Einführung der Gesundheitskarte

Spezifikation des elektronischen Heilberufsausweises

HBA-Objektsystem

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

Dokumentinformationen

Änderungen zur Vorversion

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

- SRQ 022: Zulässige Algorithmen für die Geräteauthentisierung
- SRQ 027: Konfigurierbare Algorithmen für Introductionkeys in Abhängigkeit vom Security Environment
- SRQ 033: Sichere Zufallsquellen HBA, SMC-A und SMC-B
- SRQ 37: Corrigenda 3
- SRQ 039: Optionalität DF.AUTO

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 2: HPC – 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	13.09.12		Einarbeiten Komemntare	P71
3.0.0	19.09.12		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

DieAFOses Dokument spezifiziert die Objektstruktur des HBA und beschreibt die Kartenschnittstelle zu dem Heilberufsausweis (HBA) für Angehörige approbierter Heilberufe. Die Spezifikation ist so aufgebaut, dass sie an die Anforderungen anderer Heilberufe angepasst werden kann.

Die Spezifikation berücksichtigt:

- das deutsche Signaturgesetz und die zugehörende Signaturverordnung (SigG und SigV)
- 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)

Die Spezifikation behandelt Anwendungen des elektronischen Heilberufsausweises (HBA) 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 eines HBA 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]. Diese Spezifikation ist Grundlage der Entwicklung der Kommandostrukturen und Funktionen für die Chipkartenbetriebssysteme.

Die „Äußere Gestaltung“ des HBA wird vom jeweils für die Ausgabe der HBAs verantwortlichen Sektor in eigener Verantwortung spezifiziert; dies ist nicht Aufgabe der gematik.

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_HPC.AUT_CVC.E256 oder PuK.CMS_HPC.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_0000 <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_HBA_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt

Komponente	Beschreibung
K_Personalisierung	Instanz, welche eine Chipkarte im Rahmen einer Produktion individualisiert
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.

3.1 Attributstabellen

Card-G2-A_2032 (N800.000) K_Personalisierung: Änderung von Zugriffsregeln

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

Card-G2-A_2329 (N800.100) K_Personalisierung: Verhalten der Objekte im SE#1 und im SE#2

Alle in diesem Dokument definierten Objekte MÜSSEN die in diesem Dokument spezifizierten Regeln sowohl für das Security Environment SE#1 als auch für das Security Environment SE#2 einhalten.

3.1.1 Attribute eines Ordners

Card-G2-A_2033 (N800.200) 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_2034 (N800.300) 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_2673 (N800.350) 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_2035 (N800.400) 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_2036 (N800.500) K_Personalisierung: Anzahl logischer Kanäle**

Für die Anzahl logischer Kanäle, die von einem HBA zu unterstützen ist, gilt:

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

Der HBA 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. ⌫

3.4 Kryptobox (optional)

⌦ **Card-G2-A_2865 (N800.550) K_COS: Kryptobox**

Im COS eines HBA KANN die Option_Kryptobox

a) vorhanden sein, oder

b) fehlen.⌫

3.5 Zusätzliche Schnittstellen

3.5.1 Kontaktlose Schnittstelle (optional)

⌦ **Card-G2-A_2866 (N800.600) K_COS: Vorhandensein einer kontaktlosen Schnittstelle**

Im COS einer eGK KANN die Option_kontaklose_Schnittstelle

a) vorhanden sein, oder

b) fehlen⌫

3.5.2 Definition der Card Access Number (CAN) für die Nutzung der kontaktlosen Schnittstelle (optional)

Wird für den HBA die optionale kontaktlose Schnittstelle genutzt, darf die Kommunikation zwischen Karte und Kartenleser erst nach gegenseitiger Authentifizierung und Aufbau eines sicheren Kommunikationskanals erfolgen. Hierfür wird das PACE-Protokoll genutzt. Dieses Protokoll nutzt als Basis für die Authentisierung eine 6-stellige Nummer, die Card Access Number (CAN), die dem Kartenterminal bei der Nutzung bekanntgemacht wird. Dies kann durch Eintippen, Auslesen über einen OCR-Reader oder durch Auslesen eines Barcodes erfolgen. Die Ziffernfolge muss nicht eineindeutig sein, da sie nur im Moment des Auslesens durch einen bestimmten Kartenleser verwendet und nicht gespeichert wird.

⌦ **Card-G2-A_2037 K_Personalisierung: Generierung der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle des HBA**

Für den HBA MUSS die CAN bei der Personalisierung erzeugt oder vom Herausgeber vorgegeben werden. ⌫

⌦ **Card-G2-A_2038 K_Personalisierung: Druck der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle auf den HBA**

Die CAN MUSS an einer für alle HBAs definierten Fläche (Vorschlag: im Feld zwischen Gültigkeitsangabe und Foto) aufgedruckt werden. Eine entsprechende Festlegung für Ort und Art der Bedruckung MUSS in den Spezifikationen der optischen Gestaltung der HBAs der einzelnen Sektoren festgelegt werden.⌫

Die Anbringung der CAN kann z.B. in Form der Ziffernfolge oder auch in Form eines Barcodes, der vom Leser automatisch auslesbar ist, erfolgen.

3.5.3 Verhinderung der Nutzung der kontaktlosen Schnittstelle des HBA bei einem COS, das diese Schnittstelle umsetzt (optional)

⌦ **Card-G2-A_2330 Verhinderung der Nutzung der kontaktlosen Schnittstelle des HBA**

Will der Kartenherausgeber bei einem COS, das die Umsetzung der kontaktlosen Schnittstelle gemäß [gemSpec_COS] implementiert hat, die Nutzung dieser Schnittstelle verhindern, MÜSSEN die Zugriffsregeln für die kontaktlose Schnittstelle gemäß den in Tab_HBA_ObjSys_002 dargestellten Regeln gesetzt werden. Die Zugriffsregeln für den logischen LCS „Operational state (deactivated)" kontaktlos und den logischen LCS „Operational state (terminated)" kontaktlos sind nur betroffen, wenn der jeweilige Zustand im Rahmen der Nutzung des HBA erreicht werden kann. Ansonsten sind die Zugriffsregeln für diese beiden Zustände herstellerspezifisch.

Tabelle 2: Tab_HBA_ObjSys_002 Zugriffsregeln bei Verhinderung der Nutzung der kontaktlosen Schnittstelle des HBA

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Select	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	
SELECT	ALWAYS	
andere	NEVER	

⌫

3.5.4 USB-Schnittstelle (optional)

⌦ **Card-G2-A_2867 (N800.850) K_COS: Vorhandensein einer USB-Schnittstelle**

Im COS einer eGK KANN die Option_USB_Schnittstelle

a) vorhanden sein, oder

b) fehlen.⌫

4 Spezifikation grundlegender Applikationen

Zu den grundlegenden Applikationen des elektronischen Heilberufsausweises (HBA) zählen:

- das Wurzelverzeichnis des HBA, auch root oder Master File (MF) genannt,
- die Gesundheitsanwendung DF.HPA (Health Professional Application),
- die Krypto-Anwendung DF.QES
- die Beschreibung kryptographischer Objekte DF.CIA.QES
- die Krypto-Anwendung DF.ESIGN
- die Beschreibung kryptographischer Objekte DF.CIA.ESIGN
- die organisationsspezifische Anwendung DF.AUTO.

4.1 Attribute des Objektsystems

Das Objektsystem [gemSpec_COS] enthält folgende Attribute:

⌦ **Card-G2-A_2039 (N801.000) K_Personalisierung: Wert des Attributes *root***

Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_HBA_ObjSys_004 sein.⌫

⌦ **Card-G2-A_2040 (N801.100) K_Personalisierung: Wert des Attributes answerToReset**

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

⌦ **Card-G2-A_2041 (N801.200) K_Personalisierung: Wert des Attributes iccsn8**

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

⌦ **Card-G2-A_2042 (N801.300) K_Personalisierung: Inhalt persistentPublicKeyList**

Das Attribut *persistentPublicKeyList* MUSS die Schlüssel PuK.RCA.CS.R2048 und PuK.RCA.CS.E256 (optional PuK.RCA.CS.E384) enthalten.⌫

4.1.1 ATR-Kodierung

⌦ **Card-G2-A_2043 (N801.400) K_Personalisierung: ATR-Kodierung**

Die ATR-Kodierung MUSS die in Tab_HBA_ObjSys_003 dargestellten Werte besitzen.

Tabelle 3: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten)

Parameter	Wert	Bedeutung
TS	‘3B’	Initial Character (direct convention)
T0	'Dx' oder ‘9x’	Format Character (Anzeige von TA1/TD1), 'Dx' bedeutet, dassTC1 vorhanden ist, '9x' bedeutet, dass TC1 nicht vorhanden ist, x = Zahl der Historical Bytes; x = 0 empfohlen, d.h. keine Historical Bytes im ATR, sondern nur in EF.ATR
TA1	‘xx’	Interface Character (FI/DI Wert), 'xx' = '18', '95', '96' oder '97'
TC1	'FF'	Extra Guard Time Integer; zulässige Optionen sind: a) TC1 mit dem 'FF' vorhanden (dringend empfohlen) b) TC1 nicht vorhanden
TD1	‘81’	Interface Character (T=1, Anzeige von TD2)
TD2	‘B1’	Interface Character (T=1, Anzeige von TA3/TB3/TD3)
TA3	‘FE’	Interface Character (IFSC-Kodierung)
TB3	‘45’	Interface Character (BWI/CWI-Kodierung)
TD3	‘1F’	Interface Character (T=15, Anzeige von TA4)
TA4	xx000x11	Interface Character (XI/UI-Kodierung), x = herstellerspezifisch
CI	'00' oder '80'	Category Indicator Byte (erstes Byte von max. 15 Historical Bytes) '00' bedeutet, dass ein Status Indicator in Form der letzten drei Historical Bytes vorhanden ist; '80' bedeutet, dass ein Status Indicator als Datenobjekt vorhanden (ein, zwei oder drei Bytes) ist.
Tag/Length	'6x'	Compact Header des Pre-issuing Datenobjektes (PIDO) mit x = Zahl der nachfolgenden PIDO-Bytes
ICM	'xx'	IC Manufacturer Identifier (Teil des PIDO) Die Kennung wird von ISO an den IC-Hersteller vergeben, see www.sc17.com
ICT	'xx' oder 'xxxx'	IC Type (Teil des PIDO), 1 Byte falls b8 = 0 oder 2 Bytes, falls b8 = 1 im ersten Byte; Kodierung herstellerspezifisch
OSV	'xx'	Operating System Version (Teil der PIDO) Kodierung herstellerspezifisch
DD	'xx...'	Discretionary Data (Teil der PIDO), n Bytes Kodierung herstellerspezifisch
Tag/Length	'73'	Compact Header der Card Capabilities Bytes (CCB) Die Card Capabilities sind auch im EF.ATR vorhanden.
1. CCB	1xx10110 = 'x6'	Card Capabilities Byte der Selektionsmethoden b8 b7 b6 b5 b4 = 1xx10 bezeichnet die DF-Selektion mit vollständigem DF-Namen und mit File Identifier, b3 = 1 bezeichnet die Unterstützung von Short EF Identifier, b2 = 1 bezeichnet die Unterstützung von Record Number, b1 = 0 bezeichnet keine Unterstützung von Record Identifier
2. CCB	00100001 = '21'	Card Capabilities Byte der Daten-Kodierung b8 = 0 bezeichnet keine Unterstützung von EFs mit TLV-Struktur, b7 b6 = 01 bezeichnet das proprietäres Verhalten der Schreibfunktionen, b5 =

Parameter	Wert	Bedeutung
		0 bezeichnet den Wert 'FF' als erstes Byte von TLV-Tagfeldern als unzulässig, b4 b3 b2 b1 = 0001 bezeichnet die Größe der Dateneinheiten in Vierbiteinheiten (Zweierpotenz), d.h. ein Byte
3. CCB	11010yzt = 'Dx'	Card Capabilities Byte von Command Chaining, Längenfeldern und logischen Kanälen b8 = 1 bezeichnet die Unterstützung von Command Chaining, z.B. für LOAD APPLICATION, b7 = 1 bezeichnet die Unterstützung von Extended Lc- und Le-Feldern, b6 ist RFU (b6 = 0 empfohlen), b5 b4 = 10 bezeichnet die Zuweisung der Nummern logischer Kanäle durch die Karte, b3 b2 b1 = yzt bezeichnet die maximale Anzahl logischer Kanäle: y, z, t nicht alle auf 1 gesetzt bedeutet 4y+2z+t+1, d.h. eins bis sieben; y = z = t = 1 bedeutet acht oder mehr
Tag/Length	'81' oder '82' oder '83'	Compact header des Status Indicator - nicht vorhanden, falls Category Indicator Byte = '00' - vorhanden, falls Category Indicator Byte = '80'
LCS	'00' oder '05' oder '07'	Life Cycle Status - 1. Status Indicator Byte, falls CI = '00' oder - 1. Status Indicator Byte, falls CI = '80' u. Status Indicator Header = '81' o. '83' - nicht vorhanden, falls CI = '80' und Status Indicator Header = '82' - LCS = '05' empfohlen
SW1	'6x' oder '9x'	1. Status Word - 2. Status Indicator Byte, falls CI = '00' oder - 1. Status Indicator Byte, falls CI = '80' und Status Indicator header = '82' oder - 2. Status Indicator Byte, falls CI = '80' und Status Indicator header = '83' oder - nicht vorhanden, falls CI = '80' und Status Indicator Header = '81' - SW1 = '90' empfohlen
SW2	'xx'	2. Status Word - 3. Status Indicator Byte, falls CI = '00' oder - 2. Status Indicator Byte, falls CI = '80' und Status Indicator Header = '82' oder - 3. Status Indicator Byte, falls CI = '80' und Status Indicator Header = '83' oder - nicht vorhanden, falls CI = '80' und Status Indicator Header = '81' - SW2 = '00' empfohlen
TCK	'xx'	Check Character: 'xx' = exclusives OR aller ATR-Bytes; Hinweis: Gemäß [ISO7816-3] gehört TS nicht zum ATR und geht folglich nicht in die Berechnung der XOR-Summe ein

⌫

⌦ **Card-G2-A_2044 (N801.600) K_Personalisierung: TC1 Byte im ATR**

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

⌦ **Card-G2-A_2045 (N801.700) K_Personalisierung: Historical Bytes**

Die Historical Bytes MÜSSEN gemäß [ISO7816-4] codiert werden.⌫

4.2 Allgemeine Struktur

⌦ **Card-G2-A_2046 (N801.800) K_Personalisierung: Kompatibilität zu G1-Karten**

Der HBA der Generation 2 MUSS rückwärtskompatibel zu den Karten der Generation 1 sein. Deshalb MUSS er 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_2331 (N801.820) K_Personalisierung: Container und Schlüssel für eine längere Laufzeit des HBA 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_2332 (N801.840) 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.⌫

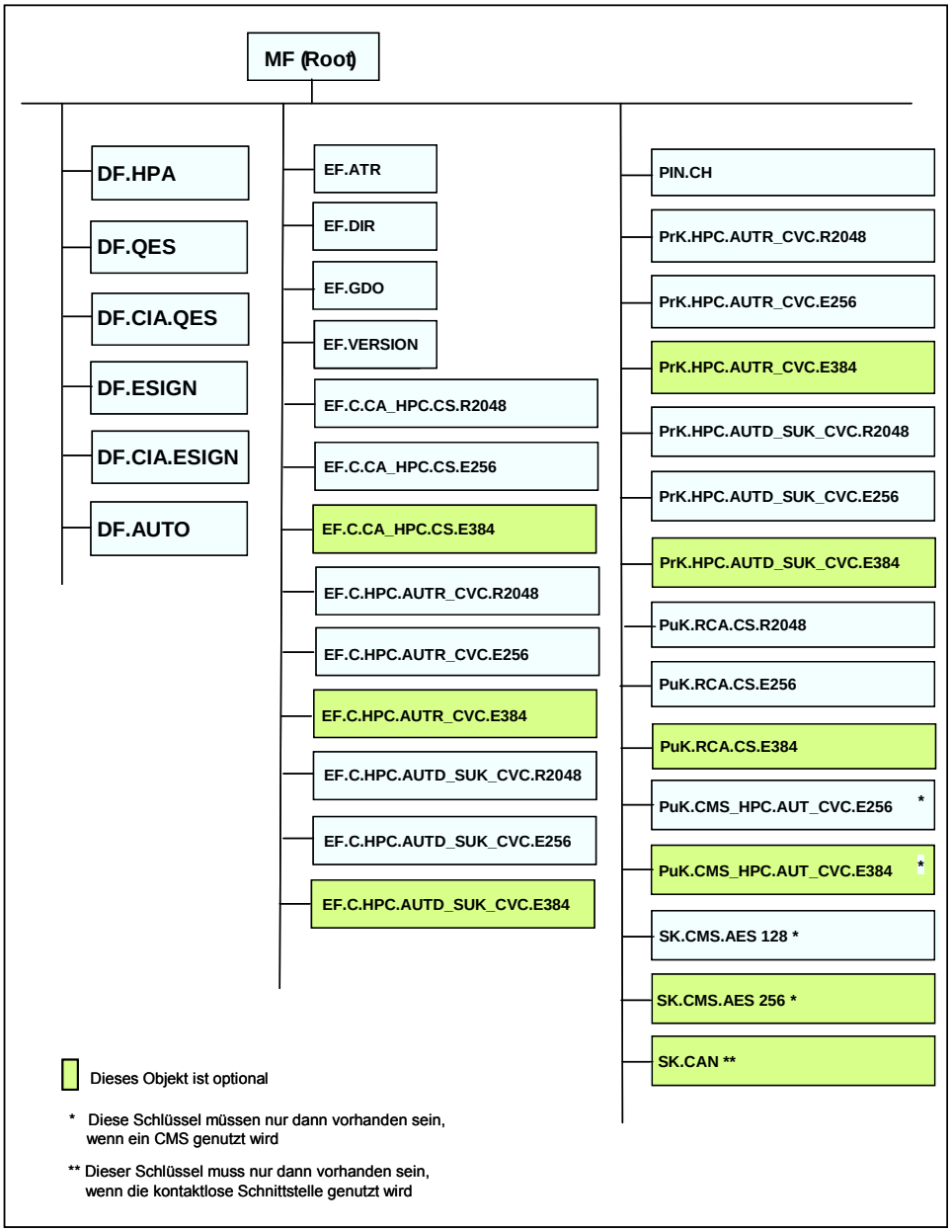

Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA

4.3 Root, die Wurzelapplikation MF

MF ist ein „Application Dedicated File“ (siehe [gemSpec_COS#8.3.1.3]).

⌦ **Card-G2-A_2047 (N802.000) K_Personalisierung: Attribute von MF**

MF MUSS die in Tab_HBA_ObjSys_004 dargestellten Werte besitzen.

Tabelle 4: Tab_HBA_ObjSys_004 Attribute von MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	

AID	´D27600014601´	
FID	´3F 00´	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
FINGERPRINT	SmMac(cvc_FlagList_TI, flag=49)	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 2: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis 3: Da sich dieser Ordner nicht deaktivieren lässt, braucht dieser Zustand für Objekte im Kapitel 4.3 nicht berücksichtigt werden.

Hinweis 4: Nur dann ausführbar, wenn ein CMS genutzt wird (optional), siehe Kapitel 4.9

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_2048 (N802.100) K_Personalisierung: Attribute von MF / EF.ATR**

EF.ATR MUSS die in Tab_HBA_ObjSys_005 dargestellten Werte besitzen.

Tabelle 5: Tab_HBA_ObjSys_005 Attribute von MF **/ EF.ATR**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 01´	siehe Hinweis 6:
shortFileIdentifier	´1D´= 29	
numberOfOctet	herstellerspezifisch	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	siehe unten
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ ” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 5: 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 6: Der Wert des Attributs fileIdentifier ist in [ISO7816-4] festgelegt.

Für das Attribut body gelten folgende Festlegungen:

⌦ **Card-G2-A_2049 (N802.200) 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_2050 (N802.300) 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_2051 (N802.400) 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´.
2. Die Oktette eins bis drei MÜSSEN gemäß Tab_HBA_ObjSys_006 codiert werden.

Tabelle 6: Tab_HBA_ObjSys_006 Wert des 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 Recordnummern
-	-	-	-	-	-	-	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
-	-	-	-	0	0	0	1	unzulässig 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
-	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

d) Das Wertfeld von DO_CardData KANN weitere DER–TLV codierte Datenobjekte enthalten.⌫

Das Wertfeld von DO_HistoricalBytes KANN weitere DER-TLV-codierte Datenobjekte enthalten. ⌫

⌦ **Card-G2-A_2053 (N802.500) K_Personalisierung: Weitere Datenobjekte in EF.ATR**

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

4.3.2 MF / EF.DIR

Die Datei enthält eine Liste mit Anwendungs-Templates gemäß [ISO7816-4]. Diese Liste wird dann angepasst, wenn sich die Applikationsstruktur durch Löschen oder Anlegen von Anwendungen verändert.

⌦ **Card-G2-A_2055 (N802.700) K_Personalisierung: Attribute von MF / EF.DIR**

EF.DIR MUSS die in Tab_HBA_ObjSys_007 dargestellten Werte besitzen.

Tabelle 7: Tab_HBA_ObjSys_007 Attribute von MF / EF.DIR

Attribute	Wert	Bemerkung
Objekttyp	linear variables Elementary File	
fileIdentifier	´2F 00´	Siehe Hinweis 8:
shortFileIdentifier	´1E´= 30	Siehe Hinweis 8:
numberOfOctet	´00BE´ Oktett = 190 Oktett	
maxNumRecords	10 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 Rekord 6 Rekord 7 Rekord 8 …	 ´61-L_{61}-(4F 06 D27600014601 || …)’ ´61-L_{61}- (4F 06 D27600014602 || …)´ ´61-L_{61}-(4F 06 D27600006601 || …)´ ´61-L_{61}- (4F 0B E828BD080F D27600006601 || …)´ ´61-L_{61}- (4F 0A A000000167 455349474E || …)´ ´61-L_{61}- (4F 0F E828BD080F A000000167 455349474E || …)´ ´61-L_{61}- (4F 06 D27600014603 || …)´ nicht vorhanden, MUSS mittels APPEND RECORD angelegt werden Ergänzungen zum DO ’61 siehe Card-G2-A_2056	 AID.MF AID.HPA AID.QES AID.CIA.QES AID.ESIGN AID.CIA ESIGN AID AUTO
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
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)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
APPEND RECORD	AUT_CMS	siehe Hinweis 9:
DELETE	AUT_CMS	siehe Hinweis 9:
READ RECORD SEARCH RECORD	SmMac(CAN) AND SmRspEnc	
UPDATE RECORD	AUT_CMS	siehe Hinweis 9:
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 7: Kommandos, die gemäß [gemSpec_COS] mit einem linear variable EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD, TERMINATE

Hinweis 8: Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

Hinweis 9: Nur dann ausführbar, wenn ein CMS genutzt wird (optional), siehe Kapitel 4.9.

⌦ **Card-G2-A_2056 (N802.750) 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_HBA_ObjSys_007 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 [Beschluss 190].

⌦ **Card-G2-A_2057 (N802.800) K_Personalisierung: Attribute von MF / EF.GDO**

EF.GDO MUSS die in Tab_HBA_ObjSys_008 dargestellten Werte besitzen.

Tabelle 8: Tab_HBA_ObjSys_008 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
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 10: 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_2058 (N802.900) 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 [EN1867]).
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 11: 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 12: Die Kennung des Kartenherausgebers entsprechend [EN1867] wird in Deutschland im Auftrag des DIN durch GS1 Germany GmbH, Köln (www.gs1-germany.de) vergeben. Der Kartenherausgeber ist gewöhnlich der rechtmäßige Besitzer der ausgegebenen Karte.

4.3.4 MF / EF.Version

Die Datei EF.Version 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 zum HBA 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 der HBA durchsetzt.

⌦ **Card-G2-A_2059 (N803.000) K_Personalisierung: Attribute von MF / EF.Version**

EF.Version MUSS die in Tab_HBA_ObjSys_009 dargestellten Werte besitzen.

Tabelle 9: Tab_HBA_ObjSys_009 Attribute von MF / EF.Version

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´2F 10´	
shortFileIdentifier	´10´= 16	
maxNumRecords	4 Rekord	
maxRecordLength	5 Oktett	
numberOfOctet	´14´ Oktett = 20 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 wir im Produkttypsteckbrief des HBA festgelegt.
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT_CMS	Siehe Hinweis 14:
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT_CMS	Siehe Hinweis 14:
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 13: 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 14: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

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

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

⌦ **Card-G2-A_2060 (N803.100) K_Personalisierung: Attribute von MF / EF.C.CA_HPC.CS.R2048**

EF.C.CA_HPC.CS.R2048 MUSS die in Tab_HBA_ObjSys_010 dargestellten Werte besitzen.

Tabelle 10: Tab_HBA_ObjSys_010 Attribute von MF / EF.C.CA_HPC.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 XX…YY´	siehe [gemSpec_COS]
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 16:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 16:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 16:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 16:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 15: 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 16: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

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

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

⌦ **Card-G2-A_2061 (N803.200) K_Personalisierung: Attribute von MF / EF.C.CA_HPC.CS.E256**

EF.C.CA_HPC.CS.E256 MUSS die in Tab_HBA_ObjSys_011 dargestellten Werte besitzen.

Tabelle 11: Tab_HBA_ObjSys_011 Attribute von MF / EF.C.CA_HPC.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´	siehe [gemSpec_COS]
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 18:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 18:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 18:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 18:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 17: 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 18: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

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

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

Diese Datei kann mit dem Kommando LOAD APPLICATION zum Nutzungsbeginn dieser Schlüssellänge erstellt werden, wenn ein System zum Nachladen verfügbar ist (Sicherheitsanker siehe Kapitel 4.3.25 bzw. Kapitel 4.3.27).

⌦ **Card-G2-A_2062 (N803.300) K_Personalisierung: Attribute von MF / EF.C.CA_HPC.CS.E384**

EF.C.CA_HPC.CS.E384 MUSS die in Tab_HBA_ObjSys_012 dargestellten Werte besitzen.

Tabelle 12: Tab_HBA_ObjSys_012 Attribute von MF / EF.C.CA_HPC.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´	siehe [gemSpec_COS]
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 20:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 20:
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 20:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 20:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 19: 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 20: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

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

EF.C.HPC.AUTR_CVC.R2048 enthält das CV-Zertifikat der HPC für die Kryptographie mit RSA für rollenbasierte C2C-Authentisierung zwischen HPC und eGK und für die Autorisierung der SMC-B. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_HPC.CS.R2048 (siehe Tab_HBA_ObjSys_010) prüfen. Das zugehörende private Schlüsselobjekt PrK.HPC.AUTR_CVC.R2048 ist im Kapitel 4.3.15 definiert.

⌦ **Card-G2-A_2063 (N803.400) K_Personalisierung: Attribute von MF / EF.C.HPC.AUTR_CVC.R2048**

EF.C.HPC.AUTR_CVC.R2048 MUSS die in Tab_HBA_ObjSys_013 dargestellten Werte besitzen.

Tabelle 13: Tab_HBA_ObjSys_013 Attribute von MF / EF.C.HPC.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		siehe [gemSpec_COS]
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 22:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 22:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 22:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 22:
Andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

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

Hinweis 22: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

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

EF.C.HPC.AUTR_CVC.E256 enthält das CV-Zertifikat der HPC für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen HPC und eGK und für die Autorisierung der SMC-B. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_HPC.CS.E256 (siehe Tab_HBA_ObjSys_011) prüfen. Das zugehörende private Schlüsselobjekt PrK.HPC.AUTR_CVC.E256 ist im Kapitel 4.3.16 definiert.

⌦ **Card-G2-A_2064 (N803.500) K_Personalisierung: Attribute von MF / EF.C.HPC.AUTR_CVC.E256**

EF.C.HPC.AUTR_CVC.E256 MUSS die in Tab_HBA_ObjSys_014 dargestellten Werte besitzen.

Tabelle 14: Tab_HBA_ObjSys_014 Attribute von MF / EF.C.HPC.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		siehe [gemSpec_COS]
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 24:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 24:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 24:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 24:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 23: 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 24: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

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

EF.C.HPC.AUTR_CVC.E384 enthält das CV-Zertifikat der HPC für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen HPC und eGK und für die Autorisierung der SMC-B. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_HPC.CS.E384 (siehe Tab_HBA_ObjSys_012) prüfen. Das zugehörende private Schlüsselobjekt PrK.HPC.AUTR_CVC.E384 ist im Kapitel 4.3.17 definiert.

Diese Datei kann mit dem Kommando LOAD APPLICATION zum Nutzungsbeginn dieser Schlüssellänge erstellt werden, wenn ein System zum Nachladen verfügbar ist (Sicherheitsanker siehe Kapitel 4.3.25 bzw. Kapitel 4.3.27).

⌧ **Card-G2-A_2065 (N803.600) K_Personalisierung: Attribute von MF / EF.C.HPC.AUTR_CVC.E384**

EF.C.HPC.AUTR_CVC.E384 MUSS die in Tab_HBA_ObjSys_015 dargestellten Werte besitzen.

Tabelle 15: Tab_HBA_ObjSys_015 Attribute von MF / EF.C.HPC.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		siehe [gemSpec_COS]
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 26:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 26:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 26:
READ BINARY	SmMac(CAN) AND SmRspEnc ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 26:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 25: 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 26: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.11 MF / EF.C.HPC.AUTD_SUK_CVC.R2048

EF.C.HPC.AUTD_SUK_CVC.R2048 enthält das CV-Zertifikat des HBA für die Kryptographie mit RSA für funktionsbasierte C2C-Authentisierung zwischen HBA/SMC-B und HBA/gSMC-K mit dem HBA als Signaturkarte für Stapel- und Komfortsignaturen (SUK), um PIN-Daten und die zu signierenden Daten (DTBS) zu empfangen. Das zugehörende private Schlüsselobjekt PrK.HPC.AUTD_SUK_CVC.R2048 ist im Kapitel 4.3.18 definiert.

⌦ **Card-G2-A_2066 (N803.700) K_Personalisierung: Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.R2048**

EF.C.HPC.AUTD_SUK_CVC.R2048 MUSS die in Tab_HBA_ObjSys_016 dargestellten Werte besitzen.

Tabelle 16: Tab_HBA_ObjSys_016 Attribute von MF / EF.C.HPC.AUTD_SUK_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	´7F21 XX…YY´	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 28:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 28:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 28:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 28:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 27: 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 28: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.12 MF / EF.C.HPC.AUTD_SUK_CVC.E256

EF.C.HPC.AUTD_SUK_CVC.E256 enthält das CV-Zertifikat des HBA für die Kryptographie mit elliptischen Kurven für funktionsbasierte C2C-Authentisierung zwischen HBA/SMC-B und HBA/gSMC-K mit dem HBA als Signaturkarte für Stapel- und Komfortsignaturen (SUK), um PIN-Daten und die zu signierenden Daten (DTBS) zu empfangen. Das zugehörende private Schlüsselobjekt PrK.HPC.AUTD_SUK_CVC.E256 ist im Kapitel 4.3.19 definiert.

⌦ **Card-G2-A_2067 (N803.800) K_Personalisierung: Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256**

EF.C.HPC.AUTD_SUK_CVC.E256 MUSS die in Tab_HBA_ObjSys_017 dargestellten Werte besitzen.

Tabelle 17: Tab_HBA_ObjSys_017 Attribute von MF / EF.C.HPC.AUTD_SUK_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	´7F21 XX…YY´	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 30:
READ BINARY	ALWAYS	

SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 30:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 30:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 30:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 29: 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 30: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.13 MF / EF.C.HPC.AUTD_SUK_CVC.E384 (optional)

EF.C.HPC.AUTD_SUK_CVC.E384 (optional) enthält das CV-Zertifikat des HBA für die Kryptographie mit elliptischen Kurven für funktionsbasierte C2C-Authentisierung zwischen HBA/SMC-B und HBA/gSMC-K mit dem HBA als Signaturkarte für Stapel- und Komfortsignaturen (SUK), um PIN-Daten und die zu signierenden Daten (DTBS) zu empfangen. Das zugehörende private Schlüsselobjekt PrK.HPC.AUTD_SUK_CVC.E384 ist im Kapitel 4.3.20 definiert.

Diese Datei kann mit dem Kommando LOAD APPLICATION zum Nutzungsbeginn dieser Schlüssellänge erstellt werden, wenn ein System zum Nachladen verfügbar ist (Sicherheitsanker siehe Kapitel 4.3.25 bzw. Kapitel 4.3.27).

⌦ **Card-G2-A_2068 (N803.900) K_Personalisierung: Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E384**

EF.C.HPC.AUTD_SUK_CVC.E384 MUSS die in Tab_HBA_ObjSys_018 dargestellten Werte besitzen.

Tabelle 18: Tab_HBA_ObjSys_018 Attribute von MF / EF.C.HPC.AUTD_SUK_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	´7F21 XX…YY´	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 32:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 32:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 32:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS	siehe Hinweis 32:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 31: 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 32: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.14 MF / PIN.CH

Das Passwortobjekt PIN.CH wird zur Freischaltung von Schlüsseln und Inhalten des HBA verwendet.

⌦ **Card-G2-A_2069 (N804.000) K_Personalisierung: Attribute von MF / PIN.CH**

PIN.CH MUSS die in Tab_HBA_ObjSys_019 dargestellten Werte besitzen.

Tabelle 19: Tab_HBA_ObjSys_019 Attribute von MF / PIN.CH

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	5	

maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword, Transport-PIN}	
flagEnabled	True	
startSsec	unendlich	
PUK	…	siehe Card-G2-A_2070 (N804.100)
pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
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)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	SmMac(CAN) AND SmCmdEnc	
GET PIN STATUS	SmMac(CAN)	
RESET RC. P1 aus der Menge {0, 1}	SmMac(CAN) AND SmCmdEnc	
VERIFY	SmMac(CAN) AND SmCmdEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

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

⌦ **Card-G2-A_2070 (N804.100) K_Personalisierung: Länge der PUK für des HBA**

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

4.3.15 MF / PrK.HPC.AUTR_CVC.R2048

PrK.HPC.AUTR_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für C2C-Authentisierungen zwischen HPC/eGK und HPC/CMS, und zur Autorisierung der SMC-B. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTR_CVC.R2048 ist in C.HPC.AUTR_CVC.R20484.5.2.6 (siehe Kapitel 4.3.8) enthalten.

⌦ **Card-G2-A_2071 (N804.200) K_Personalisierung: Attribute von MF / PrK.HPC.AUTR_CVC.R2048**

PrK.HPC.AUTR_CVC.R2048 MUSS die in Tab_HBA_ObjSys_020 dargestellten Werte besitzen.

Tabelle 20: Tab_HBA_ObjSys_020 Attribute von MF / PrK.HPC.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}	
lifeCycleStatus	„Operational state (activated)"	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	ALWAYS	

GENERATE ASYM	AUT_CMS	siehe Hinweis 35:
INTERNAL AUTH.	PWD(PIN.CH)	
TERMINATE	AUT_CMS	siehe Hinweis 35:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	SmMac(CAN)	
GENERATE ASYM	AUT_CMS	siehe Hinweis 35:
INTERNAL AUTH.	SmMac(CAN) AND PWD(PIN.CH)	
TERMINATE	AUT_CMS	siehe Hinweis 35:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 34: 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 35: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.16 MF / PrK.HPC.AUTR_CVC.E256

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

⌧ **Card-G2-A_2072 (N804.300) K_Personalisierung: Attribute von MF / PrK.HPC.AUTR_CVC.E256**

PrK.HPC.AUTR_CVC.E256 MUSS die in Tab_HBA_ObjSys_021 dargestellten Werte besitzen.

Tabelle 21: Tab_HBA_ObjSys_021 Attribute von MF / PrK.HPC.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}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 37:
INTERNAL AUTH.	PWD(PIN.CH)	
TERMINATE	AUT_CMS	siehe Hinweis 37:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	SmMac(CAN)	
GENERATE ASYM	AUT_CMS	siehe Hinweis 37:
INTERNAL AUTH.	SmMac(CAN) AND PWD(PIN.CH)	
TERMINATE	AUT_CMS	siehe Hinweis 37:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 36: 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 37: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.17 MF / PrK.HPC.AUTR_CVC.E384 (optional)

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

⌦ **Card-G2-A_2073 (N804.400) K_Personalisierung: Attribute von MF / PrK.HPC.AUTR_CVC.E384**

PrK.HPC.AUTR_CVC.E384 MUSS die in Tab_HBA_ObjSys_022 dargestellten Werte besitzen.

Tabelle 22: Tab_HBA_ObjSys_022 Attribute von MF / PrK.HPC.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}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 39:
INTERNAL AUTH.	PWD(PIN.CH)	
TERMINATE	AUT_CMS	siehe Hinweis 39:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	SmMac(CAN)	
GENERATE ASYM	AUT_CMS	siehe Hinweis 39:
INTERNAL AUTH.	SmMac(CAN) AND PWD(PIN.CH)	
TERMINATE	AUT_CMS	siehe Hinweis 39:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 38: 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 39: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.18 MF / PrK.HPC.AUTD_SUK_CVC.R2048

PrK.HPC.AUTD_SUK_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für C2C-Authentisierungen zwischen HPC/SMC-B und HPC/gSMC-K für die Übertragung von PIN-Daten und der DTBS zum HPC. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTD_SUK_CVC.R2048 ist in C.HPC.AUTD_SUK_CVC.R2048 (siehe Kapitel 4.3.11) enthalten.

⌦ **Card-G2-A_2074 (N804.500) K_Personalisierung: Attribute von MF / PrK.HPC.AUTD_SUK_CVC.R2048**

PrK.HPC.AUTD_SUK_CVC.R2048 MUSS die in Tab_HBA_ObjSys_023 dargestellten Werte besitzen.

Tabelle 23: Tab_HBA_ObjSys_023 Attribute von MF / PrK.HPC.AUTD_SUK_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´11´ = 17	
privateKey	…, Moduluslänge 2048Bit	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge {rsaSessionkey4SM}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 41:
INTERNAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 41:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	SmMac(CAN)	
GENERATE ASYM	AUT_CMS	siehe Hinweis 41:
INTERNAL AUTH.	SmMac(CAN)	
TERMINATE	AUT_CMS	siehe Hinweis 41:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 40: 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 41: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Der zu PrK.HPC.AUTD_SUK_CVC.R2048 (mit CVC-Inhaberprofil 53) gehörende öffentliche Schlüssel ist im Zertifikat C.HPC. AUTD_SUK_CVC.R2048 enthalten.

4.3.19 MF / PrK.HPC.AUTD_SUK_CVC.E256

PrK.HPC.AUTD_SUK_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit RSA für C2C-Authentisierungen zwischen HPC/SMC-B und HPC/gSMC-K für die Übertragung von PIN-Daten und der DTBS zum HPC. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTD_SUK_CVC.E256 ist in C.HPC.AUTD_SUK_CVC.E256 (siehe Kapitel 4.3.12) enthalten.

⌦ **Card-G2-A_2075 (N804.600) K_Personalisierung: Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256**

PrK.HPC.AUTD_SUK_CVC.E256 MUSS die in Tab_HBA_ObjSys_024 dargestellten Werte besitzen.

Tabelle 24: Tab_HBA_ObjSys_024 Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´09´ = 9	
privateKey	Domainparameter = brainpoolP256r1	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge {elcSessionkey4SM}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 43:
INTERNAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 43:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	SmMac(CAN)	
GENERATE ASYM	AUT_CMS	siehe Hinweis 43:
INTERNAL AUTH.	SmMac(CAN)	
TERMINATE	AUT_CMS	siehe Hinweis 43:
andere	NEVER	

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

⌫

Hinweis 42: 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 43: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Der zu PrK.HPC.AUTD_SUK_CVC.E256 (mit CVC-Inhaberprofil 53) gehörende öffentliche Schlüssel ist im Zertifikat C.HPC. AUTD_SUK_CVC.E256 enthalten.

4.3.20 MF / PrK.HPC.AUTD_SUK_CVC.E384 (optional)

PrK.HPC.AUTD_SUK_CVC.E384 ist der globale private Schlüssel für die Kryptographie mit RSA für C2C-Authentisierungen zwischen HPC/SMC-B und HPC/gSMC-K für die Übertragung von PIN-Daten und der DTBS zum HPC.

⌦ **Card-G2-A_2076 (N804.700) K_Personalisierung: Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E384**

PrK.HPC.AUTD_SUK_CVC.E384 MUSS die in Tab_HBA_ObjSys_025 dargestellten Werte besitzen.

Tabelle 25: Tab_HBA_ObjSys_025 Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´0E´ = 14	
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	Ein Wert aus der Menge {elcSessionkey4SM}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	ALWAYS	
GENERATE ASYM	AUT_CMS	siehe Hinweis 45:
INTERNAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 45:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
EXTERNAL AUTH.	SmMac(CAN)	
GENERATE ASYM	AUT_CMS	siehe Hinweis 45:
INTERNAL AUTH.	SmMac(CAN)	
TERMINATE	AUT_CMS	siehe Hinweis 45:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 44: 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 45: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Der zu EF.C.HPC.AUTD_SUK_CVC.E384 (mit CVC-Inhaberprofil 53) gehörende öffentliche Schlüssel ist im Zertifikat C.HPC. AUTD_SUK_CVC.E384 enthalten.

4.3.21 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_2077 (N804.800) K_Personalisierung: Attribute von MF / PuK.RCA.CS.R2048**

PuK.RCA.CS.R2048 MUSS die in Tab_HBA_ObjSys_026 dargestellten Werte besitzen.

Tabelle 26: Tab_HBA_ObjSys_026 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)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 47:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	SmMac(CAN)	

TERMINATE	AUT_CMS	siehe Hinweis 47:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 46: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen RSA-Signaturprüfobjekt arbeiten, sind:
PSO Verify Certificate, TERMINATE

Hinweis 47: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Die Schlüsselreferenz von PuK.RCA.CS.R2048 kann aus der HPC ausgelesen werden.

4.3.22 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_2078 (N804.900) K_Personalisierung: Attribute von MF / PuK.RCA.CS.E256**

PuK.RCA.CS.E256 MUSS die in Tab_HBA_ObjSys_027 dargestellten Werte besitzen.

Tabelle 27: Tab_HBA_ObjSys_027 Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Signaturprüfobjekt	
keyIdentifier	E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes)	wird personalisiert
expirationDate		wird personalisiert
CHAT	• OIDflags = cvc_Flags_TI • flagList = ´FF 0000 0000 7FC3´	
publicKey	brainpoolP256r1 ´2B2403030208010107´ = {1.3.36.3.3.2.8.1.1.7}	wird personalisiert
oid	ecdsa-with-SHA256 ´2A8648CE3D040302´ = {1.2.840.10045.4.3.2}	
lifeCycleStatus	„Operational state (activated)"	

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 49:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	SmMac(CAN)	
TERMINATE	AUT_CMS	siehe Hinweis 49:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 48: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen ELC-Signaturprüfobjekt arbeiten, sind:
PSO Verify Certificate, TERMINATE

Hinweis 49: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Die Schlüsselreferenz von PuK.RCA.CS.E256 kann aus dem HBA ausgelesen werden.

4.3.23 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, siehe Kapitel 4.3.22) in die Karte geladen.

⌦ **Card-G2-A_2674 (N804.950) K_Personalisierung: Attribute für PuK.RCA.CS.E384**

Die Attribute für PuK.RCA.CS.E384 MÜSSEN mit Ausnahme des keyIdentifiers, der oid und des Domainparameters den Attributen für PuK.RCA.CS.E256 entsprechen.

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⌫

4.3.24 MF / PuK.CMS_HPC.AUT_CVC.E256 (optional)

PuK.CMS_HPC.AUT_CVC.E256 (optional) ist der öffentliche Schlüssel für die Kryptographie mit elliptischen Kurven, mit dem eine Authentisierung zwischen HBA und CMS mit der Einrichtung eines TC durchgeführt wird.

⌦ **Card-G2-A_2079 (N805.100) K_Personalisierung: Attribute von MF / PuK.CMS_HPC.AUT_CVC.E256**

PuK.CMS_HPC.AUT_CVC.E256 MUSS die in Tab_HBA_ObjSys_028 dargestellten Werte besitzen.

Tabelle 28: Tab_HBA_ObjSys_028 Attribute von MF / PuK.CMS_HPC.AUT_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Authentisierungsobjekt	
keyIdentifier	'yy…..yy'	12 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	
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERAL AUTHENTICATE	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 51:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
INTERNAL AUTHENTICATE	SmMac(CAN)	
EXTERNAL AUTHENTICATE	SmMac(CAN)	
TERMINATE	AUT_CMS	siehe Hinweis 51:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 50: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen ELC-Authentisierungsobjekt arbeiten, sind: INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE, TERMINATE,

Hinweis 51: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

PuK.CMS_HPC.AUT_CVC.E256 muss genau dann in der Karte vorhanden sein, wenn ein CMS mit asymmetrischer Authentisierung mit elliptischen Kurven und der Schlüssellänge 256 bit verwendet wird. PuK.CMS_HPC.AUT_CVC.E256 ist ein globaler Schlüssel mit einem einheitlichen Key Identifier und einem CMS-spezifischen Schlüsselwert, der

zudem vom Ausgabejahr der HBA 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 HBA und CMS zum Einsatz, während die CHAT in Zugriffsregeln verwendet wird.

4.3.25 MF / PuK.CMS_HPC.AUT_CVC.E384 (optional)

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

PuK.CMS_HPC.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_HPC.AUT_CVC.E256 gehört, siehe Kapitel 4.3.22) in die Karte geladen.

⌧ **Card-G2-A_2855 (N805.200) K_Personalisierung: Attribute für PuK.CMS_HPC.AUT_CVC.E384**

Die Attribute für PuK.CMS_HPC.AUT_CVC.E384 MÜSSEN mit Ausnahme des keyIdentifiers, der oid und des Domainparameters den Attributen für PuK.CMS_HPC.AUT_CVC.E256 entsprechen.

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_HPC.AUT_CVC.E384 muss genau dann in der Karte vorhanden sein, wenn ein CMS mit asymmetrischer Authentisierung mit elliptischen Kurven und der Schlüssellänge 384 bit verwendet wird. PuK.CMS_HPC.AUT_CVC.E384 ist ein globaler Schlüssel mit einem einheitlichen Key Identifier und einem CMS-spezifischen Schlüsselwert, der zudem vom Ausgabejahr des HBA 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 HBA und CMS zum Einsatz, während die CHAT in Zugriffsregeln verwendet wird.

4.3.26 MF / SK.CMS.AES128 (optional)

SK.CMS.AES128 (optional) ist der geheime AES-Schlüssel mit 128 bit Schlüssellänge für die Durchführung des HPC/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.

⌧ **Card-G2-A_2080 (N805.300) K_Personalisierung: Attribute von MF / SK.CMS.AES128**

SK.CMS.AES128 MUSS die in Tab_HBA_ObjSys_029 dargestellten Werte besitzen.

Tabelle 29: Tab_HBA_ObjSys_029 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)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
MUTUAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 53:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
MUTUAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 53:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 52: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE; TERMINATE

Hinweis 53: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.27 MF / SK.CMS.AES256 (optional)

SK.CMS.AES256 (optional) ist der geheime AES-Schlüssel mit 256 bit Schlüssellänge für die Durchführung des HPC/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.

⌦ **Card-G2-A_2081 (N805.400) K_Personalisierung: Attribute von MF / SK.CMS.AES256**

SK.CMS.AES256 MUSS die in Tab_HBA_ObjSys_030 dargestellten Werte besitzen.

Tabelle 30: Tab_HBA_ObjSys_030 Attribute von MF / SK.CMS.AES256

Attribute	Wert	Bemerkung
Objekttyp	AES Authentisierungsobjekt	
keyIdentifier	´18´ = 22	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
MUTUAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 55:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
MUTUAL AUTH.	ALWAYS	
TERMINATE	AUT_CMS	siehe Hinweis 55:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 54: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE; TERMINATE

Hinweis 55: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.3.28 MF / SK.CAN

Das Schlüsselobjekt CAN (Card Access Number) dient dazu, eine kontaklose Kommunikationsschnittstelle zum HBA kryptographisch abzusichern.

⌦ **Card-G2-A_2868 K_Personalisierung: Attribute von MF / SK.CAN**

Wird die kontaktlose Schnittstelle genutzt, dann MUSS SK.CAN vorhanden sein und die in Tab_HBA_ObjSys_073 dargestellten Attribute besitzen.

Tabelle 31: Tab_HBA_ObjSys_073 Attribute von MF / SK.CAN

Attribute	Wert	Bemerkung
Objekttyp	symmetrisches Kartenverbindungsobjekt	
keyIdentifier	'02' = 2	
lifeCycleStatus	„Operational state (activated)"	
can	…	wird personalisiert
algorithmIdentifier	id-PACE-ECDH-GM-AES-CBC-CMAC-256	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERAL AUTHENTICATE	ALWAYS	
TERMINATE	AUT_CMS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERAL AUTHENTICATE	ALWAYS	
TERMINATE	AUT_CMS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

⌫

Hinweis 56: Kommandos, die gemäß [gemSpec_COS]] mit symmetrischen Kartenverbindungsobjekten arbeiten, sind: ACTIVATE; DEACTIVATE; DELETE, GENERAL AUTHENTICATE, TERMINATE.

⌦ **Card-G2-A_2869 (N800.750) K_Personalisierung: Generierung der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle des HBA**

Bei Nutzung der optionalen kontaktlosen Schnittstelle des HBA MUSS die Personalisierung für das Attribut *can* von SK.CAN eine sechstellige Ziffernfolge setzen⌫

⌦ **Card-G2-A_2870 (N800.800) K_Personalisierung: Druck der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle auf den HBA**

Die in SK.CAN personalisierte CAN MUSS an einer für alle HBAs definierten Fläche (Vorschlag: im Feld zwischen Gültigkeitsangabe und Foto) aufgedruckt werden. Eine entsprechende Festlegung für Ort und Art der Bedruckung MUSS in den Spezifikationen der optischen Gestaltung der HBAs der einzelnen Sektoren festgelegt werden.⌫

Die Anbringung der CAN kann z.B. in Form der Ziffernfolge oder auch in Form eines Barcodes, der vom Leser automatisch auslesbar ist, erfolgen.

4.3.29 Sicherheitsumgebungen auf MF-Ebene

Auf MF-Ebene wird ausschließlich die Sicherheitsumgebung SE#1 (Default-SE) verwendet. Es ist möglich, z. B. für die entfernte PIN-Eingabe, in SE#1 einen Trusted Channel aufzubauen.

4.4 Die Heilberufsanwendung DF.HPA

4.4.1 Dateistruktur und Dateiinhalt

Die Abbildung Abb_HBA_ObjSys_002 zeigt die Dateistruktur von DF.HPA.

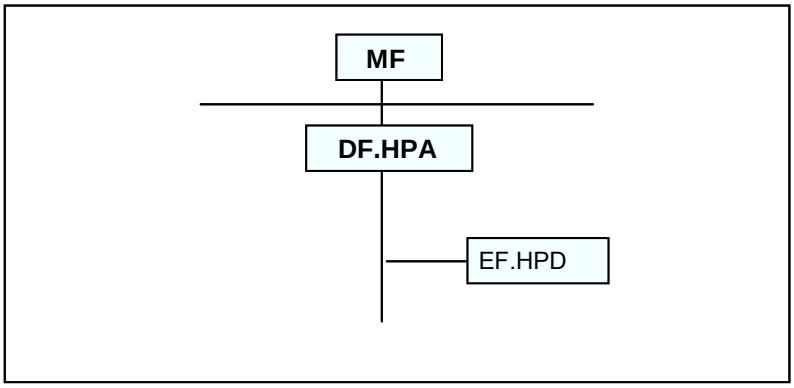

Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA

4.4.2 MF / DF.HPA (Health Professional Application)

DF.HPA ist eine “Application” gemäß [gemSpec_COS#8.3.1.1], d. h. ist mittels Anwendungskennung selektierbar.

⌧ **Card-G2-A_2082 (N806.000) K_Personalisierung: Attribute von MF / DF.HPA**

DF.HPA MUSS die in Tab_HBA_ObjSys_031 dargestellten Werte besitzen.

Tabelle 32: Tab_HBA_ObjSys_031 Attribute von MF / DF.HPA

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D27600014602’	
fileIdentifier	–	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
LOAD APPLICATION (after HPC issuing)	AUT_CMS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
LOAD APPLICATION (after HPC issuing)	AUT_CMS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 57: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: LOAD APPLICATION, SELECT

Schlüssel und CVCs für den Authentisierungsprozess befinden sich auf MF-Ebene. Die Heilberufsanwendung erlaubt das Anlegen weiterer Dateien, falls dafür in der Zukunft eine Notwendigkeit bestehen sollte, siehe Kapitel 4.9.

4.4.2.1 MF / DF.HPA / EF.HPD (Health Professional Data)

Das transparente Datei EF.HPD ist für die Speicherung von Daten vorgesehen, die sich auf den jeweiligen Heilberufler beziehen, z.B. die Bestätigung der Teilnahme an Fortbildungsmaßnahmen. Das File kann immer gelesen werden, aber eine Aktualisierung ist nur nach erfolgreicher Eingabe der PIN.CH möglich.

⌦ **Card-G2-A_2083 (N806.100) K_Personalisierung: Attribute von MF / DF.HPA / EF.HPD**

EF.HPD MUSS die in Tab_HBA_ObjSys_032 dargestellten Werte besitzen.

Tabelle 33: Tab_HBA_ObjSys_032 Attribute von MF / DF.HPA / EF.HPD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 01´	
shortFileIdentifier	´01´= 1	
numberOfOctet	´0800´ Oktett = 2048 Oktett	
flagTransactionMode	False	

flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.CH)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
ERASE / WRITE / UPDATE BINARY	SmMac(CAN) AND SmCmdEnc AND PWD(PIN.CH)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 58: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

4.4.2.2 Sicherheitsumgebungen

In DF.HPA wird das SE#1 verwendet.

4.5 Die Anwendung für die qualifizierte elektronische Signatur (DF.QES)

Dieses Kapitel enthält die Objekte, die die QES-Anwendung beschreiben. Dies ist gleichzeitig die Sicht einer Signaturanwendungskomponente, welche diese Anwendung nutzen möchte.

4.5.1 Dateistruktur und Dateiinhalt

Die Abbildung Abb_HBA_ObjSys_003 zeigt die prinzipielle Dateistruktur der QES-Anwendung, die in Übereinstimmung mit [DIN66291-1] definiert ist.

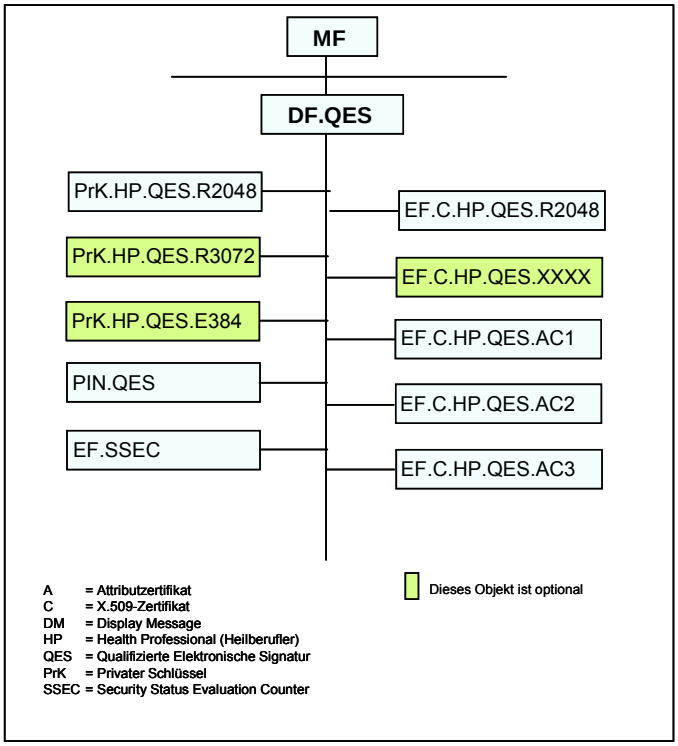

Abbildung 3: Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung

Die QES-Anwendung besitzt EFs für das X.509-QES-Zertifikat und maximal drei Attributzertifikate. Zusätzlich ist ein EF zur Anzeige des unterstützten Maximalwertes des SSEC angelegt.

4.5.2 MF / DF.QES (Qualified Electronic Signature Application)

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

⌧ **Card-G2-A_2084 (N807.000) K_Personalisierung: Attribute von MF / DF.QES**

DF.QES MUSS die in Tab_HBA_ObjSys_033 dargestellten Werte besitzen.

Tabelle 34: Tab_HBA_ObjSys_033 Attribute von MF / DF.QES

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	´D276000066 01´	siehe Hinweis 60:
FID	–	siehe Hinweis 61:
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 63:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 63:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 59: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis 60: Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 61: Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [ISO7816-4#8.1.1]

Hinweis 62: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 4.5.2 nicht berücksichtigt zu werden.

Hinweis 63: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.5.2.1 MF / DF.QES / PrK.HP.QES.R2048

PrK.HP.QES.R2048 ist der private Schlüssel für die Kryptographie mit RSA zur Berechnung von qualifizierten elektronischen Signaturen. Die Eigenschaften der PIN.QES werden in Kapitel 4.5.2.4 dargestellt. Der zugehörige öffentliche Schlüssel PuK.HP.QES.R2048 ist in C.HP.QES.R2048 (siehe Kapitel 4.5.2.6) enthalten.

⌧ Card-G2-A_2085 (N807.100) K_Personalisierung: Attribute von MF / DF.QES / PrK.HP.QES.R2048

PrK.HP.QES.R2048 MUSS die in Tab_HBA_ObjSys_034 dargestellten Werte besitzen.

Tabelle 35: Tab_HBA_ObjSys_034 Attribute von MF / DF.QES / PrK.HP.QES.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Signierobjekt	
keyIdentifier	´04´ = 4	siehe Hinweis 65:
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	
algorithmIdentifier	alle Werte aus der Menge { signPSS, sign9796_2_DS2-}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
GEN. ASYM KEY PAIR.	nicht Gegenstand dieser Spezifikation	siehe Hinweis 67:
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
TERMINATE	AUT_CMS	siehe Hinweis 66:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
COMPUTE DIGITAL SIGNATURE	PWD(PIN.QES) AND SmMac('D27600004000' || '33') AND SmCmdEnc AND SmRespEnc	siehe Hinweis 68:

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
GEN. ASYM KEY PAIR.	nicht Gegenstand dieser Spezifikation	siehe Hinweis 67:
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
TERMINATE	AUT_CMS	siehe Hinweis 66:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
COMPUTE DIGITAL SIGNATURE	SmMac(CAN) AND SmCmdEnc AND SmRspEnc AND {PWD(PIN.QES) AND SmMac('D27600004000' || '33') AND SmCmdEnc AND SmRespEnc }	siehe Hinweis 68:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

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

Hinweis 65: Der Wert des Attributes keyIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 66: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Hinweis 67: Die Zugriffsbedingung wird durch den ZDA festgelegt

Hinweis 68: Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115]. Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)

4.5.2.2 MF / DF.QES / PrK.HP.QES.R3072 (optional)

DF.QES / PrK.HP.QES.R3072 ist der private Schlüssel für die Kryptographie mit RSA zur Berechnung von qualifizierten elektronischen Signaturen. Der zugehörige öffentliche Schlüssel PuK.HP.QES.R3072 ist in C.HP.QES.R30724.5.2.6 (siehe Kapitel 4.5.2.7) enthalten. Die Eigenschaften der PIN.QES werden in Kapitel 4.5.2.4 dargestellt.

⌦ **Card-G2-A_2086 (N807.200) K_Personalisierung: Attribute von MF / DF.QES / DF.QES / PrK.HP.QES.R3072**

DF.QES / PrK.HP.QES.R3072 MUSS die in Tab_HBA_ObjSys_035 dargestellten Werte besitzen.

Tabelle 36: Tab_HBA_ObjSys_035 Attribute von MF / DF.QES / DF.QES / PrK.HP.QES.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Signierobjekt	
keyIdentifier	´05´ = 5	siehe Hinweis 70:
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
keyAvailable	True	
algorithmIdentifier	alle Werte aus der Menge {signPSS, sign9796_2_DS2}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
GENERATE ASYM	nicht Gegenstand dieser Spezifikation	siehe Hinweis 72:
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
TERMINATE	AUT_CMS	siehe Hinweis 71:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
COMPUTE DIGITAL SIGNATURE	{PWD(PIN.QES) AND SmMac(‘D27600004000’ || '33') AND SmCmdEnc AND SmRespEnc }	siehe Hinweis 73:
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
GENERATE ASYM	nicht Gegenstand dieser Spezifikation	siehe Hinweis 72:
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
TERMINATE	AUT_CMS	siehe Hinweis 71:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
COMPUTE DIGITAL SIGNATURE	SmMac(CAN) AND SmCmdEnc AND SmRspEnc AND {PWD(PIN.QES) AND SmMac('D27600004000' || '33') AND SmCmdEnc AND SmRespEnc }	siehe Hinweis 73:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 69: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Signierobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, TERMINATE

Hinweis 70: Der Wert des Attributes keyIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 71: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Hinweis 72: Die Zugriffsbedingung wird durch den ZDA festgelegt

Hinweis 73: Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115]. Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)

4.5.2.3 MF / DF.QES / PrK.HP.QES.E384 (optional)

PrK.HP.QES.E384 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven zur Berechnung von qualifizierten elektronischen Signaturen. Der zugehörige öffentliche Schlüssel PuK.HP.QES.RE384 ist in C.HP.QES.E3844.5.2.6 (siehe Kapitel 4.5.2.7) enthalten. Die Eigenschaften der PIN.QES werden in Kapitel 4.5.2.4 dargestellt.

⌧ **Card-G2-A_2087 (N807.300) K_Personalisierung: Attribute von MF / DF.QES / PrK.HP.QES.E384**

PrK.HP.QES.E384 MUSS die in Tab_HBA_ObjSys_036 dargestellten Werte besitzen.

Tabelle 37: Tab_HBA_ObjSys_036 Attribute von MF / DF.QES / PrK.HP.QES.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Signierobjekt	
keyIdentifier	´07´ = 7	siehe Hinweis 75:
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
keyAvailable	True	
algorithmIdentifier	alle Werte aus der Menge { signPSS, sign9796_2_DS2}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
GENERATE ASYM	nicht Gegenstand dieser Spezifikation	siehe Hinweis 77:
TERMINATE	AUT_CMS	siehe Hinweis 76:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
COMPUTE DIGITAL SIGNATURE	PWD(PIN.QES) AND SmMac(cvc_FlagList_TI, flag=51) AND SmCmdEnc AND SmRespEnc	siehe Hinweis 78:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
GENERATE ASYM	nicht Gegenstand dieser Spezifikation	siehe Hinweis 67:
TERMINATE	AUT_CMS	siehe Hinweis 76:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
COMPUTE DIGITAL SIGNATURE	SmMac(CAN) AND SmCmdEnc AND SmRspEnc AND {PWD(PIN.QES) AND SmMac(cvc_FlagList_TI, flag=51) AND SmCmdEnc AND SmRespEnc }	siehe Hinweis 78:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 74: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Signierobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, TERMINATE

Hinweis 75: Der Wert des Attributes keyIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 76: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Hinweis 77: Die Zugriffsbedingung wird durch den ZDA festgelegt

Hinweis 78: Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115]. Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)

Anmerkung – Trotz der AND-Relation der Sicherheitsbedingungen kann die HPC allein nicht ausschließen, dass die Authentisierung mit Profil 51 ohne Vereinbarung von SM-Schlüsseln erfolgte und die SM-Schlüssel mit einem von 51 verschiedenen Profil der Gegenseite vereinbart wurden (die Authentisierung mit Profil 51 könnte dabei bestehen bleiben). Das wird durch zwei beschränkende Maßnahmen verhindert: Erstens kann der private Schlüssel der gSMC-K mit Profil 51 (SAK) nur unter Vereinbarung von SM-Schlüsseln genutzt werden. Zweitens verlangt die Zugriffsregel der dem Profil 51 zugeordneten Authentisierungsschlüssels der gSMC-K, dass sich die HPC mit Profil 53 zuerst gegenüber der gSMC-K authentisiert. Da die Speicherung von Vorstellungsschlüsseln keinen Sicherheitsstatus setzt, können nach Authentisierung der gSMC-K ggf. in der HPC vorliegende SM-Schlüssel nur aus eben jener Authentisierung stammen.

4.5.2.4 MF / DF.QES / PIN.QES

PIN.QES ist eine DF-spezifische PIN, die nur zum Schutz des privaten Schlüssels für die qualifizierte elektronische Signatur des Heilberuflers (PrK.HP.QES.R2048) gemäß SigG/SigV verwendet wird. Die PIN besteht aus 6 bis 8 Ziffern.

Die Nutzung eines 8 bis 12-stelligen Rücksetz-Codes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Sicherheitsstatus von PIN.QES kann nur für eine begrenzte Anzahl von Signaturen verwendet werden, d. h. der SSEC-Maximalwert ist endlich.

Die PIN-Referenz für die Kommandos VERIFY, CHANGE REFERENCE DATA und RESET RETRY COUNTER und andere PIN-Eigenschaften sind in der folgenden Tabelle Tab_HBA_ObjSys_037 zusammengefasst.

⌧ **Card-G2-A_2088 (N807.400) K_Personalisierung: Attribute von MF / DF.QES / PIN.QES**

PIN.QES MUSS die in Tab_HBA_ObjSys_037 dargestellten Werte besitzen.

Tabelle 38: Tab_HBA_ObjSys_037 Attribute von MF / DF.QES / PIN.QES

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	
startRetryCounter	3	
retryCounter	3	
transportStatus	Ein Wert aus der Menge {Transport-PIN, Reguläres Passwort}…	wird personalisiert
flagEnabled	True	
Start Security Status Evaluation Counter	SE # 1: SSEC = 1 SE # 2: 1 ≤ SSEC ≤ 250	Max. Wert in SE # 2 wie in EF.SSEC angezeigt
PUK	…	wird personalisiert
pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC., P1=1	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	SmMac(CAN) AND SmCmdEnc	
GET PIN STATUS	SmMac(CAN)	
RESET RC., P1=1	SmMac(CAN) AND SmCmdEnc	
VERIFY	SmMac(CAN) AND SmCmdEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 79: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind:
ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE

4.5.2.5 MF / DF.QES / EF.SSEC

Die transparente Datei EF.SSEC zeigt die SSEC-Maximalwerte an, die für eine konkrete Anwendungsumgebung der HPC gemäß Evaluierung und Bestätigung der HPC als Sichere Signaturerstellungseinheit definiert wurden.

⌦ **Card-G2-A_2089 (N807.500) K_Personalisierung: Attribute von MF / DF.QES / EF.SSEC**

EF.SSEC MUSS die in Tab_HBA_ObjSys_038 dargestellten Werte besitzen.

Tabelle 39: Tab_HBA_ObjSys_038 Attribute von MF / DF.QES / EF.SSEC

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘D0 05’	
shortFileIdentifier	‘05’ = 5	
numberOfOctet	´002E´ Oktett = 46 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7B2C XX…YY´	Wird personalisiert, siehe Tab_HBA_ObjSys_039
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	

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

⌫

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

Der Inhalt von EF.SSEC (siehe Tab_HBA_ObjSys_038) wird während der Personalisierung gespeichert. Die externe Signaturanwendungskomponente kann den Inhalt der Datei lesen, um die Größe des Signaturstapels zu optimieren. Es ist allerdings nicht möglich, die aktuellen SSEC-Werte aus der Karte auszulesen, da die zulässigen SSEC-Maximalwerte während der Kartenproduktion im RAM fest implementiert werden und der aktuelle Stand vom COS verwaltet wird. Die Angaben in EF.SSEC müssen den implementierten SSEC-Maximalwerten entsprechen.

⌦ **Card-G2-A_2090 (N807.600) K_Personalisierung: Inhalt von EF.SSEC**

Der Inhalt von EF.SSEC MUSS die in Tab_HBA_ObjSys_039 dargestellten Werte besitzen.

Tabelle 40: Tab_HBA_ObjSys_039 Inhalt von EF.SSEC

Tag	Länge	Bedeutung					
'7B'	'2C'	Datenobjekte der Sicherheitsumgebung					
		Tag	Länge	Wert	Bedeutung		
		'80'	'01'	'01'	Sicherheitsumgebung: 1		
		'A4'	'11'	Authentication Template			
				Tag	Länge	Wert	Bedeutung
				'82'	'06'	'D27600006601'	DF-Name: DF.QES
				'83'	'01'	'81'	Schlüsselreferenz: PIN.QES
				'95'	'01'	'08'	Usage Qualifier: Benutzerauthentisierung
				'C0'	'01'	'01'	SSEC-Maximalwert: 1
		Tag	Länge	Wert	Bedeutung		
		'80'	'01'	'02'	Sicherheitsumgebung: 2		

		‘A4’	‘11’	Authentication Template			
				Tag	Länge	Wert	Bedeutung
				‘82’	‘06’	‘D27600006601’	DF-Name: PIN.QES
				‘83’	‘01’	‘81’	Schlüsselreferenz: PIN.QES
				‘95’	‘01’	‘08’	Usage Qualifier: Benutzerauthentisierung
				‘C0’	‘01’	‘xx’	SSEC-Maximalwert, z.B. 250

⌫

Anmerkung 1 – Abgesehen vom SSEC-Object werden unterhalb des Tag ‘7B’ die Datenobjekte gemäß [ISO7816-4] verwendet. Der SSEC-Maximalwert könnte auch in der CIA.QES-Datei EF.PrKD als “Common Object Attribute” “userConsent” ausgedrückt werden. Allerdings würde ein Wert von beispielsweise 250 die in [ISO7816-15] definierte Obergrenze („cia-ub-userConsent“ = 15) überschreiten. Zudem kann das Attribut “userConsent” schwerlich mit einzelnen Sicherheitsumgebungen verknüpft werden.

Anmerkung 2 – Die SSEC-Maximalwerte im Bereich 251-254 sollten nicht verwendet werden, da diese Werte im COS möglicherweise eine andere Bedeutung haben. Falls ein unbegrenzter SSEC notwendig ist, muss das in EF.SSEC durch die Kodierung ‘FF’ im SSEC-Feld angezeigt werden.

4.5.2.6 MF / DF.QES / EF.C.HP.QES.R2048

Die transparente Datei EF.C.HP.QES.R2048 enthält das X.509-Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel des Heilberuflers PuK.HP.QES.R2048 für die qualifizierte elektronische Signatur gemäß SiG/SigV. Das zugehörende private Schlüsselobjekt PrK.HP.QES.R2048 ist im Kapitel 4.5.2.1 definiert.

⌦ **Card-G2-A_2091 (N807.700) K_Personalisierung: Attribute von MF / DF.QES / EF.C.HP.QES.R2048**

EF.C.HP.QES.R2048 MUSS die in Tab_HBA_ObjSys_040 dargestellten Werte besitzen.

Tabelle 41: Tab_HBA_ObjSys_040 Attribute von MF / DF.QES / EF.C.HP.QES.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C0 00´	siehe Hinweis 82:
shortFileIdentifier	´10´= 16	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, Zertifikat für PrK.CH.QES.R2048	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 83:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	AUT_CMS	siehe Hinweis 83:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 83:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	AUT_CMS	siehe Hinweis 83:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
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: Der Wert des Attributes fileIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 83: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.5.2.7 MF / DF.QES / EF.C.HP.QES.XXXX (optional)

Die Datei EF.C.HP.QES.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 4.5.2.2 und 4.5.2.3 definiert.

⌦ **Card-G2-A_2092 (N807.800) K_Personalisierung: Attribute von MF / DF.QES / EF.C.HP.QES.XXXX**

Die Attribute von EF.C.HP.QES.XXXX MÜSSEN mit Ausnahme von FID und SFID identisch zu denen von EF.C.HP.QES.R2048 sein.⌫

⌦ **Card-G2-A_2093 (N807.900) K_Personalisierung: Werte für FID und SFID für MF / DF.QES / EF.C.HP.QES.XXXX**

Als fileIdentifier und shortFileIdentifier für EF.C.HP.QES.XXXX MÜSSEN die Werte aus Tab_HBA_ObjSys_041 verwendet werden:

Tabelle 42: Tab_HBA_ObjSys_041 Fileidentifier für optionale Nachfolgezertifikate in DF.QES

Datei	FID	SFID
EF.C.HP.QES.XXXX	C0 04	04
EF.C.HP.QES-AC1.XXXX	C0 05	05
EF.C.HP.QES-AC2.XXXX	C0 06	06
EF.C.HP.QES-AC3.XXXX	C0 07	07

⌫

4.5.2.8 MF / DF.QES / EF.C.HP.QES-AC1, MF / DF.QES / EF.C.HP.QES-AC2 und MF / DF.QES / EF.C.HP.QES-AC3

Die transparenten Dateien EF.C.HP.QES-AC1, EF.C.HP.QES-AC2 und EF.C.HP.QES-AC3 können X.509-Attributzertifikate enthalten, z. B. von einer Heilberufskammer (z. B. Ärztekammer, Apothekerkammer) oder von einer entsprechenden Organisation (z. B. einer Ärztevereinigung). Die charakteristischen Dateiattribute und Zugriffsregeln sind in den nachfolgenden Tabellen dargestellt. Bei Nutzung eines neuen Zertifikates (EF.C.HP.QES.R2048) oder Umstellung auf R3072, E256 oder E384 müssen die vorhandenen Attributzertifikate durch neue ersetzt werden, die an das neue Zertifikat gebunden sind.

⌦ **Card-G2-A_2094 (N808.000) K_Personalisierung: Attribute von MF / DF.QES / EF.C.HP.QES-AC1**

EF.C.HP.QES-AC1 MUSS die in Tab_HBA_ObjSys_042 dargestellten Werte besitzen.

Tabelle 43: Tab_HBA_ObjSys_042 Attribute von MF / DF.QES / EF.C.HP.QES-AC1

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C0 01’	siehe Hinweis 85:

shortFileIdentifier	'01' = 1	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
Body	´XX…YY´, Attributs-Zertifikat für PrK.HP.QES.R2048	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	SmMac(CAN) AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	SmMac(CAN) AND SmCmdEnc AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung

Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

⌦ **Card-G2-A_2095 (N808.100) K_Personalisierung: Attribute von MF / DF.QES / EF.C.HP.QES-AC2**

EF.C.HP.QES-AC2 MUSS die in Tab_HBA_ObjSys_043 dargestellten Werte besitzen.

Tabelle 44: Tab_HBA_ObjSys_043 Attribute von MF / DF.QES / EF.C.HP.QES-AC2

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C0 02	siehe Hinweis 85:
shortFileIdentifier	‘02 = 2	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
Body	´XX…YY´, Attributs-Zertifikat für PrK.HP.QES.R2048	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	SmMac(CAN) AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	SmMac(CAN) AND SmCmdEnc AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

⌦ **Card-G2-A_2096 (N808.200) K_Personalisierung: Attribute von MF / DF.QES / EF.C.HP.QES-AC3**

EF.C.HP.QES-AC3 MUSS die in Tab_HBA_ObjSys_044 dargestellten Werte besitzen.

Tabelle 45: Tab_HBA_ObjSys_044 Attribute von MF / DF.QES / EF.C.HP.QES-AC3

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C0 03	siehe Hinweis 85:
shortFileIdentifier	‘03= 3	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
Body	´XX…YY´, Attributs-Zertifikat für PrK.HP.QES.R2048	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	SmMac(CAN) AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	SmMac(CAN) AND SmCmdEnc AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
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

Hinweis 85: Der Wert des Attributes fileIdentifier ist in [ISO7816-4] festgelegt.

Alle TLV-kodierten X.509-Zertifikate besitzen als erstes Byte das Tag ‘30’ (eines Sequence-Objektes). Wenn die Datei kein Zertifikat enthält, so muss das dadurch angezeigt werden, dass das erste Byte auf ’00’ gesetzt ist.

4.6 Die ESIGN-Anwendung (DF.ESIGN)

4.6.1 Dateistruktur und Dateiinhalt

Die Abbildung Abb_HBA_ObjSys_004 zeigt die prinzipielle Struktur der ESIGN-Anwendung, die in Übereinstimmung mit [EN14890-1] definiert ist.

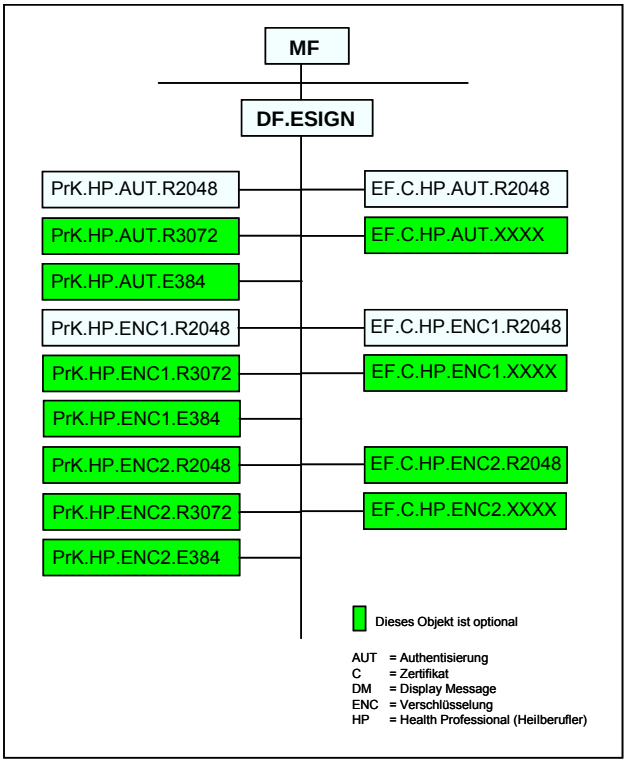

Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN

4.6.2 MF / DF.ESIGN

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

Die allgemeine ESIGN Anwendung ist in DF.ESIGN dargestellt und wird im HBA für folgende Funktionen genutzt:

- Die Client/Server-Authentisierung,

- die Nachrichtensignatur,
- die Schlüssel-Chiffrierungsfunktion für die kryptographische Sicherung von Daten und

⌦ **Card-G2-A_2097 (N809.000) K_Personalisierung: Attribute von MF / DF.ESIGN**

DF.ESIGN MUSS die in Tab_HBA_ObjSys_045 dargestellten Werte besitzen.

Tabelle 46: Tab_HBA_ObjSys_045 Attribute von MF / DF.ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	´A000000167 455349474E´	siehe Hinweis 87:
fileIdentifier	–	siehe Hinweis 88:
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 90:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 90:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 86: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis 87: Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 88: Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1].

Hinweis 89: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 4.6 nicht berücksichtigt zu werden.

Hinweis 90: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.6.2.1 MF / DF.ESIGN / PrK.HP.AUT.R2048

PrK.HP.AUT.R2048 ist der private Schlüssel für die Kryptographie mit RSA für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HP.AUT.R2048 ist in C.HP.AUT.R2048 (siehe Kapitel 4.6.2.10) enthalten.

⌦ **Card-G2-A_2098 (N809.100) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048**

PrK.HP.AUT.R2048 MUSS die in Tab_HBA_ObjSys_046 dargestellten Werte besitzen.

Tabelle 47: Tab_HBA_ObjSys_046 Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´02´ = 2	wird personalisiert
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)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYM	AUT_CMS	siehe Hinweis 92:
TERMINATE	AUT_CMS	siehe Hinweis 92:

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
INTERNAL AUTH. PSO Comp Dig Sig	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYM	AUT_CMS	siehe Hinweis 92:
TERMINATE	AUT_CMS	siehe Hinweis 92:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 91: 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 92: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.6.2.2 MF / DF.ESIGN / PrK.HP.AUT.R3072 (optional)

PrK.HP.AUT.R3072 ist der private Schlüssel für die Kryptographie mit RSA für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HP.AUT.R3072 ist in C.HP.AUT.R3072 (siehe Kapitel 4.6.2.11) enthalten.

⌦ **Card-G2-A_2099 (N809.200) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.AUT.R3072**

PrK.HP.AUT.R3072 MUSS die in Tab_HBA_ObjSys_047 dargestellten Werte besitzen.

Tabelle 48: Tab_HBA_ObjSys_047 Attribute von MF / DF.ESIGN / PrK.HP.AUT.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´05´ = 5	wird personalisiert
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)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 94:
TERMINATE	AUT_CMS	siehe Hinweis 94:
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 94:
TERMINATE	AUT_CMS	siehe Hinweis 94:
INTERNAL AUTH. PSO Comp Dig Sig	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	

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

⌫

Hinweis 93: 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 94: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.6.2.3 MF / DF.ESIGN / PrK.HP.AUT.E384 (optional)

PrK.HP.AUT.E384 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HP.AUT.E384 ist in C.HP.AUT.E384 (siehe Kapitel 4.6.2.11) enthalten.

⌦ **Card-G2-A_2100 (N809.300) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.AUT.E384**

PrK.HP.AUT.E384 MUSS die in Tab_HBA_ObjSys_048 dargestellten Werte besitzen.

Tabelle 49: Tab_HBA_ObjSys_048 Attribute von MF / DF.ESIGN / PrK.HP.AUT.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´08´ = 8	wird personalisiert
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcRoleAuthentication}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS c	siehe Hinweis 96:

INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
TERMINATE	AUT_CMS	siehe Hinweis 96:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 96:
INTERNAL AUTH. PSO Comp Dig Sig	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
TERMINATE	AUT_CMS	siehe Hinweis 96:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Elliptischen Kurven-Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 95: 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 96: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.6.2.4 MF / DF.ESIGN / PrK.HP.ENC1.R2048

PrK.HP.ENC1.R2048 ist der private Schlüssel für die Kryptographie mit RSA für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Der zugehörige öffentliche Schlüssel PuK.HP.ENC1.R2048 ist in C.HP.ENC1.R2048 (siehe Kapitel 4.6.2.12) enthalten.

Card-G2-A_2101 (N809.400) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.ENC1.R2048

PrK.HP.ENC1.R2048 MUSS die in Tab_HBA_ObjSys_049 dargestellten Werte besitzen.

Tabelle 50: Tab_HBA_ObjSys_049 Attribute von MF / DF.ESIGN / PrK.HP.ENC1.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´03´ = 3	wird personalisiert
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Decipher PSO Transcipher	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	

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

⌫

Hinweis 97: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, PSO Encipher, PSO Transcipher, TERMINATE

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.6.2.5 MF / DF.ESIGN / PrK.HP.ENC2.R2048

PrK.HP.ENC2.R2048 ist der private Schlüssel zur Nutzung nach dem Ablauf des Zertifikats EF.C.HP.ENC1.2048 und des dazugehörenden Schlüssels PrK.HP.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.HP.ENC2.R2048 ist in C.HP.ENC2.R2048 (siehe Kapitel 4.6.2.13) enthalten.

⌦ **Card-G2-A_2102 (N809.500) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.ENC2.R2048**

PrK.HP.ENC2.R2048 MUSS die in Tab_HBA_ObjSys_050 dargestellten Werte besitzen.

Tabelle 51: Tab_HBA_ObjSys_050 Attribute von MF / DF.ESIGN / PrK.HP.ENC2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´0B´ = 11	wird personalisiert
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5}	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

GENERATE ASYM	AUT_CMS	siehe Hinweis 99:
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 99:
PSO Decipher PSO Transcipher	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 98: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, PSO Encipher, PSO Transcipher, TERMINATE

Hinweis 99: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9. Es MUSS organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HP.ENC2.R2048 genutzt werden kann.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.6.2.6 MF / DF.ESIGN / PrK.HP.ENC1.R3072 (optional)

PrK.HP.ENC1.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 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HP.ENC1.R3072 ist in C.HP.ENC1.R3072 (siehe Kapitel 4.6.2.14) enthalten.

⌧ **Card-G2-A_2103 (N809.600) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.ENC1.R3072**

PrK.HP.ENC1.R3072 MUSS die in Tab_HBA_ObjSys_051 dargestellten Werte besitzen.

Tabelle 52: Tab_HBA_ObjSys_051 Attribute von MF / DF.ESIGN / PrK.HP.ENC1.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´0E´ = 14	wird personalisiert
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 101:
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung

GENERATE ASYM	AUT_CMS	siehe Hinweis 101:
PSO Decipher PSO Transcipher	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 100: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, PSO Encipher, PSO Transcipher, TERMINATE

Hinweis 101: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9. Es MUSS organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HP.ENC1.R3072 genutzt werden kann.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.6.2.7 MF / DF.ESIGN / PrK.HP.ENC2.R3072 (optional)

PrK.HP.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.HP.ENC1.R3072 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HP.ENC2.R3072 ist in C.HP.ENC2.R3072 (siehe Kapitel 4.6.2.15) enthalten.

Card-G2-A_2104 (N809.700) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.ENC2.R3072

PrK.HP.ENC2.R3072 MUSS die in Tab_HBA_ObjSys_052 dargestellten Werte besitzen.

Tabelle 53: Tab_HBA_ObjSys_052 Attribute von MF / DF.ESIGN / PrK.HP.ENC2.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´0C´ = 12	wird personalisiert
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 103:
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 103:
PSO Decipher PSO Transcipher	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		

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

⌫

Hinweis 102: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, PSO Encipher, PSO Transcipher, TERMINATE

Hinweis 103: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9. Es MUSS organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HP.ENC2.R3072 genutzt werden kann.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.6.2.8 MF / DF.ESIGN / PrK.HP.ENC1.E384 (optional)

PrK.HP.ENC1.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 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HP.ENC1.E384 ist in C.HP.ENC1.E384 (siehe Kapitel 4.6.2.14) enthalten.

⌦ **Card-G2-A_2105 (N809.800) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.ENC1.E384**

PrK.HP.ENC1.E384 MUSS die in Tab_HBA_ObjSys_053 dargestellten Werte besitzen.

Tabelle 54: Tab_HBA_ObjSys_053 Attribute von MF / DF.ESIGN / PrK.HP.ENC1.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Entschlüsselungsobjekt	
keyIdentifier	´09´ = 9	wird personalisiert
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { elcSharedSecretCalculation }	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 105:
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 105:
PSO Decipher PSO Transcipher	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 104: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, PSO Encipher, PSO Transcipher, TERMINATE

Hinweis 105: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9. Es MUSS organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HP.ENC1.E384 genutzt werden kann.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.6.2.9 MF / DF.ESIGN / PrK.HP.ENC2.E384 (optional)

PrK.HP.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.HP.ENC1.E384 und des dazugehörenden Schlüssels PrK.HP.ENC1.E384 von der dazu berechtigten Instanz mit dem Kommando GENERATE ASYMMETRIC KEY PAIR angestoßen. Der zugehörige öffentliche Schlüssel PuK.HP.ENC2.E384 ist in C.HP.ENC2.E384 (siehe Kapitel 4.6.2.15) enthalten.

⌧ **Card-G2-A_2106 (N809.900) K_Personalisierung: Attribute von MF / DF.ESIGN / PrK.HP.ENC2.E384**

PrK.HP.ENC2.E384 MUSS die in Tab_HBA_ObjSys_054 dargestellten Werte besitzen.

Tabelle 55: Tab_HBA_ObjSys_054 Attribute von MF / DF.ESIGN / PrK.HP.ENC2.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Entschlüsselungsobjekt	
keyIdentifier	´0D´ = 13	wird personalisiert
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] { elcSharedSecretCalculation }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 107:
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYM	AUT_CMS	siehe Hinweis 107:
PSO Decipher PSO Transcipher	SmMac(CAN) AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 106: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature, PSO Encipher, PSO Transcipher, TERMINATE

Hinweis 107: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9. Es MUSS organisatorisch sichergestellt werden, dass dieses Kommando nur bei der erstmaligen Erzeugung von PrK.HP.ENC2.E384 genutzt werden kann.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.6.2.10 MF / DF.ESIGN / EF.C.HP.AUT.R2048

Die Datei EF.C.HP.AUT.R2048 enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.AUT.R2048. Das zugehörende private Schlüsselobjekt PrK.HP.AUT.R2048 ist in Kapitel 4.6.2.1 definiert.

⌦ **Card-G2-A_2107 (N810.000) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048**

EF.C.HP.AUT.R2048 MUSS die in Tab_HBA_ObjSys_055 dargestellten Werte besitzen.

Tabelle 56: Tab_HBA_ObjSys_055 Attribute von MF / DF.ESIGN / EF.C.HP.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
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 109:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	AUT_CMS	siehe Hinweis 109:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis 109:
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	AUT_CMS	siehe Hinweis 109:
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	

⌫

Hinweis 108: 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 109: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.6.2.11 MF / DF.ESIGN / EF.C.HP.AUT.XXXX (optional)

Die Datei EF.C.HP.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 4.6.2.2 und 4.6.2.3 definiert.

⌦ **Card-G2-A_2108 (N810.100) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HP.AUT.XXXX**

Die Attribute von EF.C.HP.AUT.XXXX MÜSSEN mit Ausnahme der FID und der SFID identisch zu denen von EF.C.HP.AUT.R2048 sein.⌫

⌦ **Card-G2-A_2109 (N810.150) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HP.AUT.XXXX**

Folgende Werte MÜSSEN für FID und SFID für EF.C.HP.AUT.XXXXXXXX verwendet werden:

FID: ’C5 06’

SFID: ’06’ ⌫

4.6.2.12 MF / DF.ESIGN / EF.C.HP.ENC1.2048

Die Datei EF.C.HP.ENC1.2048 enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.ENC1.R2048. Das zugehörende private Schlüsselobjekt PrK.HP.ENC1.R2048 ist im Kapitel 4.6.2.4 definiert.

⌦ **Card-G2-A_2110 (N810.200) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HP.ENC1.2048**

EF.C.HP.ENC1.2048 MUSS die in Tab_HBA_ObjSys_056 dargestellten Werte besitzen.

Tabelle 57: Tab_HBA_ObjSys_056 Attribute von MF / DF.ESIGN / EF.C.HP.ENC1.2048

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
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 110: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, TERMINATE, WRITE BINARY

4.6.2.13 MF / DF.ESIGN / EF.C.HP.ENC2.2048

Die Datei EF.C.HP.ENC2.2048 ist dafür vorgesehen, nach dem Ablauf des Zertifikats EF.C.HP.ENC1.2048 und des dazugehörenden Schlüssels PrK.HP.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 im Kapitel 4.6.2.5 definiert.

⌦ **Card-G2-A_2111 (N810.300) K_Personalisierung: Zugriffsregeln für EF.C.HP.ENC2.2048**

Die Zugriffsrechte für EF.C.HP.ENC2.2048 MÜSSEN mit Ausnahme von FID und SFID mit folgender Ergänzung identisch zu denen für EF.C.HP.ENC1.2048 sein.

UPDATE BINARY	AUT_CMS	siehe Hinweis 111:

⌫

Hinweis 111: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

⌦ **Card-G2-A_2112 (N810.350) K_Personalisierung: Werte für FID und SFID für EF.C.HP.ENC2.2048**

Folgende Werte MÜSSEN für FID und SFID für EF.C.HP.ENC2.2048verwendet werden:

FID: ’C2 03´

SFID: ´ ’03´= 3⌫

4.6.2.14 MF / DF.ESIGN / EF.C.HP.ENC1.XXXX (optional)

Die Datei EF.C.HP.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 4.6.2.6 und 4.6.2.8 definiert.

⌦ **Card-G2-A_2113 (N810.400) K_Personalisierung: Attribute von MF / DF.ESIGN / EF.C.HP.ENC1.XXXX**

Die Attribute von EF.C.HP.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.HP.ENC1.2048 sein.

UPDATE BINARY	AUT_CMS	siehe Hinweis 112:

⌫

Hinweis 112: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9

⌦ **Card-G2-A_2114 (N810.450) K_Personalisierung: Werte für FID und SFID für MF / DF.ESIGN / EF.C.HP.ENC1.XXXX**

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

FID: ’C2 08´

SFID: ´ ’08´= 8⌫

4.6.2.15 MF / DF.ESIGN / EF.C.HP.ENC2.XXXX (optional)

Die Datei EF.C.HP.ENC2.XXXX ist dafür vorgesehen, nach dem Ablauf des Zertifikats EF.C.HP.ENC1.XXXX und des dazugehörenden Schlüssels (PrK.HP.ENC1.R3072 bzw. PrK.HP.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 4.6.2.7 und 4.6.2.9 definiert.

⌦ **Card-G2-A_2115 (N810.500) K_Personalisierung: Attribute von EF.C.HP.ENC1.XXXX**

Die Attribute von EF.C.HP.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.HP.ENC1.2048 sein.

UPDATE BINARY	AUT_CMS	siehe Hinweis 113:

⌫

Hinweis 113: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9

⌦ **Card-G2-A_2116 (N810.600) K_Personalisierung: Werte für FID und SFID für EF.C.HP.ENC2.XXXX**

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

FID: ’C2 0B´

SFID: ´ ’0B´= 11⌫

4.6.3 Sicherheitsumgebungen

DF.ESIGN wird ausschließlich in SE#1 (Default SE) genutzt. Es ist möglich, in SE#1 einen Trusted Channel aufzubauen, um beispielsweise Remote-Konfigurationen mit einer stationären HPC zu ermöglichen.

4.7 Die kryptographischen Informationsanwendungen

Die Abbildung Abb_HBA_ObjSys_005 zeigt die prinzipielle Struktur der kryptographischen Informationsanwendungen (CIAs), die mit der QES- und der ESIGN-Anwendung verknüpft sind.

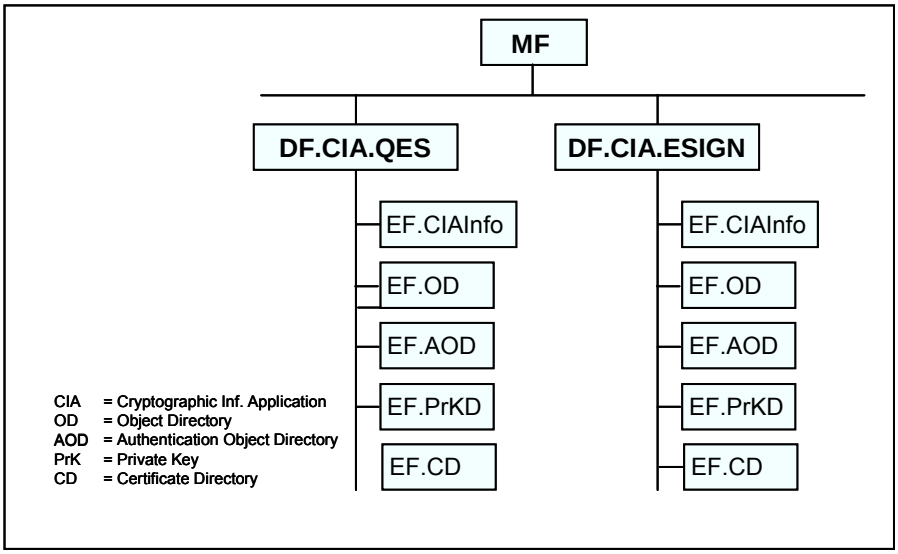

Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen

4.7.1 MF / DF.CIA.QES und MF / DF.CIA.ESIGN (Cryptographic Information Applications)

In [EN14890-1] ist das Vorhandensein einer kryptographischen Informationsanwendung (CIA) vorgeschrieben, um unterstützte Algorithmen, Dateikennungen etc. anzuzeigen, welche für die entsprechende QES- bzw. ESIGN-Anwendung relevant sind. Allgemein enthält DF.CIA.x die Dateien EF.CIAInfo und EF.OD (Object Directory) sowie möglicherweise weitere Dateien, welche die FIDs, Schlüssel, PINs, Zertifikate etc. beschreiben.

⌧ **Card-G2-A_2117 (N811.000) K_Personalisierung: Attribute von MF / DF.CIA.QES**

DF.CIA.QES MUSS die in Tab_HBA_ObjSys_057 dargestellten Werte besitzen.

Tabelle 58: Tab_HBA_ObjSys_057 Attribute von MF / DF.CIA.QES

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	‘'E828BD080F D27600006601’	siehe Hinweis 115:
FID	–	siehe Hinweis 116:
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 118:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 118:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

⌦ **Card-G2-A_2118 (N811.050) K_Personalisierung: Attribute von MF / DF.CIA_ESIGN**

DF.CIA_ESIGN MUSS die in Tab_HBA_ObjSys_058 dargestellten Werte besitzen.

Tabelle 59: Tab_HBA_ObjSys_058 Attribute von MF / DF.CIA_ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	´E828BD080F A000000167455349474E´	siehe Hinweis 115:
FID	–	siehe Hinweis 116:
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 114: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis 115: Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [ISO7816-15] sowie als PIX den applicationIdentifier von [ISO7816-4].

Hinweis 116: Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS# 8.1.1]

Hinweis 117: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 4.7 nicht berücksichtigt zu werden.

Hinweis 118: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.7.2 Dateien mit kryptographischen Informationsobjekten (CIOs)

Die logischen File-Namen, File Identifier, Short File Identifier und die Dateiinhalte sind konform zu [ISO7816-15]. Die entsprechenden CIO-Dateien beider Anwendungen DF.CIA.QES und DF.CIA.ESIGN besitzen die gleichen charakteristischen Attribute und Zugriffsregeln.

⌦ **Card-G2-A_2119 (N811.100) K_Personalisierung: Attribute von EF.CIA.CIAInfo**

EF.CIA.CIAInfo MUSS die in Tab_HBA_ObjSys_059 dargestellten Werte besitzen.

Tabelle 60: Tab_HBA_ObjSys_059 Attribute von EF.CIA.CIAInfo (Cryptographic Information Application Info)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´50 32´	siehe Hinweis 120:

shortFileIdentifier	´12´= 18	siehe Hinweis 120:
numberOfOctet	´0100' Oktett = 256 Oktett oder auf die Länge der CIOs beschränkt	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 119: 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 120: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

Card-G2-A_2120 (N811.200) K_Personalisierung: Attribute von EF.OD (Object Directory)

EF.OD MUSS die in Tab_HBA_ObjSys_060 dargestellten Werte besitzen.

Tabelle 61: Tab_HBA_ObjSys_060 Attribute von EF.OD (Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	’50 31’	siehe Hinweis 122:
shortFileIdentifier	‘11’ = 17	siehe Hinweis 122:
numberOfOctet	’0040’ Oktett = 64 Oktett oder auf die Länge der CIOs beschränkt	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
body	...	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 121: 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 122: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

⌦ **Card-G2-A_2121 (N811.300) K_Personalisierung: Attribute von EF.AOD (Authentication Object Directory)**

EF.AOD MUSS die in Tab_HBA_ObjSys_061 dargestellten Werte besitzen.

Tabelle 62: Tab_HBA_ObjSys_061 Attribute von EF.AOD (Authentication Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 34'	siehe Hinweis 124:
shortFileIdentifier	'14' = 20	siehe Hinweis 124:
numberOfOctet	'0080' Oktett = 128 Oktett oder auf die Länge der CIOs beschränkt	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
body	...	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 123: 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 124: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

⌦ **Card-G2-A_2122 (N811.400) K_Personalisierung: Attribute von EF.PrKD (Private Key Directory)**

EF.PrKD MUSS die in Tab_HBA_ObjSys_062 dargestellten Werte besitzen.

Tabelle 63: Tab_HBA_ObjSys_062 Attribute von EF.PrKD (Private Key Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 35'	siehe Hinweis 126:
shortFileIdentifier	'15' = 21	siehe Hinweis 126:
numberOfOctet	'0080' Oktett = 128 Oktett oder auf die Länge der CIOs beschränkt	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
body	...	

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 125: 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 126: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

⌦ **Card-G2-A_2123 (N811.500) K_Personalisierung: Attribute von EF.CD (Certificate Directory)**

EF.CD MUSS die in Tab_HBA_ObjSys_063 dargestellten Werte besitzen.

Tabelle 64: Tab_HBA_ObjSys_063 Attribute von EF.CD (Certificate Directory)

Attribute	Wert	Bemerkung

Objekttyp	transparentes Elementary File	
fileIdentifier	’50 38’	siehe Hinweis 128:
shortFileIdentifier	‘16’ = 22	siehe Hinweis 128:
numberOfOctet	‘0080’ Oktett = 128 Oktett oder auf die Länge der CIOs beschränkt	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
body	...	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Hinweis 127: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis 128: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

4.8 Die Organisationsspezifische Authentisierungsanwendung (DF.AUTO)

Die Organisationsspezifische Authentisierungsanwendung DF.AUTO ist eine Anwendung, deren Struktur auf einem HBA stets vorhanden ist. Es liegt im Ermessen der HPC-Herausgeberorganisation (Berufskammer), ob die Anwendung nutzbar gemacht werden kann. Die eigentliche Nutzung der Anwendung liegt im Ermessen des Karteninhabers. Falls die Organisationsspezifische Authentisierungsanwendung genutzt wird, dann ist der Inhalt dieses Kapitels verbindlich vorgeschrieben.

4.8.1 Dateistruktur und Dateiinhalt

DF.AUTO wird genutzt für

- organisationsspezifische Authentisierungsprozesse (z. B. Windows Logon mit Smart Card), welche mit der ESIGN-Anwendung aufgrund technischer Unterschiede (z. B. proprietäre Zertifikatserweiterungen) oder eines unvereinbaren Verfahrens (z. B. vorgeschriebenes PIN-Caching) nicht umgehen können.

Die Abbildung Abb_HBA_ObjSys_006 zeigt die prinzipielle Struktur der AUTO-Anwendung.

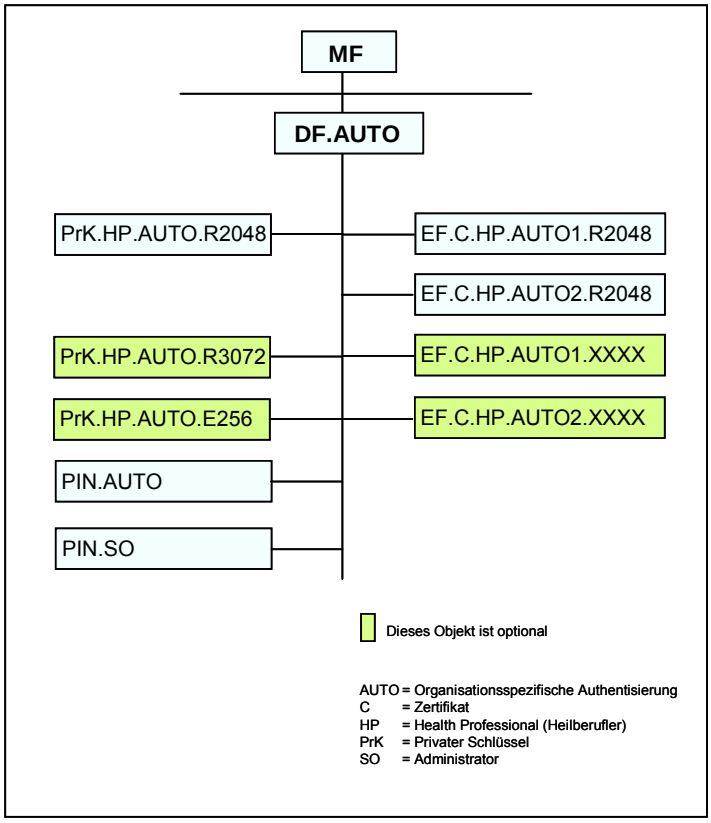

Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO

4.8.2 DF.AUTO (Organization-specific Authentication Application)

DF.AUTO ist ein “Application Directory” gemäß [gemSpec_COS#8.3.1.1], d.h., es ist mittels Anwendungskennung selektierbar.

⌧ **Card-G2-A_2124 (N812.000) K_Personalisierung: Attribute von MF / DF.AUTO**

DF.AUTO MUSS die in Tab_HBA_ObjSys_064 dargestellten Werte besitzen.

Tabelle 65: Tab_HBA_ObjSys_064 Attribute von MF / DF.AUTO

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D27600014603’	siehe Hinweis 130:
fileIdentifier	–	siehe Hinweis 131:
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 133:

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 133:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 129: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis 130: Der Wert des Attributes applicationIdentifier ist in [ISO7816-4].

Hinweis 131: Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1]

Hinweis 132: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 4.8 nicht berücksichtigt zu werden.

Hinweis 133: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

4.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R2048

PrK.HP.AUTO.R2048 ist der private Schlüssel für die Kryptographie mit RSA für Client-/Server-Authentisierung.

⌦ **Card-G2-A_2125 (N812.100) K_Personalisierung: Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048**

PrK.HP.AUTO.R2048 MUSS die in Tab_HBA_ObjSys_065 dargestellten Werte besitzen.

Tabelle 66: Tab_HBA_ObjSys_065 Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´02´ = 2	wird personalisiert
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication , rsign9796_2_DS2, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR	PWD(PIN.SO)	
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.AUTO)	
TERMINATE	AUT_CMS	siehe Hinweis 135:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR	SmMac(CAN) AND SmCmdEnc AND SmRspEnc AND PWD(PIN.SO)	
INTERNAL AUTH. PSO Comp Dig Sig	SmMac(CAN) AND PWD(PIN.AUTO)	
TERMINATE	AUT_CMS	siehe Hinweis 135:

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

⌫

Hinweis 134: 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 135: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Anmerkung – PrK.HP.AUTO.R2048 ist ein privates RSA-Objekt, welches gemäß Kapitel 9.6.3 in [gemSpec_COS] das GENERATE ASYMMETRIC KEY PAIR Kommando unterstützt. Da die organisationsspezifische Zertifikatsinformation dem Personalisierer wahrscheinlich nicht bekannt ist, kann es notwendig sein, dieses Kommando während der Kartennutzung zu verwenden, um eine Generierung von Zertifikaten zu ermöglichen.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.8.2.2 MF / DF.AUTO / PrK.HP.AUTO.R3072 (optional)

PrK.HP.AUTO.R3072 ist der private Schlüssel für die Kryptographie mit RSA für Client-/Server-Authentisierung.

⌦ **Card-G2-A_2126 (N812.200) K_Personalisierung: Attribute von MF / DF.AUTO/PrK.HP.AUTO.R3072**

PrK.HP.AUTO.R3072 MUSS die in Tab_HBA_ObjSys_066 dargestellten Werte besitzen.

Tabelle 67: Tab_HBA_ObjSys_066 Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´04´ = 4	wird personalisiert
privateKey	…, Moduluslänge 3072 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication , rsign9796_2_DS2, signPKCS1_V1_5, signPSS}	

lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR	PWD(PIN.SO)	
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.AUTO)	
TERMINATE	AUT_CMS	siehe Hinweis 137:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated) ”kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR	SmMac(CAN) AND SmCmdEnc AND SmRspEnc AND PWD(PIN.SO)	
INTERNAL AUTH. PSO Comp Dig Sig	SmMac(CAN) AND PWD(PIN.AUTO)	
TERMINATE	AUT_CMS	siehe Hinweis 137:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

Hinweis 136: 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 137: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Anmerkung – PrK.HP.AUTO.R3072 ist ein privates RSA-Objekt, welches gemäß Kapitel 9.6.3 in [gemSpec_COS] das GENERATE ASYMMETRIC KEY PAIR Kommando unterstützt. Da die organisationsspezifische Zertifikatsinformation dem Personalisierer wahrscheinlich nicht bekannt ist, kann es notwendig sein, dieses Kommando während der Kartennutzung zu verwenden, um eine Generierung von Zertifikaten zu ermöglichen.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.8.2.3 MF / DF.AUTO / PrK.HP.AUTO.E384 (optional)

PrK.HP.AUTO.E384 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für Client-/Server-Authentisierung.

⌧ **Card-G2-A_2127 (N812.300) K_Personalisierung: Attribute von MF / DF.AUTO / PrK.HP.AUTO.E384**

PrK.HP.AUTO.E384 MUSS die in Tab_HBA_ObjSys_067 dargestellten Werte besitzen.

Tabelle 68: Tab_HBA_ObjSys_067 Attribute von MF / DF.AUTO / PrK.HP.AUTO.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Authentisierungsobjekt	
keyIdentifier	´06´ = 6	wird personalisiert
privateKey	Domainparameter = brainpoolP384r1	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {elcRoleAuthentication, sign9796_2_DS2, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR	PWD(PIN.SO)	
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.AUTO)	
TERMINATE	AUT_CMS	siehe Hinweis 139:
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated) "kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR	SmMac(CAN) AND SmCmdEnc AND SmRspEnc AND PWD(PIN.SO)	
INTERNAL AUTH. PSO Comp Dig Sig	SmMac(CAN) AND PWD(PIN.AUTO)	
TERMINATE	AUT_CMS	siehe Hinweis 139:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
SELECT	ALWAYS	
andere	NEVER	

⌫

Hinweis 138: 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 139: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 4.9.

Anmerkung – PrK.HP.AUTO.E384 ist ein privates RSA-Objekt, welches gemäß Kapitel 9.6.3 in [gemSpec_COS] das GENERATE ASYMMETRIC KEY PAIR Kommando unterstützt. Da die organisationsspezifische Zertifikatsinformation dem Personalisierer wahrscheinlich nicht bekannt ist, kann es notwendig sein, dieses Kommando während der Kartennutzung zu verwenden, um eine Generierung von Zertifikaten zu ermöglichen.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116].

4.8.2.4 MF / DF.AUTO / PIN.AUTO

PIN.AUTO ist eine DF-spezifische PIN, die ausschließlich dem Schutz des privaten Authentisierungsschlüssels für den organisationsspezifischen Authentisierungsmechanismus des Heilberuflers (PrK.HP.AUT.R2048, optional PrK.HP.AUT.R3072) dient. PIN.AUTO muss genau 5 Ziffern besitzen.

Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Sicherheitsstatus von PIN.AUTO kann unbegrenzt verwendet werden, d. h. der Default-Wert von SSEC beträgt unendlich.

Die nachfolgende Tabelle Tab_HBA_ObjSys_068 zeigt die PIN-Referenz, wie sie in den Kommandos VERIFY, CHANGE REFERENCE DATA und RESET RETRY COUNTER verwendet wird, und weitere PIN-Eigenschaften.

⌦ **Card-G2-A_2128 (N812.400) K_Personalisierung: Attribute von MF / DF.AUTO / PIN.AUTO**

PIN.AUTO MUSS die in Tab_HBA_ObjSys_068 dargestellten Werte besitzen.

Tabelle 69: Tab_HBA_ObjSys_068 Attribute von MF / DF.AUTO / PIN.AUTO

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	Wird personalisiert
minimumLength	5	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	Ein Verfahren gemäß [gemSpec_COS#8.2.5]	
flagEnabled	True	
startSsec	unendlich	
PUK	…	Wird personalisiert
pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC. P1=1	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	SmMac(CAN) AND SmCmdEnc	
GET PIN STATUS	SmMac(CAN) AND SmCmdEnc	
RESET RC. P1=1	SmMac(CAN) AND SmCmdEnc	
VERIFY	SmMac(CAN) AND SmCmdEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 140: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind:
ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE

Die Initialisierung von PIN.AUTO, z. B. durch Nutzung einer Transport-PIN, unterliegt den Richtlinien der zuständigen Organisation. Falls eine Transport-PIN verwendet wird, so muss ein Verfahren aus [gemSpec_COS#8.2.5] zum Einsatz kommen.

4.8.2.5 MF / DF.AUTO / PIN.SO

PIN.SO ist eine DF-spezifische PIN, die für administrative Zwecke bezüglich DF.AUTO verwendet wird, d. h. zur Generierung des asymmetrischen Schlüsselpaars und zum Aktualisieren der organisationsspezifischen Authentisierungszertifikate. PIN.SO besteht aus 6 bis 8 Ziffern.

Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Sicherheitsstatus von PIN.SO kann unbegrenzt verwendet werden, d. h. der Default-Wert von SSEC beträgt unendlich.

Die nachfolgende Tabelle Tab_HBA_ObjSys_069 zeigt die PIN-Referenz, wie sie in den Kommandos VERIFY, CHANGE REFERENCE DATA und RESET RETRY COUNTER verwendet wird, und weitere PIN-Eigenschaften.

Card-G2-A_2129 (N812.500) K_Personalisierung: Attribute von MF / DF.AUTO / PIN.SO

PIN.SO MUSS die in Tab_HBA_ObjSys_069 dargestellten Werte besitzen.

Tabelle 70: Tab_HBA_ObjSys_069 Attribute von MF / DF.AUTO / PIN.SO

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´03´ = 3	
secret	…	Wird personalisiert
minimumLength	6	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	Ein Verfahren gemäß [gemSpec_COS#8.2.5]	
flagEnabled	True	
startSsec	unendlich	
PUK	…	Wird personalisiert
pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC. P1=1	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	alle	alle
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	andere
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	SmMac(CAN) AND SmCmdEnc	
GET PIN STATUS	SmMac(CAN) AND SmCmdEnc	
RESET RC. P1=1	SmMac(CAN) AND SmCmdEnc	
VERIFY	SmMac(CAN) AND SmCmdEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis 141: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind:
ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE

Die Initialisierung von PIN.SO, z. B. durch Nutzung einer Transport-PIN, unterliegt den Richtlinien der zuständigen Organisation. Falls eine Transport-PIN verwendet wird, so muss ein Verfahren aus [gemSpec_COS#8.2.5] zum Einsatz kommen.

4.8.2.6 MF / DF.AUTO / EF.C.HP.AUTO1.R2048 und MF / DF.AUTO / EF.C.HP.AUTO2.R2048

EF.C.HP.AUTO1.R2048 und EF.C.HP.AUTO2.R2048 enthalten die organisationsspezifischen X.509-AUT-Zertifikate des Heilberuflers für die Kryptographie mit RSA. Damit können dem Heilberufler zwei verschiedene Identitäten zur Verfügung stehen, die beide mit demselben privaten Schlüssel PrK.HP.AUTO.R2048 (optional PrK.HP.AUTO.R3072) verknüpft sind.

Die Zertifikate können nach erfolgreicher Authentisierung mit PIN.SO aktualisiert werden, siehe Tab_HBA_ObjSys_070 und Tab_HBA_ObjSys_071.

⌦ **Card-G2-A_2130 (N812.600) K_Personalisierung: Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048**

EF.C.HP.AUTO1.R2048 MUSS die in Tab_HBA_ObjSys_070 dargestellten Werte besitzen.

Tabelle 71: Tab_HBA_ObjSys_070 Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘E0 01’	
shortFileIdentifier	‘01’ = 1	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
body	´	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	PWD(PIN.SO)	
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.SO)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	SmMac(CAN) AND PWD(PIN.SO)	
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE /	SmMac(CAN)	

UPDATE BINARY	AND SmCmdEnc AND PWD(PIN.SO)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

⌦ **Card-G2-A_2131 (N812.700) K_Personalisierung: MF / DF.AUTO / EF.C.HP.AUTO2.R2048**

EF.C.HP.AUTO2.R2048 MUSS die in Tab_HBA_ObjSys_071 dargestellten Werte besitzen.

Tabelle 72: Tab_HBA_ObjSys_071 Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'E0 02'	
shortFileIdentifier	'02' = 2	
numberOfOctet	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
body		wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	PWD(PIN.SO)	
READ BINARY	ALWAYS	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	PWD(PIN.SO)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	SmMac(CAN) AND PWD(PIN.SO)	
READ BINARY	SmMac(CAN) AND SmRspEnc	
SELECT	ALWAYS	
ERASE / WRITE / UPDATE BINARY	SmMac(CAN) AND SmCmdEnc AND PWD(PIN.SO)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

4.8.2.7 MF / DF.AUTO / EF.C.HP.AUTO1.XXXX und MF / DF.AUTO / EF.C.HP.AUTO2.XXXX (optional)

EF.C.HP.AUTO1.XXXX und EF.C.HP.AUTO2.XXXX können mit dem Kommando LOAD APPLICATION zum Nutzungsbeginn des ausgewählten Verfahrens mit der dazugehörenden Schlüssellänge erstellt werden, wenn ein System zum Nachladen verfügbar ist (Sicherheitsanker siehe Kapitel 4.3.25 bzw. Kapitel 4.3.27).

Diese Verzeichnisse enthalten die organisationsspezifischen X.509-AUT-Zertifikate des Heilberuflers für die Kryptographie mit R3072 oder mit E384. Damit können dem Heilberufler zwei verschiedene Identitäten zur Verfügung stehen, die beide mit demselben privaten Schlüssel (entweder PrK.HP.AUTO.R3072 oder PrK.HP.AUTO.E384) verknüpft sind.

⌦ **Card-G2-A_2132 (N812.800) K_Personalisierung: Attribute von MF / DF.AUTO/ EF.C.HP.AUTO1.XXXX und MF / DF.AUTO/ EF.C.HP.AUTO2.XXXX**

Die Attribute von EF.C.HP.AUTO1.XXXX bzw. EF.C.HP.AUTO2.XXXX MÜSSEN mit Ausnahme von FID und SFID identisch mit den Attributen von EF.C.HP.AUTO1.R2048 bzw. EF.C.HP.AUTO2.R2048 sein.⌫

⌦ **Card-G2-A_2133 (N812.900) K_Personalisierung: Werte für FID und SFID für MF / DF.AUTO/ EF.C.HP.AUTO1.XXXX und MF / DF.AUTO/ EF.C.HP.AUTO2.XXXX**

Als fileIdentifier und shortFileIdentifier MÜSSEN für EF.C.HP.AUTO1.XXXX und EF.C.HP.AUTO2.XXXX die Werte in Tab_HBA_ObjSys_072 verwendet werden:

Tabelle 73: Tab_HBA_ObjSys_072 FileIdentifier für optionale Nachfolge-Zertifikate in DF.AUTO

Datei	FID	SFID
EF.C.HP.AUTO1.XXXX	'E0 03'	'03'
EF.C.HP.AUTO2.XXXX	'E0 04'	'04'

⌫

Die Zertifikate können nach erfolgreicher Authentisierung mit PIN.SO aktualisiert werden.

4.8.2.8 Sicherheitsumgebungen

In DF.AUTO wird ausschließlich das voreingestellte SE#1 verwendet.

4.8.2.9 Vorgaben für die Nutzung von DF.AUTO

Falls die HPC-Herausgeberorganisation (Berufskammer) die Nutzung der Anwendung ermöglichen will, dann gilt bezüglich der zu personalisierenden Daten:

⌦ **Card-G2-A_2675 (N813.000) K_Personalisierung: Wert von PrK.AUTO.XXXX**

PrK.HP.AUTO.XXXX (XXXX aus der Menge {R2048, R3048, E384}) MUSS auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2676 (N813.100) K_Personalisierung: Wert von PIN.AUTO**

PIN.AUTO MUSS auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2677 (N813.200) K_Personalisierung: Wert von PUK für PIN.AUTO**

PUK für PIN.AUTO MUSS auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2678 (N813.300) K_Personalisierung: Wert von PIN.SO**

PIN.SO MUSS auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2679 (N813.400) K_Personalisierung: Wert von PUK für PIN.SO**

PUK für PIN.SO MUSS auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2680 (N813.500) K_Personalisierung: Inhalt von EF.C.HP.AUTO1.XXXX**

EF.C.HP.AUTO1.XXXX (XXXX aus der Menge {R2048, R3048, E384}) KANN einen beliebigen Wert enthalten. Falls hier kein passendes X.509-Zertifikat eingetragen ist, so liegt es im Ermessen des Karteninhabers ein passendes X.509-Zertifikat einzutragen.⌫

⌦ **Card-G2-A_2681 (N813.600) K_Personalisierung: Inhalt von EF.C.HP.AUTO1.XXXX**

EF.C.HP.AUTO2.XXXX (XXXX aus der Menge {R2048, R3048, E384}) KANN einen beliebigen Wert enthalten. Falls hier kein passendes X.509-Zertifikat eingetragen ist, so liegt es im Ermessen des Karteninhabers ein passendes X.509-Zertifikat einzutragen.⌫

⌦ **Card-G2-A_2682 (N813.700) K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.AUTO**

Falls die HPC-Herausgeberorganisation (Berufskammer) die Nutzung der Anwendung DF.AUTO unterbinden will, dann DARF sich der Sicherheitszustand von PIN.AUTO NICHT setzen lassen.⌫

⌦ **Card-G2-A_2856 (N813.800) K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.SO**

Falls die HPC-Herausgeberorganisation (Berufskammer) die Nutzung der Anwendung DF.AUTO unterbinden will, dann DARF sich der Sicherheitszustand von PIN.SO NICHT setzen lassen.⌫

Hinweis 142: Hinweis: Um das Setzen eines Sicherheitszustandes zu unterbinden wird es als hinreichend angesehen, wenn die Attribute "Secret" und "PUK" eines Passwortobjektes auf zufällige acht- bis zwölfstellige Werte gesetzt werden.

4.9 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des HBA

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien und EF.Version) nach der Ausgabe des HBA von einem Card Application Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CMS optional. Die Inhalte in [gemSpec_COS#14] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe des HBA durchgeführt werden sollen.

Anhang A – Verzeichnisse

A1 - Abkürzungen

Kürzel	Erläuterung
AID	Application Identifier (Anwendungskennung)
AOD	Authentication Object Directory
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
ASCII	American Standard Code for Information Interchange
AT	Authentication Template
ATR	Answer-to-Reset
AUT	Authentisierung
AUTD	CV-basierte Geräteauthentisierung
AUTR	CV-basierte Rollenauthentisierung
AUTO	Organisationsspezifische Authentisierung
BA	Berufsausweis
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
BNA	Bundesnetzagentur
C	Zertifikat
C2C	Card to Card
CA	Certification Authority (Zertifizierungsdiensteanbieter)
CMS	Card Application Management System
CAR	Certification Authority Reference
CC	Cryptographic Checksum (kryptographische Prüfsumme)
CD	Certificate Directory
CER	Canonical Encoding Rules
CG	Cryptogram
CH	Cardholder (Karteninhaber)
CHAT	Certificate Holder Autorisation Template Liste von Rechten, die ein Zertifikatsinhaber besitzt
CHR	Certificate Holder Reference
CIA	Cryptographic Information Application
CIO	Cryptographic Information Objects
CLA	Class-Byte einer Kommando-APDU

Kürzel	Erläuterung
COS	Card Operating System (Chipkartenbetriebssystem)
CPI	Certificate Profile Identifier
CRL	Certificate Revocation List (Zertifikatssperrliste)
CS	CertSign (CertificateSigning)
CTA	Card Terminal Application (Kartenterminalanwendung)
CV	Card Verifiable
CVC	Card Verifiable Certificate
D,DIR	Directory
DE	Datenelement
DER	Distinguished Encoding Rules
DES	Daten Encryption Standard
DF	Dedicated File
DI	Baud rate adjustment factor
DM	Display Message
DO	Datenobjekt
DS	Digital Signature
DSI	Digital Signature Input
DTBS	Data to be signed
EF	Elementary File
eGK	elektronische Gesundheitskarte
EHIC	European Health Insurance Card
ENC	Encryption
ES	Electronic Signature
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 Plattform
HB	Historical Bytes
HCI	Health Care Institution (Institution des Gesundheitswesens)
HP	Health Professional (Heilberufler)
HPA	Health Professional Application
HPC	Health Professional Card (Heilberufsausweis)
HPD	Health Professional related Data

Kürzel	Erläuterung
ICC	Integrated Circuit Card (Chipkarte)
ICCSN	ICC Serial Number (Chip-Seriennummer)
ICM	IC Manufacturer (Kartenhersteller)
ID	Identifier
IFSC	Information Field Size Card
IIN	Issuer Identification Number
INS	Instruction-Byte einer Kommando-APDU
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)
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
QES	Qualifizierte Elektronische Signatur
RA	Registration Authority (Registrierungsinstanz)
RAM	Random Access Memory
RC	Retry Counter (Fehlbedienungszähler)
RCA	Root CA

Kürzel	Erläuterung
RD	Referenzdaten
RF	Radio Frequency
RFC	Request für Comment
RFID	Radio Frequency Identification
RFU	Reserved for future use
RID	Registered Application Provider Identifier
RND	Random Number (Zufallszahl)
ROM	Read Only Memory
RPE	Remote PIN-Empfänger
RPS	Remote PIN-Sender
RSA	Algorithmus von Rivest, Shamir, Adleman
SAK	Signaturanwendungskomponente
SE	Security Environment (Sicherheitsumgebung)
SFID	Short EF Identifier
SIG	Signatur
SigG	Signaturgesetz
SigV	Signaturverordnung
SK	Secret Key
SM	Secure Messaging
SMA	Security Module Application
SMC	Security Module Card
SMD	Security Module Data
SMKT	Sicherheitsmodul Kartenterminal
SN	Seriennummer
SO	Security Officer (Administrator)
SSCD	Secure Signature Creation Device (Sichere Signaturerstellungseinheit)
SSEC	Security Status Evaluation Counter
SSEE	Sichere Signaturerstellungseinheit
SSL	Security Sockets Layer
SUK	Stapel- und Komfortsignatur
TLV	Tag Length Value
TC	Trusted Channel
TLS	Transport Layer Security
ZDA	Zertifizierungsdiensteanbieter

A2 - Glossar

Das Glossar 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 COS - Spezifikation der elektrischen Schnittstelle

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) in der aktuellen Fassung, siehe www.bundesnetzagentur.de
[DIN66291-1]	DIN V66291-1: 2000 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 1: Anwendungsschnittstelle
[EN14890-1]	EN 14890-1: 2008 Application Interface for smart cards used as secure signature creation devices, Part 1: Basic services
[EN1867]	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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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
[ISO7816-15]	ISO/IEC 7816-15: 2004 Identification cards - Integrated circuit cards - Part 15: Cryptographic information application
[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)
[PKCS#1]	RSA Laboratories (June 14, 2002): RSA Cryptography Standard v2.1 (earlier versions: V1.5: Nov. 1993, V2.0: July, 1998)
[Beschluss 190]	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 Level http://tools.ietf.org/html/rfc2119
[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
[TR-03114]	BSI: TR-0311, Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007, www.bsi.de/literat/tr/tr03114/BSI-TR-03114.pdf
[TR-03115]	BSI: TR-03115, Komfortsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007, www.bsi.de/literat/tr/tr03115/BSI-TR-03115.pdf
[TR-03116]	BSI: TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 3.0, 08.04.2009, www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf