Attribute von MF / DF.SMA / EF.CONF**

EF.CONF MUSS die in Tab_SMC-B_ObjSys_037 dargestellten Werte besitzen.

Tabelle 37: Tab_SMC-B_ObjSys_037 Attribute von MF / DF.SMA / EF.CONF

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	‘D0 02’	
shortFileIdentifier	‘02’ = 2	
numberOfOctet	´2000´ Oktett = 8192 Oktett	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body		wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ERASE / READ / WRITE / UPDATE BINARY	PWD(PIN.CONF)	Authentisierung mit PIN.CONF, siehe Tab_SMC-B_ObjSys_039
SELECT	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 83: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

4.4.2.3 MF / DF.SMA / EF.NET

Die transparente Datei EF.NET kann Netzwerkkonfigurationsdaten speichern, z.B.

- DNS-Namen oder IP-Adressen in Verbindung mit Portnummer und Protokolltyp (TCP oder UDP) der Access Gateways,
- VPN IP-Version (IPv4 oder IPv6)
- DNS-Name des Aktualisierungsservers.

Die Daten sind organisationsspezifisch. Das Lesen der Daten ist immer möglich. Aktualisieren und Löschen ist nur nach erfolgreicher Präsentation der PIN.SMC zugelassen.

Card-G2-A_2200 (N706.300) K_Personalisierung: Attribute von MF / DF.SMA / EF.NET

EF.NET MUSS die in Tab_SMC-B_ObjSys_038 dargestellten Werte besitzen.

Tabelle 38: Tab_SMC-B_ObjSys_038 Attribute von MF / DF.SMA / EF.NET

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	‘D003’	
shortFileIdentifier	‘03’ = 3	
numberOfOctet	´0800´ Oktett = 2048 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body		wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ERASE / WRITE / UPDATE BINARY	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
READ BINARY	ALWAYS	
SELECT	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 84: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

4.4.2.4 MF / DF.SMA / PIN.CONF

PIN.CONF ist eine lokale PIN für den schreibenden und löschenden Zugriff auf Daten in EF.CONF. Die PIN besteht aus 6 bis 8 Ziffern und ist änderbar. Der Wiederholungszähler muss den Anfangswert 3 besitzen.

Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Nutzungszähler wird bei jeder Nutzung heruntergezählt, unabhängig davon, ob der eingegebene Rücksetzcode richtig oder falsch ist. Die Eingabe des korrekten Wertes setzt den Wiederholungszähler von PIN.CONF auf den Anfangswert zurück. Der Sicherheitsstatus der PIN.CONF kann unbegrenzt verwendet werden, d.h. der Default-Wert von SSEC beträgt unendlich.

⌦ **Card-G2-A_2201 (N706.400) K_Personalisierung: Attribute von MF / DF.SMA / PIN.CONF**

PIN.CONF MUSS die in Tab_SMC-B_ObjSys_039 dargestellten Werte besitzen.

Tabelle 39: Tab_SMC-B_ObjSys_039 Attribute von MF / DF.SMA / PIN.CONF

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword, Leer–PIN, Transport–PIN}	
flagEnabled	True	
startSsec	unendlich	

PUK	…	wird personalisiert
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=1	ALWAYS	siehe Hinweis 86:
	herstellerspezifisch	siehe Hinweis 86:
CHANGE RD, P1=0	ALWAYS	siehe Hinweis 87:
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	ALWAYS	
VERIFY	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 85: 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 86: Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN

Hinweis 87: Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN

⌦ **Card-G2-A_2202 (N706.500) K_Personalisierung: Länge der PUK für PIN.Conf**

Bei der Personalisierung MUSS eine PUK mit acht Ziffern gewählt werden.⌫

Als PIN-Transportschutz muss ein Verfahren aus Kapitel 8.2.5 von [gemSpec_COS] verendet werden. Es wird empfohlen, ein Leer-PIN-Verfahren zu nutzen, bei dem der Benutzer nur die neue PIN eingeben muss. Zum Setzen der regulären PIN wird das Kommando CHANGE REFERENCE DATA verwendet.

4.5 Die ESIGN-Anwendung DF.ESIGN

4.5.1 Dateistruktur und Dateiinhalt

Die allgemeine ESIGN-Anwendung ist in [EN14890-1]dargestellt und wird in der SMC-B für folgende Funktionen genutzt:

- die Berechnung einer Organisationssignatur (die Signatur ist an die entsprechende Institution im Gesundheitswesen gebunden, nicht an eine einzelne Person, siehe Abbildung 3.
- die Client/Server-Authentisierung z.B. zur Verbindung der Institution im Gesundheitswesen oder eines Teils dieser Institution mit dem VPN des Gesundheitswesens und
- die Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels zur vertraulichen Weitergabe von Dokumenten, welche an die entsprechende Institution im Gesundheitswesen und nicht an eine einzelne Person adressiert sind.

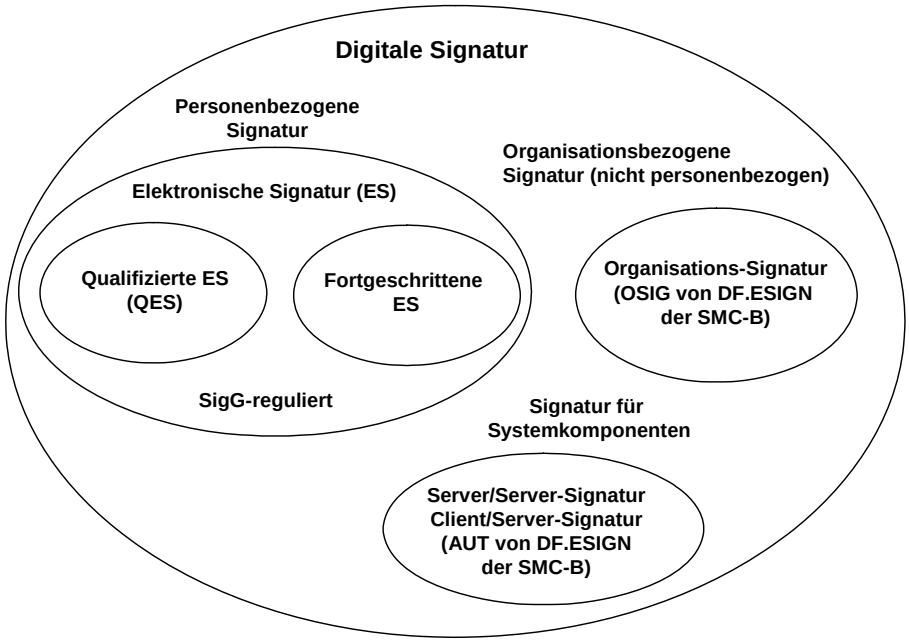

Abbildung 3: (Abb_SMC-B_ObjSys_003) Arten der digitalen Signatur

Abbildung 4 zeigt die prinzipielle Dateistruktur der ESIGN-Anwendung gemäß EN14890.

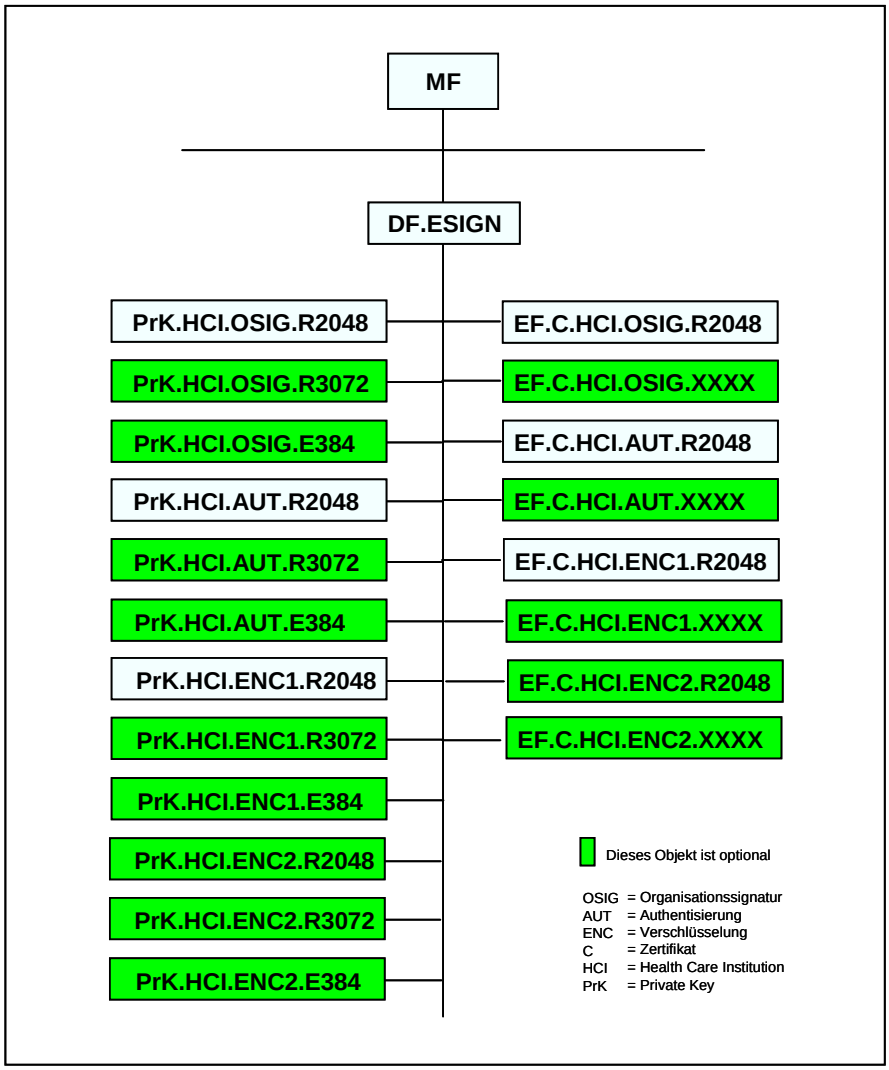

Abbildung 4: (Abb_SMC-B_ObjSys_004) Allgemeine Struktur von MF / DF.ESIGN

4.5.2 MF / DF.ESIGN

⌧ Card-G2-A_2203 (N707.000) K_Personalisierung: Attribute von MF / DF.ESIGN

DF.ESIGN MUSS die in Tab_SMC-B_ObjSys_040 dargestellten Werte besitzen.

Tabelle 40: Tab_SMC-B_ObjSys_040 Attribute von MF / DF.ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	'A000000167 455349474E'	siehe Hinweis 89:
fileIdentifier	–	siehe Hinweis 90:

lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
LOAD APPLICATION	AUT_CMS	siehe Hinweis 92:
SELECT	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 88: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis 89: Der Wert des Attributes applicationIdentifier ist in [EN14890-1]festgelegt.

Hinweis 90: Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls [‘1000’, ‘FEFF’]; siehe [gemSpec_COS#8.1.1]

Hinweis 91: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 4.5 nicht berücksichtigt zu werden.

Hinweis 92: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.1 MF / DF.ESIGN / EF.C.HCI.OSIG.R2048

EF.C.HCI.OSIG.R2048 enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.HCI.OSIG.R2048 zu PrK.HCI.OSIG.R2048 (siehe Kapitel 4.5.2.8).

⌦ **Card-G2-A_2204 (N707.100) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048**

EF.C.HCI.OSIG.R2048 MUSS die in Tab_SMC-B_ObjSys_041 dargestellten Werte besitzen.

Tabelle 41: Tab_SMC-B_ObjSys_041 Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C0 00´	
shortFileIdentifier	´10´= 16	

numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 94:
READ BINARY	ALWAYS	
ERASE / WRITE / UPDATE BINARY	AUT_CMS	siehe Hinweis 94:
SELECT	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 93: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 94: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.2 MF / DF.ESIGN / EF.C.HCI.OSIG.XXXX (optional)

Die Datei EF.C.HCI.OSIG.XXXX wird erst bei der Aktivierung des jeweiligen Verfahrens (RSA3072 oder ELC384) mit dem Kommando LOAD APPLICATION von der dazu berechtigten Instanz angelegt. Die zu den jeweiligen Verfahren gehörenden privaten Schlüsselobjekte sind in den Kapiteln 4.5.2.10 und 4.5.2.11 zu finden.

⌦ **Card-G2-A_2205 (N707.200) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.XXXX**

Die Attribute von EF.C.HCI.OSIG.XXXX MÜSSEN mit Ausnahme von FID und SFID identisch mit den Attributen von EF.C.HCI.OSIG.R2048 sein. ⌫

⌦ **Card-G2-A_2206 (N707.250) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HCI.OSIG.XXXX**

Folgende Werte MÜSSEN für FID und SFID für EF.C.HCI.OSIG.XXXX verwendet werden:

- FID: ’C0 11´
- SFID: ’11´= 17⌫

4.5.2.3 MF / DF.ESIGN / EF.C.HCI.AUT.R2048

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.HCI.AUT.R2048 zu PrK.HCI.AUT.R2048 (siehe Kapitel 4.5.2.12).

⌦ **Card-G2-A_2207 (N707.300) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048**

EF.C.HCI.AUT.R2048 MUSS die in Tab_SMC-B_ObjSys_042 dargestellten Werte besitzen.

Tabelle 42: Tab_SMC-B_ObjSys_042 Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	´C5 00´	
shortFileIdentifier	´01´= 1	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS	siehe Hinweis 96:
READ BINARY	ALWAYS	
ERASE / WRITE / UPDATE BINARY	AUT_CMS	siehe Hinweis 96:
SELECT	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 95: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: CTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 96: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.4 MF / DF.ESIGN / EF.C.HCI.AUT.XXXX (optional)

Die Datei EF.C.HCI.AUT.XXXX wird erst bei der Aktivierung des jeweiligen Verfahrens (RSA3072 oder ELC384) mit dem Kommando LOAD APPLICATION von der dazu berechtigten Instanz angelegt. Die zu den jeweiligen Verfahren gehörenden privaten Schlüsselobjekte sind in den Kapiteln 4.5.2.13 und 4.5.2.14 zu finden.

⌦ **Card-G2-A_2208 (N707.400) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.XXXX**

Die Attribute von EF.C.HCI.AUT.XXXX MÜSSEN mit Ausnahme von FID und SFID identisch mit den Attributen von EF.C.HCI.AUT.R2048 sein.⌫

⌦ **Card-G2-A_2209 (N707.450) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HCI.AUT.XXXXX**

Folgende Werte MÜSSEN für FID und SFID für EF.C.HCI.AUT.XXXX verwendet werden:

- FID: ’C5 06´
- SFID: ’06´= 6 ⌫

4.5.2.5 MF / DF.ESIGN / EF.C.HCI.ENC1.R2048

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.HCI.ENC1.R2048. Das zugehörende private Schlüsselobjekt PrK.HCI.ENC1.R2048 ist in Kapitel 4.5.2.15 definiert.

⌦ **Card-G2-A_2210 (N707.500) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.ENC1.R2048**

EF.C.HCI.ENC1.R2048 MUSS die in Tab_SMC-B_ObjSys_043 dargestellten Werte besitzen.

Tabelle 43: Tab_SMC-B_ObjSys_043 Attribute von MF / DF.ESIGN / EF.C.HCI.ENC1.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C2 00´	

shortFileIdentifier	´02´= 2	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	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 97: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: CTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY:

4.5.2.6 MF / DF.ESIGN / EF.C.HCI.ENC2.R2048 (optional)

EF.C.HCI.ENC2.R2048 ist dafür vorgesehen, nach dem Ablauf des Zertifikats EF.C.HCI.ENC1.R2048 und des dazugehörenden Schlüssels PrK.HCI.ENC1.R2048 ein Zertifikat für die RSA-2048-Kryptographie aufzunehmen. Sie wird von der dazu berechtigten Instanz mit dem Kommando LOAD APPLICATION angelegt. Das zugehörende private Schlüsselobjekt ist in Kapitel 4.5.2.16 definiert.

⌦ **Card-G2-A_2211 (N707.600) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.ENC2.R2048**

Die Attribute von EF.C.HCI.ENC2.R2048 MÜSSEN mit Ausnahme von FID und SFID mit folgender Ergänzung (sowohl für kontaktbehaftet als auch für kontaktlos) identisch zu denen von EF.C.HCI.ENC1.R2048 sein.

UPDATE BINARY	AUT_CMS	Hinweis 98:

⌫

Hinweis 98: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7

⌦ **Card-G2-A_2212 (N707.650) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HCI.ENC2.R2048**

Folgende Werte MÜSSEN für FID und SFID für EF.C.HCI.ENC2.R2048 verwendet werden:

FID: ’C2 03´

SFID: ’03´= 3⌫

4.5.2.7 MF / DF.ESIGN / EF.C.HCI.ENC1.XXXX (optional)

Die Datei EF.C.HCI.ENC1.XXXX wird erst bei der Aktivierung des jeweiligen Verfahrens (RSA3072 oder ELC384) mit dem Kommando LOAD APPLICATION von der dazu berechtigten Instanz angelegt. Die zu den jeweiligen Verfahren gehörenden privaten Schlüsselobjekte sind in den Kapiteln 4.5.2.17 und 4.5.2.19 zu finden.

⌦ **Card-G2-A_2213 (N707.700) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.ENC1.XXXX**

Die Attribute von EF.C.HCI.ENC1.XXXX MÜSSEN mit Ausnahme von FID und SFID mit folgender Ergänzung (sowohl für kontaktbehaftet als auch für kontaktlos) identisch zu denen von EF.C.HCI.ENC1.R2048 sein.

UPDATE BINARY	AUT_CMS	siehe Hinweis 99:

⌫

Hinweis 99: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7

⌦ **Card-G2-A_2214 (N707.750) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HCI.ENC1.XXXX**

Folgende Werte MÜSSEN für FID und SFID für EF.C.HCI.ENC1.XXXX verwendet werden:

FID: ’C2 08´

SFID: ’08´= 8⌫

4.5.2.8 MF / DF.ESIGN / EF.C.HCI.ENC2.XXXX (optional)

Die Datei EF.C.HCI.ENC2.XXXX ist dafür vorgesehen, nach dem Ablauf des Zertifikats EF.C.HCI.ENC1.XXXX und des dazugehörenden Schlüssels (PrK.HCI.ENC1.R3072 bzw. PrK.HCI.ENC1.E384) ein Zertifikat zur Nutzung aufzunehmen, das für die Kryptographie mit dem Verfahren verwendet wird, das als Nachfolger der RSA-2048-Kryptographie ausgewählt wird. Sie wird nach der Aktivierung des jeweiligen Verfahrens (RSA3072 oder ELC384) mit dem Kommando LOAD APPLICATION von der dazu berechtigten Instanz angelegt. Die zu den jeweiligen Verfahren gehörenden privaten Schlüsselobjekte sind in den Kapiteln 4.5.2.18 und 4.5.2.20 definiert.

Card-G2-A_2215 (N707.800) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HCI.ENC2.XXXX

Die Attribute von EF.C.HCI.ENC2.XXXX MÜSSEN mit Ausnahme von FID und SFID mit folgender Ergänzung (sowohl für kontaktbehaftet als auch für kontaktlos) identisch zu denen von EF.C.HCI.ENC1.R2048 sein.

UPDATE BINARY	AUT_CMS	Hinweis 100:

Hinweis 100: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7

Card-G2-A_2216 (N707.850) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HCI.ENC2.XXXX

Folgende Werte MÜSSEN für FID und SFID für EF.C.HCI.ENC2.XXXX verwendet werden:

FID: ’C2 0B´

SFID: ’0B´= 11

4.5.2.9 MF / DF.ESIGN / PrK.HCI.OSIG.R2048

PrK.HCI.OSIG.R2048 ist der private Schlüssel zur Berechnung einer Organisationssignatur. Der zugehörige öffentliche Schlüssel PuK.HCI.OSIG.R2048 ist in C.HCI.OSIG.R2048 (siehe Kapitel 4.5.2.1) enthalten.

Card-G2-A_2217 (N707.900) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048

PrK.HCI.OSIG.R2048 MUSS die in Tab_SMC-B_ObjSys_044 dargestellten Werte besitzen.

Tabelle 44: Tab_SMC-B_ObjSys_044 Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´04´ = 4	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {signPSS, sign9796_2_DS2}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
COMPUTE DIGITAL SIGNATURE	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-

		Ebene definiert
GENERATE ASYM	AUT_CMS	siehe Hinweis 102:
TERMINATE	AUT_CMS	siehe Hinweis 102:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 101: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 102: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.10 MF / DF.ESIGN / PrK.HCI.OSIG.R3072 (optional)

PrK.HCI.OSIG.R3072 ist der private Schlüssel zur Berechnung einer Organisationssignatur. Der zugehörige öffentliche Schlüssel PuK.HCI.OSIG.R3072 ist in C.HCI.OSIG.R3072 (siehe Kapitel 4.5.2.2) enthalten.

⌦ **Card-G2-A_2218 (N708.000) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R3072**

PrK.HCI.OSIG.R3072 MUSS die in Tab_SMC-B_ObjSys_045 dargestellten Werte besitzen.

Tabelle 45: Tab_SMC-B_ObjSys_045 Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´13´ = 19	
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {signPSS, sign9796_2_DS2}	
lifeCycleStatus	„Operational state (activated)"	

Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
COMPUTE DIGITAL SIGNATURE	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
GENERATE ASYM	AUT_CMS	siehe Hinweis 104:
TERMINATE	AUT_CMS	siehe Hinweis 104:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 103: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 104: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.11 MF / DF.ESIGN / PrK.HCI.OSIG.E384 (optional)

PrK.HCI.OSIG.E384 ist der private Schlüssel zur Berechnung einer Organisationssignatur. Der zugehörige öffentliche Schlüssel PuK.HCI.OSIG.E384 ist in C.HCI.OSIG.E384 (siehe Kapitel 4.5.2.2) enthalten.

⌦ **Card-G2-A_2219 (N708.100) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E384**

PrK.HCI.OSIG.E384 MUSS die in Tab_SMC-B_ObjSys_046 dargestellten Werte besitzen.

Tabelle 46: Tab_SMC-B_ObjSys_046 Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´0A´ = 10	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert

algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { elcSharedSecretCalculation }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
COMPUTE DIGITAL SIGNATURE	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
GENERATE ASYM	AUT_CMS	siehe Hinweis 106:
TERMINATE	AUT_CMS	siehe Hinweis 106:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 105: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 106: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.12 MF / DF.ESIGN / PrK.HCI.AUT.R2048

PrK.HCI.AUT.R2048 ist der private Schlüssel für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HCI.AUT.R2048 ist in C.HCI.AUT.R2048 (siehe Kapitel 4.5.2.3) enthalten.

⌦ **Card-G2-A_2220 (N708.200) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048**

PrK.HCI.AUT.R2048 MUSS die in Tab_SMC-B_ObjSys_047 dargestellten Werte besitzen.

Tabelle 47: Tab_SMC-B_ObjSys_047 Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´02´ = 2	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYM	AUT_CMS	siehe Hinweis 108:
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert
TERMINATE	AUT_CMS	siehe Hinweis 108:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 107: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 108: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.13 MF / DF.ESIGN / PrK.HCI.AUT.R3072 (optional)

PrK.HCI.AUT.R3072 ist der private Schlüssel für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HCI.AUT.R3072 ist in C.HCI.AUT.R3072 (siehe Kapitel 4.5.2.4) enthalten.

⌦ **Card-G2-A_2221 (N708.300) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R3072**

PrK.HCI.AUT.R3072 MUSS die in Tab_SMC-B_ObjSys_048 dargestellten Werte besitzen.

Tabelle 48: Tab_SMC-B_ObjSys_048 Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R3072

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´05´ = 5	
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYM	AUT_CMS	siehe Hinweis 110:
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
TERMINATE	AUT_CMS	siehe Hinweis 110:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 109: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 110: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.14 MF / DF.ESIGN / PrK.HCI.AUT.E384 (optional)

PrK.HCI.AUT.E384 ist der private Schlüssel für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HCI.AUT.E384 ist in C.HCI.AUT.E384 (siehe Kapitel 4.5.2.4) enthalten.

⌦ **Card-G2-A_2222 (N708.400) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E384**

PrK.HCI.AUT.E384 MUSS die in Tab_SMC-B_ObjSys_049 dargestellten Werte besitzen.

Tabelle 49: Tab_SMC-B_ObjSys_049 Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E384

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´08´ = 8	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcClientAuthentication}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYM	AUT_CMS	siehe Hinweis 112:
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
TERMINATE	AUT_CMS	siehe Hinweis 112:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

*Hinweis 111: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE*

ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, TERMINATE

Hinweis 112: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7:

4.5.2.15 MF / DF.ESIGN / PrK.HCI.ENC1.R2048

PrK.HCI.ENC1.R2048 ist der private Schlüssel für den PKI-Dienst zur Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC1.R2048 ist in C.HCI.ENC1.R2048 (siehe Kapitel 4.5.2.5) enthalten.

⌦ **Card-G2-A_2223 (N708.500) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.ENC1.R2048**

PrK.HCI.ENC1.R2048 MUSS die in Tab_SMC-B_ObjSys_050 dargestellten Werte besitzen.

Tabelle 50: Tab_SMC-B_ObjSys_050 Attribute von MF / DF.ESIGN / PrK.HCI.ENC1.R2048

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´03´ = 3	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
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**
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

*Hinweis 113: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER*

4.5.2.16 MF / DF.ESIGN / PrK.HCI.ENC2.R2048 (optional)

PrK.HCI.ENC2.R2048 ist der private Schlüssel zur Nutzung nach dem Ablauf des Zertifikats EF.C.HCI.ENC1.R2048 und des dazugehörenden Schlüssels PrK.HCI.ENC1.R2048 für die Kryptographie mit RSA für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Die Schlüsselgenerierung wird von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC2.R2048 ist in C.HCI.ENC2.R2048 (siehe Kapitel 4.5.2.6) enthalten.

⌦ **Card-G2-A_2224 (N708.600) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.ENC2.R2048**

PrK.HCI.ENC2.R2048 MUSS die in Tab_SMC-B_ObjSys_051 dargestellten Werte besitzen.

Tabelle 51: Tab_SMC-B_ObjSys_051 Attribute von MF / DF.ESIGN / PrK.HCI.ENC2.R2048

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´0B´ = 11	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
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	AUT_CMS	siehe Hinweis 115:
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 114: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

Hinweis 115: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7: Es muss organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HCI.ENC2.R2048 genutzt werden kann.

4.5.2.17 MF / DF.ESIGN / PrK.HCI.ENC1.R3072 (optional)

PrK.HCI.ENC1.R3072 ist der private Schlüssel für den PKI-Dienst zur Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels. Die Schlüsselgenerierung wird bei der Nutzung des Verfahrens RSA3072 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC1.R3072 ist in C.HCI.ENC1.R3072 (siehe Kapitel 4.5.2.7) enthalten.

⌦ **Card-G2-A_2225 (N708.700) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.ENC1.R3072**

PrK.HCI.ENC1.R3072 MUSS die in Tab_SMC-B_ObjSys_052 dargestellten Werte besitzen.

Tabelle 52: Tab_SMC-B_ObjSys_052 Attribute von MF / DF.ESIGN / PrK.HCI.ENC1.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´0E´ = 14	
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
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	AUT_CMS	siehe Hinweis 117:
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		

Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 116: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

Hinweis 117: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7: Es muss organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HCI.ENC1.R3072 genutzt werden kann.

4.5.2.18 MF / DF.ESIGN / PrK.HCI.ENC2.R3072 (optional)

PrK.HCI.ENC2.R3072 ist der private Schlüssel für die Kryptographie mit RSA für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Die Schlüsselgenerierung wird bei der Nutzung des Verfahrens RSA3072 nach dem Ablauf von Zertifikat EF.C.HP.ENC1.R3072 und dem dazugehörenden Schlüssel PrK.HCI.ENC1.R3072 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC2.RE384 ist in C.HCI.ENC2.E384 (siehe Kapitel 4.5.2.8) enthalten.

⌦ **Card-G2-A_2226 (N708.800) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.ENC2.R3072**

PrK.HCI.ENC2.R3072 MUSS die in Tab_SMC-B_ObjSys_053 dargestellten Werte besitzen.

Tabelle 53: Tab_SMC-B_ObjSys_053 Attribute von MF / DF.ESIGN / PrK.HCI.ENC2.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´0C´ = 12	
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
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	AUT_CMS	siehe Hinweis 119:
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 118: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

Hinweis 119: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7: Es muss organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HCI.ENC2.R3072 genutzt werden kann.

4.5.2.19 MF / DF.ESIGN / PrK.HCI.ENC1.E384 (optional)

PrK.HCI.ENC1.E384 ist der private Schlüssel für den PKI-Dienst zur Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels. Die Schlüsselgenerierung wird bei der Aktivierung des Verfahrens ELC384 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC1.E384 ist in C.HCI.ENC1.E384 (siehe Kapitel 4.5.2.7) enthalten.

⌦ **Card-G2-A_2227 (N708.900) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.ENC1.E384**

PrK.HCI.ENC1.E384 MUSS die in Tab_SMC-B_ObjSys_054 dargestellten Werte besitzen.

Tabelle 54: Tab_SMC-B_ObjSys_054 Attribute von MF / DF.ESIGN / PrK.HCI.ENC1.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Entschlüsselungsobjekt	
keyIdentifier	´09´ = 9	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcSharedSecretCalculation}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

GENERATE ASYM	AUT_CMS	siehe Hinweis 121:
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 120: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

Hinweis 121: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7: Es muss organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HCI.ENC1.E384 genutzt werden kann.

4.5.2.20 MF / DF.ESIGN / PrK.HCI.ENC2.E384 (optional)

PrK.HCI.ENC2.E384 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Die Schlüsselgenerierung wird bei der Aktivierung des Verfahrens ELC384 nach dem Ablauf des Zertifikats EF.C.HCI.ENC1.E384 und des dazugehörenden Schlüssels PrK.HCI.ENC1.E384 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC2.E384 ist in C.HCI.ENC2.E384 (siehe Kapitel 4.5.2.8) enthalten.

⌦ **Card-G2-A_2228 (N709.000) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HCI.ENC2.E384**

PrK.HCI.ENC2.E384 MUSS die in Tab_SMC-B_ObjSys_055 dargestellten Werte besitzen.

Tabelle 55: Tab_SMC-B_ObjSys_055 Attribute von MF / DF.ESIGN / PrK.HCI.ENC2.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Entschlüsselungsobjekt	
keyIdentifier	´0D´ = 13	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcSharedSecretCalculation}	

lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYM	AUT_CMS	siehe Hinweis 123:
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 122: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

Hinweis 123: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.7: Es muss organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HCI.ENC2.E384 genutzt werden kann.

4.6 Die Kartenterminalanwendung DF.KT

⌦ **Card-G2-A_2229 (N710.000) K_Personalisierung: DF.KT in der SMC-B**

Die Kartenterminalanwendung DF.KT MUSS zu der in [gemSpec_gSMC-KT_ObjSys] spezifizierten Kartenterminalanwendung DF.KT identisch sein. ⌫

4.7 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der SMC-B

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) oder das Anlegen von neuen EFs in DF.SMA oder das Nachladen von Zertifikaten oder das Generieren und Sperren von Schlüsseln nach der Ausgabe der SMC-B von einem Card Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CMS optional. Die Inhalte des Kapitels 14.2.5 in [gemSpec_COS] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe der SMC-B durchgeführt werden müssen.

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AID	Application Identifier (Anwendungskennung)
APDU	Application Protocol Data Unit [ISO7816-3]
ASN.1	Abstract Syntax Notation One
ATR	Answer-to-Reset
AUT	Authentisierung
AUTD	CV-basierte Geräteauthentisierung
AUTR	CV-basierte Rollenauthentisierung
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
C	Zertifikat
C2C	Card to Card
CA	Certification Authority (Zertifizierungsdiensteanbieter)
CMS	Card Application Management System
CAR	Certification Authority Reference
CC	Cryptographic Checksum (kryptographische Prüfsumme)
CER	Canonical Encoding Rules
CH	Cardholder (Karteninhaber)
CHAT	Certificate Holder Autorisation Template Liste von Rechten, die ein Zertifikatsinhaber besitzt
COS	Card Operating System (Chipkartenbetriebssystem)
CPI	Certificate Profile Identifier
CRL	Certificate Revocation List (Zertifikatssperrliste)
CV	Card Verifiable
CVC	Card Verifiable Certificate
D,DIR	Directory
DER	Distinguished Encoding Rules
DES	Daten Encryption Standard
DF	Dedicated File

DO	Datenobjekt
DS	Digital Signature
DSI	Digital Signature Input
DTBS	Data to be signed
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
eGK	elektronische Gesundheitskarte
ENC	Encryption
FCI	File Control Information
FCP	File Control Parameter
FI	Clock rate conversion factor
FID	File Identifier
GDO	Global Data Object
GKV	Gesetzliche Krankenversicherung
GP	Global Platform
HB	Historical Bytes
HBA	Heilberufsausweis (Health Professional Card)
HCI	Health Care Institution (Institution des Gesundheitswesens)
HP	Health Professional (Heilberufler)
HPC	Health Professional Card (Heilberufsausweis)
ICC	Integrated Circuit Card (Chipkarte)
ICCSN	ICC Serial Number (Chipkarten-Seriennummer)
ICM	IC Manufacturer (Kartenhersteller)
ID	Identifier
IIN	Issuer Identification Number
KeyRef	Key Reference
KM	Komfortmerkmal
KT	Karten-Terminal
LCS	Life Cycle Status
LSB	Least Significant Byte(s)
MAC	Message Authentication Code
MF	Master File
MII	Major Industry Identifier
MSE	Manage Security Environment

OCSP	Online Certificate Status Protocol
OD	Object Directory
OID	Object Identifier
OSIG	Organisationssignatur
PIN	Personal Identification Number
PIX	Proprietary Application Provider Extension
PK, PuK	Public Key
PKCS	Public Key Cryptography Standard (hier[PKCS#1])
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates (IETF)
PP	Protection Profile (Schutzprofil)
PrK	Private Key
PSO	Perform Security Operation
PUK	Personal Unblocking Key (Resetting Code)
PV	Plain Value
P1	Parameter P1 einer Kommando-APDU
P2	Parameter P2 einer Kommando-APDU
RA	Registration Authority (Registrierungsinstanz)
RAM	Random Access Memory
RC	Retry Counter (Fehlbedienungszähler)
RCA	Root CA
RFC	Request für Comment
RFID	Radio Frequency Identification
RFU	Reserved for future use
RND	Random Number (Zufallszahl)
ROM	Read Only Memory
RPE	Remote PIN-Empfänger
RPS	Remote PIN-Sender
RSA	Algorithmus von Rivest, Shamir, Adleman [RSA]
SE	Security Environment (Sicherheitsumgebung)
SFID	Short EF Identifier
SIG	Signatur
SK	Secret Key

SM	Secure Messaging
SMC	Security Module Card
SMD	Security Module Data
SSEE	Sichere Signaturerstellungseinheit
SSL	Security Sockets Layer
TLV	Tag Length Value
TC	Trusted Channel
TLS	Transport Layer Security
ZDA	Zertifizierungsdiensteanbieter
3TDES	3-Key-Triple-DES

A2 - Glossar

Das Glossar der Telematikinfrastruktur wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt..

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 - Referenzierte Dokumente

A5.1 - Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. 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: Einführung der Gesundheitskarte Spezifikation des Card Operating System (COS) (elektrische Schnittstelle)
[gemSpec_gSMC-KT_ObjSys]	gematik: Einführung der Gesundheitskarte Spezifikation der gSMC-KT – Objektsystem
[gemSpec_HBA_ObjSys]	gematik: Einführung der Gesundheitskarte Die Spezifikation des elektronischen Heilberufsausweises Objektsystem HBA
[gemSpec_SMC_OPT]	gematik: Einführung der Gesundheitskarte – Gemeinsame optische Merkmale der SMC

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[EN14890-1]	EN 14890-1: 2008 Application Interface for smart cards used as secure signature creation devices, Part 1: Basic services
[EN14890-2]	EN 14890-2: 2008 Application Interface for smart cards used as Secure Signature Creation Devices, Part 2: Additional services
[DIN_EN_1867]	EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers
[ISO3166-1]	ISO/IEC 3166-1: 2006 Codes for the representations of names of countries and their subdivisions – Part 1: Country codes
[ISO7816-3]	ISO/IEC 7816-3: 2006 Identification cards - Integrated circuit cards with contacts - Part 3: Electrical interface and transmission protocols
[ISO7816-4]	ISO/IEC 7816-4: 2005 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ISO8825-1]	ISO/IEC 8825-1: 2002 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
[ISO10646]	ISO/IEC 10646:2003 Information technology -- Universal Multiple-Octet Coded Character Set (UCS)
[PKCS#1]	PKCS #1 RSA Cryptography Standard V2.1: June 14, 2002
[Beschluss190]	Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte
[RFC2119]	Network Working Group, Request for Comments: 2119, S. Bradner Harvard, University, March 1997, Category: Best Current Practice Key words for use in RFCs to Indicate Requirement Levels http://www.apps.ietf.org/rfc/rfc2119.html
[RSA]	R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21 No. 2, 1978
[SD5]	ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19 Register of IC manufacturers http://www.pkicc.de/cms/media/pdfs/IC_manufacturer_ISO_SD5_1962006.pdf
[SigG01]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt Nr. 22, 2001, S.876

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[SigV01]	Verordnung zur elektronischen Signatur – SigV, 2001, Bundesgesetzblatt Nr. 509, 2001, S. 3074