Einführung der Gesundheitskarte

Spezifikation des elektronischen Heilberufsausweises

HBA-Objektsystem

Version:	3.8.1
Revision:	\main\rel_online\rel_ors1\133
Stand:	30.09.2015
Status:	freigegeben
Klassifizierung	öffentlich
Referenzierung:	[gemSpec_HBA_ObjSys]

Dokumentinformationen

Änderungen zur Vorversion

Folgende Änderungen gegenüber der Version 3.7.0 wurden durchgeführt:

1) gemErrata_R.1.4.1:
   a) D_994 wirkt sich aus auf Card-G2-A_3385, Card-G2-A_3386, Card-G2-A_3387
2) gemErrata_R1.4.2
   a) D_1000 wirkt sich aus auf Card-G2-A_3395
3) gemErrata_R1.4.3
   a) C_4812 wirkt sich aus auf Card-G2-A_2078, Card-G2-A_3327, Card-G2-A_3016, Card-G2-A_3290
4) gemErrata_R1.4.7
   a) C_4926 wirkt sich aus auf
      i) Nomenklatur in 1.5.1
      ii) Tab_HBA_ObjSys_007, Tab_HBA_ObjSys_008, Tab_HBA_ObjSys_010, Tab_HBA_ObjSys_011, Tab_HBA_ObjSys_013, Tab_HBA_ObjSys_014, Tab_HBA_ObjSys_017, Tab_HBA_ObjSys_019, Tab_HBA_ObjSys_020, Tab_HBA_ObjSys_021, Tab_HBA_ObjSys_024, Tab_HBA_ObjSys_032, Tab_HBA_ObjSys_034, Tab_HBA_ObjSys_037, Tab_HBA_ObjSys_038, Tab_HBA_ObjSys_040, Tab_HBA_ObjSys_042, Tab_HBA_ObjSys_046, Tab_HBA_ObjSys_049, Tab_HBA_ObjSys_055, Tab_HBA_ObjSys_056, Tab_HBA_ObjSys_059, Tab_HBA_ObjSys_060, Tab_HBA_ObjSys_061, Tab_HBA_ObjSys_062, Tab_HBA_ObjSys_063, Tab_HBA_ObjSys_145, Tab_HBA_ObjSys_146, Tab_HBA_ObjSys_147, Tab_HBA_ObjSys_148, Tab_HBA_ObjSys_149, Tab_HBA_ObjSys_065, Tab_HBA_ObjSys_068, Tab_HBA_ObjSys_069, Tab_HBA_ObjSys_070

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
3.0.0	19.09.12		freigegeben	gematik

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
3.1.0	30.01.13		Harmonisierung mit der Struktur der anderen ObjSys-Spezifikationen und Entfernen der N-Nummerierung	gematik
3.2.0 RC	23.10.13		Fehlerkorrekturen, Einfügen einer Anforderung zu *persistentPublicKeyList,* Attribut *shareable* wurde für alle Ordner und Dateien hinzugefügt, Ändern der Flaglist-Darstellung, Einfügen von EF.CardAccess, Kommentare eingearbeitet	gematik
3.3.0 RC	18.12.13		Aufnahme des Kommandos LIST PUBLIC KEY FÜR MF, Zuordnung der AFOs zu Initialisierung und Personalisierung, Überarbeitung der Struktur, Entfernen der Option „Lange Lebensdauer“, Modifizieren von EF.ATR, EF.DIR und EF.Version, Option „Testkarten“ aufgenommen, Änderungen in DF.QES: Keine Nutzung der CAN für Remote PIN und Stapelsignatur bei Nutzung der kontaktlosen Schnittstelle, Modifizieren von EF.GDO	gematik
3.4.0	21.02.14		Einfügen einer Liste offener Punkte, Expiration Date für Sicherheitsanker festgelegt, Einfügen Vorgaben für Inhalte von Dateien in CIA.Info, Einarbeiten Kommentare Iteration 2b	gematik
3.5.0	27.03.14		Einarbeitung Fehlerkorrektur Iteration 2b	gematik
3.6.0	06.06.14		Einarbeitung Änderungen Iteration 3	gematik
3.7.0	26.08.14		Richtigstellung in Tab_HBA_ObjSys_065, Einarbeitung weitere Änderungen Iteration 3 und Iteration 4	gematik
3.7.1	10.07.15		Folgende Errata eingearbeitet: R.1.4.1, R1.4.2, R1.4.3, R1.4.7	Technik / SPE
3.8.0	17.07.15		freigegeben	gematik
3.8.1	30.09.15		Änderung an Errata 1.4.7 bzgl. C_5027 übernommen.	gematik

Inhaltsverzeichnis

Dokumentinformationen **2**
Dokumentenhistorie **2**
Inhaltsverzeichnis **4**
1.1 Zielsetzung **7**
1.2 Zielgruppe **7**
1.3 Geltungsbereich **8**
1.4 Abgrenzung des Dokuments **8**
1.5 Methodik **8**
1.5.1 Nomenklatur 8
1.5.2 Verwendung von Schüsselworten 10
1.5.3 Komponentenspezifische Anforderungen 10
2 Optionen **12**
2.1 Kartenadministration **12**
3 Lebenszyklus von Karte und Applikation **13**
4 Anwendungsübergreifende Festlegungen **14**
4.1 Mindestanzahl logischer Kanäle **14**
4.2 Unterstützung optionaler Funktionspakete **14**
4.2.1 USB-Schnittstelle (optional) 14
4.2.2 Kontaktlose Schnittstelle (optional) 14
4.2.3 Kryptobox (optional) 15
4.3 Attributstabellen **16**
4.3.1 Attribute eines Ordners 16
4.3.2 Attribute einer Datei (EF) 17
4.4 Zugriffsregeln für besondere Kommandos **17**
4.5 Attributswerte und Personalisierung **18**
5 Spezifikation grundlegender Applikationen **19**
5.1 Attribute des Objektsystems **19**
5.1.1 ATR-Kodierung 20
5.2 Allgemeine Struktur **21**
5.3 Root, die Wurzelapplikation MF **21**
5.3.1 MF / EF.ATR 23
5.3.2 MF / EF.CardAccess(Option kontaktlose Schnittstelle) 24
5.3.3 MF / EF.DIR 25
5.3.4 MF / EF.GDO 27
5.3.5 MF / EF.Version2 28

5.3.6 MF / EF.C.CA_HPC.CS.R2048 ... 30
5.3.7 MF / EF.C.CA_HPC.CS.E256 ... 32
5.3.8 MF / EF.C.HPC.AUTR_CVC.R2048 ... 34
5.3.9 MF / EF.C.HPC.AUTR_CVC.E256 ... 36
5.3.10 MF / EF.C.HPC.AUTD_SUK_CVC.E256 ... 38
5.3.11 MF / PIN.CH ... 40
5.3.12 MF / PrK.HPC.AUTR_CVC.R2048 ... 42
5.3.13 MF / PrK.HPC.AUTR_CVC.E256 ... 44
5.3.14 MF / PrK.HPC.AUTD_SUK_CVC.E256 ... 46
5.3.15 Sicherheitsanker zum Import von CV-Zertifikaten ... 48
5.3.15.1 MF / PuK.RCA.CS.R2048 ... 48
5.3.15.2 MF / PuK.RCA.CS.E256 ... 50
5.3.16 Asymmetrische Kartenadministration ... 52
5.3.16.1 MF / PuK.RCA.ADMINCMS.CS.E256 ... 52
5.3.17 Symmetrische Kartenadministration ... 54
5.3.17.1 MF / SK.CMS.AES128 ... 55
5.3.17.2 MF / SK.CMS.AES256 ... 56
5.3.17.3 MF / SK.CUP.AES128 ... 58
5.3.17.4 MF / SK.CUP.AES256 ... 58
5.3.18 MF / SK.CAN (Option kontaktlose Schnittstelle) ... 59
5.3.19 Sicherheitsumgebungen auf MF-Ebene ... 61

5.4 Die Heilberufsanwendung DF.HPA ... 61
5.4.1 Dateistruktur und Dateiinhalt ... 61
5.4.2 MF / DF.HPA (Health Professional Application) ... 61
5.4.2.1 MF / DF.HPA / EF.HPD (Health Professional Data) ... 63
5.4.2.2 Sicherheitsumgebungen ... 64

5.5 Die Anwendung für die qualifizierte elektronische Signatur (DF.QES) ... 64
5.5.1 Dateistruktur und Dateiinhalt ... 64
5.5.2 MF / DF.QES (Qualified Electronic Signature Application) ... 65
5.5.2.1 MF / DF.QES / PrK.HP.QES.R2048 ... 66
5.5.2.2 MF / DF.QES / PIN.QES ... 69
5.5.2.3 MF / DF.QES / EF.SSEC ... 71
5.5.2.4 MF / DF.QES / EF.C.HP.QES.R2048 ... 74
5.5.2.5 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 ... 76

5.6 Die ESIGN-Anwendung (DF.ESIGN) ... 80
5.6.1 Dateistruktur und Dateiinhalt ... 80
5.6.2 MF / DF.ESIGN ... 80
5.6.2.1 MF / DF.ESIGN / PrK.HP.AUT.R2048 ... 82
5.6.2.2 MF / DF.ESIGN / PrK.HP.ENC.R2048 ... 84
5.6.2.3 MF / DF.ESIGN / EF.C.HP.AUT.R2048 ... 86
5.6.2.4 MF / DF.ESIGN / EF.C.HP.ENC.R2048 ... 88
5.6.3 Sicherheitsumgebungen ... 90

5.7 Die kryptographischen Informationsanwendungen ... 90
5.7.1 MF / DF.CIA.QES (Cryptographic Information Applications) ... 91
5.7.1.1 MF / DF.CIA.QES / EF.CIA.CIAInfo ... 92
5.7.1.2 MF / DF.CIA.QES / EF.OD ... 94
5.7.1.3 MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) ... 95
5.7.1.4 MF / DF.CIA.QES / EF.PrKD (Private Key Directory) ... 97
5.7.1.5 MF / DF.CIA.QES / EF.CD (Certificate Directory) ... 99
5.7.2 MF / DF.CIA.ESIGN (Cryptographic Information Applications) ... 101

5.7.2.1 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo 102
5.7.2.2 MF / DF.CIA.ESIGN / EF.OD 104
5.7.2.3 MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) 105
5.7.2.4 MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory) 107
5.7.2.5 MF / DF.CIA.ESIGN / EF.CD (Certificate Directory) 109

5.8 Die Organisationsspezifische Authentisierungsanwendung (DF.AUTO) . 111
5.8.1 Dateistruktur und Dateiinhalt 111
5.8.2 DF.AUTO (Organization-specific Authentication Application) 112
5.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R2048 113
5.8.2.2 MF / DF.AUTO / PIN.AUTO 115
5.8.2.3 MF / DF.AUTO / PIN.SO 118
5.8.2.4 MF / DF.AUTO / EF.C.HP.AUTO1.R2048 und MF / DF.AUTO / EF.C.HP.AUTO2.R2048 120
5.8.2.5 Sicherheitsumgebungen 123
5.8.2.6 Vorgaben für die Nutzung von DF.AUTO 123

5.9 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des HBA 124

Anhang A – Verzeichnisse 125

A1 - Abkürzungen 125

A2 - Glossar 128

A3 – Abbildungsverzeichnis 128

A4 – Tabellenverzeichnis 129

A5 - Referenzierte Dokumente 132
A5.1 – Dokumente der gematik 132
A5.2 – Weitere Dokumente 132

1 Einordnung des Dokumentes

1.1 Zielsetzung

Dieses Dokument spezifiziert die Objektstruktur des Heilberufsausweises (HBA) und beschreibt die Kartenschnittstelle zu dem 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, …).

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

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

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

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

Beispiele:

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

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

AUT_CMS		{SmMac(SK.CMS.AES128)
	OR	SmMac(SK.CMS.AES256)
	OR	SmMac(flagCMS.08)}
	AND	SmCmdEnc
	AND	SmRspEnc
AUT_CUP		{SmMac(SK.CUP.AES128)
	OR	SmMac(SK.CUP.AES256)

	OR AND AND	SmMac(flagCMS.10)} SmCmdEnc SmRspEnc
AUT_PACE	 AND AND	SmMac(SK.CAN) SmCmdEnc SmRspEnc

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

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

1.5.2 Verwendung von 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_Initialisierung	Instanz, welche eine Chipkarte im Rahmen der Initialisierung befüllt
K_Personalisierung	Instanz, welche eine Chipkarte im Rahmen der Produktion individualisiert
K_COS	Betriebssystem einer Smartcard

2 Optionen

Dieses Unterkapitel listet Funktionspakete auf, die für eine Zulassung eines HBA der Generation 2 nicht zwingend erforderlich sind.

2.1 Kartenadministration

In den Kapiteln 5.3.16 und 5.3.17 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen einem Kartenadministrationssystem (z.B. einem CMS) und einer Karte beschrieben, die bei der Ausgabe der Karte angelegt werden müssen.

⌦ **Card-G2-A_3005 Auswahl der Absicherung der Kartenadministration**

Wenn ein HBA Online administriert werden soll, MUSS ein Kartenherausgeber bei der Personalisierung Schlüssel für mindestens eines der beiden Verfahren

a. symmetrische Authentifizierung (SK.CMS und SK.CUP)
b. asymmetrische Authentifizierung (PuK.RCA.ADMIN.CS)

in die Karte einbringen und sicherstellen, dass das dazugehörende Kartenadministrationssystem (z.B. ein CMS) über die entsprechenden Schlüssel verfügt. ⌫

⌦ **Card-G2-A_3319 K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten**

Der HBA KANN als Testkarte ausgestaltet werden. Soweit in dieser Spezifikation Anforderungen an Testkarten von den Anforderungen an Produktivkarten abweichen, wird dies an der entsprechenden Stelle aufgeführt.⌫

3 Lebenszyklus von Karte und Applikation

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

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

Hinweis 1: Die in diesem Kapitel verwendeten Begriffe "Vorbereitungsphase" und "Nutzungsphase" werden in [gemSpec_COS#4] definiert.

4 Anwendungsübergreifende Festlegungen

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

- Unterstützung von mindestens vier logischen Kanälen.

4.1 Mindestanzahl logischer Kanäle

⌦ **Card-G2-A_2036 K_Initialisierung Anzahl logischer Kanäle**

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

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

b) 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. ⌫

4.2 Unterstützung optionaler Funktionspakete

4.2.1 USB-Schnittstelle (optional)

⌦ **Card-G2-A_3006 K_HBA: USB-Schnittstelle**

Falls ein HBA die Option_USB_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_USB_Schnittstelle implementiert hat.⌫

⌦ **Card-G2-A_2867 K_HBA: Vorhandensein einer USB-Schnittstelle**

Falls ein HBA die Option_USB_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_USB_Schnittstelle implementiert hat.
b) das die Option_USB_Schnittstelle nicht implementiert hat. ⌫

4.2.2 Kontaktlose Schnittstelle (optional)

⌦ **Card-G2-A_3007 K_HBA: Kontaktlose Schnittstelle**

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_kontaktlose_Schnittstelle implementiert hat.⌫

⌦ **Card-G2-A_2866 K_HBA: Vorhandensein einer kontaktlosen Schnittstelle**

Falls ein HBA die Option_kontaktlose_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_kontaktlose_Schnittstelle implementiert hat.
b) das die Option_kontaktlose_Schnittstelle nicht implementiert hat.⌫

⌦ **Card-G2-A_3009 K_HBA: Zusatzanforderungen für kontaktlose Schnittstelle**

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, dann MÜSSEN zusätzlich zu allen nicht gekennzeichneten Anforderungen auch alle Anforderungen erfüllt sein, die mit Option_kontaktlose_Schnittstelle gekennzeichnet sind.⌫

⌦ **Card-G2-A_3010 K_Initialisierung und K_Personalisierung: Kontaktlose Schnittstelle wird nicht genutzt**

Will der Kartenherausgeber eines HBA mit einem COS, das die Option_kontaktlose_Schnittstelle gemäß [gemSpec_COS] implementiert hat, die Nutzung dieser Schnittstelle verhindern, dann MUSS das Attribut *interfaceDependentAccessRules* aller Objekte so gesetzt sein, dass im Rahmen einer kontaktlosen Kommunikation die Zugriffsregelauswertung AccessRuleEvaluation (siehe [gemSpec_COS#10.4] stets den Wert „False“ liefert.⌫

⌦ **Card-G2-A_3011 K_Initialisierung: Kontaktlose Schnittstelle im COS nicht vorhanden**

Falls das COS für einen HBA die Option_kontaktlose_Schnittstelle nicht implementiert hat, MUSS der Teil des Attributes *interfaceDependentAccessRules*, welcher sich auf die kontaktlose Kommunikation bezieht, für alle Objekte irrelevant für die Zulassung sein.⌫

⌦ **Card-G2-A_3012 K_Personalisierung: Absicherung der kontaktlosen Schnittstelle**

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, MUSS die Kommunikation zwischen Karte und Kartenleser mit einer gegenseitigen Authentifizierung und Aufbau eines sicheren Kommunikationskanals abgesichert werden. Hierfür MUSS das PACE-Protokoll genutzt werden.⌫

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

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, MUSS das Attribut *can* des Objektes SK.CAN mit der Nummer übereinstimmen, die auf dem HBA aufgedruckt ist.⌫

⌦ **Card-G2-A_3277 K_Personalisierung und K_Initialisierung: Konformität kontaktlose Schnittstelle**

Ein HBA mit kontaktloser Schnittstelle MUSS in seiner endgültigen Konfiguration (einschließlich Kartenkörper und Antenne) bezüglich der elektrischen Eigenschaften dieser kontaktlosen Schnittstelle konform zu [ISO-IEC 14443] und [ISO/IEC FCD 10373-6] sein.⌫

4.2.3 Kryptobox (optional)

⌦ **Card-G2-A_3014 K_HBA: Vorhandensein Kryptobox**

Für einen HBA KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_Kryptobox implementiert hat.
b) das die Option_Kryptobox nicht implementiert hat.⌫

4.3 Attributstabellen

⌦ **Card-G2-A_2032 K_Initialisierung: Änderung von Zugriffsregeln**

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

⌦ **Card-G2-A_2329 K_Initialisierung: Verhalten der Objekte, kein konkretes SE genannt**

Falls für die SE abhängigen Attribute eines Objektes kein konkretes SE genannt ist, dann MUSS sich dieses Objekt in SE#1 wie angegeben verwenden lassen. ⌫

⌦ **Card-G2-A_3182 K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, kein konkretes SE genannt**

Falls für die SE abhängigen Attribute eines Objektes kein konkretes SE genannt ist, dann KANN dieses Objekt in SE verwendbar sein, die verschieden sind von SE#1.⌫

⌦ **Card-G2-A_3183 K_Initialisierung: Eigenschaften der Objekte in anderen SEs, kein konkretes SE genannt**

Falls für die SE abhängigen Attribute eines Objektes kein konkretes SE genannt ist und dieses Objekt in einem von SE#1 verschiedenen SE verwendbar ist, dann MUSS es dort dieselben Eigenschaften wie in SE#1 besitzen. ⌫

⌦ **Card-G2-A_3184 K_Initialisierung: Verhalten der Objekte, konkretes SE genannt**

Falls für die SE abhängigen Attribute eines Objektes ein konkretes SE genannt ist, dann MUSS sich dieses Objekt dort wie angegeben verwenden lassen. ⌫

⌦ **Card-G2-A_3185 K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, konkretes SE genannt**

Falls für die SE abhängigen Attribute eines Objektes ein konkretes SE genannt ist, dann KANN dieses Objekt in SE verwendbar sein, die nicht konkret genannt sind. ⌫

⌦ **Card-G2-A_3186 K_Initialisierung: Eigenschaften der Objekte in anderen SEs, konkretes SE genannt**

Falls für die SE abhängigen Attribute eines Objektes ein konkretes SE genannt ist und dieses Objekt ist in einem nicht konkret angegebenen SE verwendbar, dann MUSS es dort dieselben Eigenschaften wie in einem konkret angegebenen besitzen.⌫

4.3.1 Attribute eines Ordners

⌦ **Card-G2-A_2033 K_Initialisierung: Ordnerattribute**

Enthält eine Tabelle mit Ordnerattributen

a) keinen *applicationIdentifier* (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.

b) einen oder mehrere AID, dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.

c) keinen *fileIdentifier* (FID),

1. so DARF dieser Ordner 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. ⌫

4.3.2 Attribute einer Datei (EF)

⌦ **Card-G2-A_2034 K_Initialisierung: Dateiattribute**

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

⌦ **Card-G2-A_2673 K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile"**

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

4.4 Zugriffsregeln für besondere Kommandos

⌦ **Card-G2-A_2035 K_Initialisierung: Zugriffsregeln für besondere Kommandos**

Für Kommandos, für die eine Zugriffsregelauswertung gemäß [gemSpec_COS] optional ist, werden nicht in den Attributstabellen, sondern zentral in dieser Anforderung die Zugriffsbedingungen festgelegt:

a) Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.
b) Falls der HBA die Option_kontaktlose_Schnittstelle unterstützt, dann MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.
c) Falls ein Kartenherausgeber die Nutzung einer im COS vorhandenen kontaktlosen Schnittstelle unterbinden will, dann MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT für die kontaktlose Schnittstelle herstellerspezifisch stets entweder ALWAYS oder NEVER sein.⌫

4.5 Attributswerte und Personalisierung

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

Beispielsweise ist es denkbar, dass für die Datei EF.GDO das Attribut lifeCycleStatus nach der Initialisierung auf dem in [gemSpec_COS] nicht normativ geforderten Wert „Initialize“ steht und für diesen Wert die Zugriffsregeln etwa ein Update Binary Kommando erlauben. In diesem Fall wiche nicht nur der Wert des Attributes lifeCycleStatus, sondern auch der des Attributes interfaceDependentAccessRules von den Vorgaben dieses Dokumentes ab. Nach Abschluss der Personalisierung wäre dann der Wert des Attributes lifeCycleStatus bei korrekter Personalisierung spezifikationskonform auf dem Wert „Operational state (activated)“ aber in interfaceDependentAccessRules fände sich für den Zustand „Initialize“ immer noch „Update Binary“. Im Rahmen einer Sicherheitsbetrachtung wäre diese Abweichung als unkritisch einzustufen, wenn sichergestellt ist, dass der Zustand „Initialize“ unerreichbar ist.

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

Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:

⌦ Card-G2-A_3325 K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung

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

5 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.

5.1 Attribute des Objektsystems

Das Objektsystem [gemSpec_COS] enthält folgende Attribute:

⌦ **Card-G2-A_2039 K_Initialisierung: Wert des Attributes *root***

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

⌦ **Card-G2-A_2040 K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset**

Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A_2043, Card-G2-A_2044, Card-G2-A_2045 und Card-G2-A_3015 entsprechen. ⌫

⌦ **Card-G2-A_2041 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 K_Initialisierung: Inhalt persistentPublicKeyList**

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

⌦ **Card-G2-A_3181 K_Initialisierung: Größe persistentPublicKeyList**

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

⌦ **Card-G2-A_3266 K_Initialisierung: Wert von *pointInTime***

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

⌦ **Card-G2-A_3395 K_Personalisierung: personalisierter Wert von *pointInTime***

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

5.1.1 ATR-Kodierung

⌦ **Card-G2-A_2043 K_Personalisierung und K_Initialisierung: ATR-Kodierung**

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

Tabelle 2: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten)

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

⌫

⌦ **Card-G2-A_2044 K_Personalisierung und K_Initialisierung: TC1 Byte im ATR**

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

⌦ **Card-G2-A_3015 K_Personalisierung und K_Initialisierung: Historical Bytes im ATR**

Das Attribut answerToReset SOLL keine Historical Bytes enthalten. ⌫

⌦ **Card-G2-A_2045 K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes**

Falls answerToReset Historical Bytes enthält, dann MÜSSEN
a. diese gemäß [ISO7816-4] kodiert sein.
b. die dort getroffenen Angaben konsistent sein zu Angaben im EF.ATR.⌫

5.2 Allgemeine Struktur

Card-G2-A_2046 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.

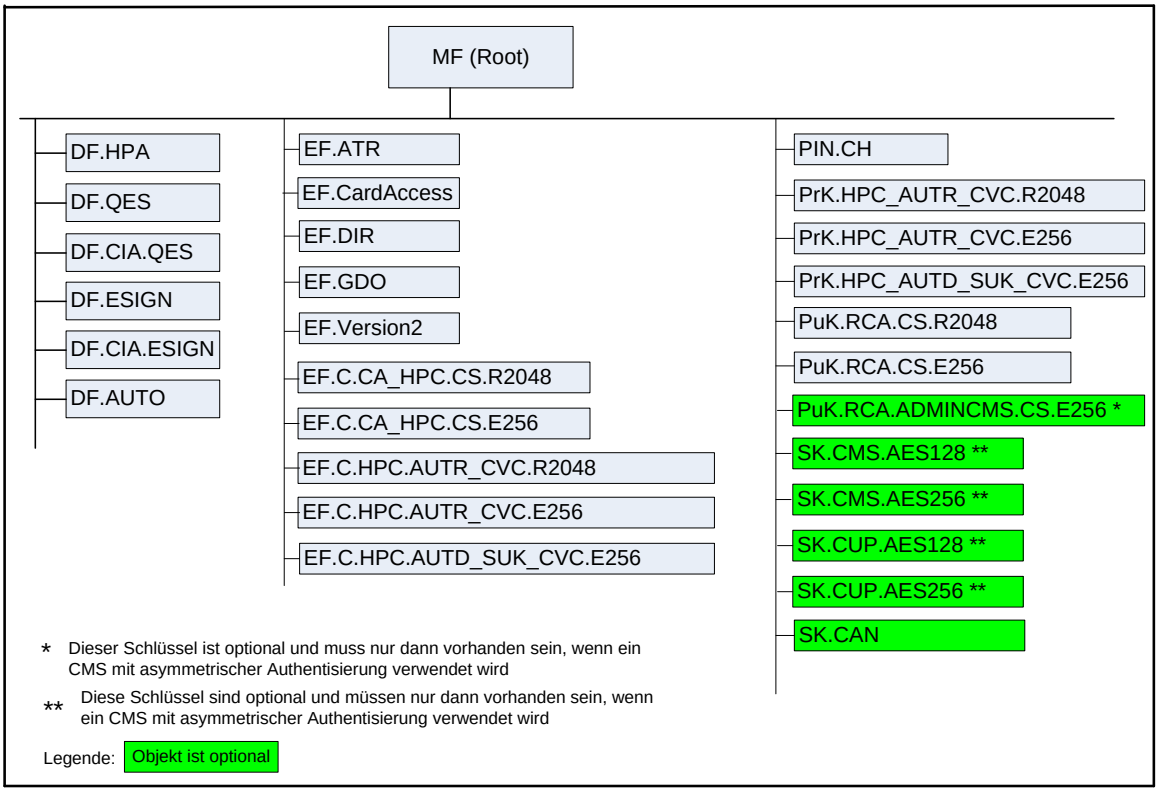

Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA

5.3 Root, die Wurzelapplikation MF

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

Card-G2-A_2047 K_Initialisierung: Initialisierte Attribute von MF

MF MUSS die in Tab_HBA_ObjSys_004 dargestellten Werte besitzen.

Tabelle 3: Tab_HBA_ObjSys_004 Initialisierte Attribute von MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D27600014601’	

fileIdentifier	'3F 00'	falls vorhanden
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
FINGERPRINT	Wildcard	
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
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
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
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, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

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

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

5.3.1 MF / EF.ATR

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

⌦ **Card-G2-A_2048 K_Initialisierung: Initialisierte Attribute von MF / EF.ATR**

EF.ATR MUSS die in Tab_HBA_ObjSys_005 dargestellten Werte besitzen.

Tabelle 4: Tab_HBA_ObjSys_005 Initialisierte Attribute von MF / EF.ATR

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 01'	siehe Hinweis 6:
shortFileIdentifier	'1D'= 29	
numberOfOctet	herstellerspezifisch	
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	siehe unten
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY WRITE BINARY	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 WRITE BINARY	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, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

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

⌦ **Card-G2-A_3278 K_Initialisierung: Initialisiertes Attribut *numberOfOctet* von MF / EF.ATR**

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

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

5.3.2 MF / EF.CardAccess(Option kontaktlose Schnittstelle)

EF.CardAccess wird für das PACE-Protokoll bei Nutzung der kontaktlosen Schnittstelle benötigt.

⌦ **Card-G2-A_3199 K_Initialisierung: Initialisierte Attribute von MF / EF.CardAccess**

Falls die kontaktlose Schnittstelle für den HBA genutzt wird, MUSS EF.CardAccess vorhanden sein und die in Tab_HBA_ObjSys_083 dargestellten Attribute besitzen.

Tabelle 5: Tab_HBA_ObjSys_083 Initialisierte Attribute von MF / EF.CardAccess

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'01 1C'	siehe Hinweis 6:
shortFileIdentifier	'1C'= 28	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	False	
flagChecksum	True	
numberOfOctet	passend zum Inhalt	
positionLogicalEndOfFile	passend zum Inhalt	
shareable	True	
body	passend zu den Attributen von SK.CAN gemäß [TR-03110-3]	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos		
alle	herstellerspezifisch	

⌫

5.3.3 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 K_Initialisierung: Initialisierte Attribute von MF / EF.DIR**

EF.DIR MUSS die in Tab_HBA_ObjSys_007 dargestellten Werte besitzen.

Tabelle 6: Tab_HBA_ObjSys_007 Initialisierte 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	'00 BE' Oktett = 190 Oktett	
maxNumRecords	10 Rekord	
maxRecordLength	32 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
recordList		
Rekord 1	'61- 08- (4F 06 D27600014601)'	AID.MF
Rekord 2	'61- 08- (4F 06 D27600014602)'	AID.HPA
Rekord 3	'61- 08- (4F 06 D27600006601)'	AID.QES
Rekord 4	'61- 0D- (4F 0B E828BD080F D27600006601)'	AID.CIA.QES
Rekord 5	'61- 0C- (4F 0A A000000167 455349474E)'	AID.ESIGN
Rekord 6	'61- 11- (4F 0F E828BD080F A000000167	AID.CIA ESIGN

Rekord 7 Rekord 8 …	455349474E)' 61- 08- (4F 06 D27600014603)' nicht vorhanden, MUSS mittels APPEND RECORD angelegt werden	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 RECORD	AUT_CMS	siehe Hinweis 8:
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT_CMS	siehe Hinweis 8:
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 RECORD	AUT_CMS	siehe Hinweis 9:
READ RECORD SEARCH RECORD	AUT_PACE OR AUT_CMS	
UPDATE RECORD	AUT_CMS	siehe Hinweis 9:
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 variablen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, DELETE RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, TERMINATE, UPDATE RECORD, WRITE RECORD.

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

Hinweis 9: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

5.3.4 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 K_Initialisierung: Initialisierte Attribute von MF / EF.GDO**

EF.GDO MUSS die in Tab_HBA_ObjSys_008 dargestellten Werte besitzen.

Tabelle 7: Tab_HBA_ObjSys_008 Initialisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 02’	
shortFileIdentifier	‘02’= 2	
numberOfOctet	‘00 0C’ Oktett = 12 Oktett	
positionLogicalEndOfFile	Wildcard	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Wildcard	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_2058 K_Personalisierung: Personalisiertes Attribut von EF.GDO**

Bei der Personalisierung von EF.GDO MÜSSEN die in Tab_HBA_ObjSys_151 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 8: Tab_HBA_ObjSys_151 Personalisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00 0C' Oktett = 12 Oktett	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	

⌫

5.3.5 MF / EF.Version2

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

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

Die konkrete Befüllung ist in [gemSpec_Karten_Fach_TIP] beschrieben.

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

⌦ Card-G2-A_2059 K_Initialisierung: Attribute von MF / EF.Version2

EF.Version2 MUSS die in Tab_HBA_ObjSys_009 dargestellten Werte besitzen.

Tabelle 9: Tab_HBA_ObjSys_009 Initialisierte Attribute von MF / EF.Version2

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 11’	
shortFileIdentifier	‘11’= 17	
numberOfOctet	‘00 3C’ Oktett = 60 Oktett	
positionLogicalEndOfFile	passend zum Inhalt	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
UPDATE BINARY SET LOGICAL EOF	AUT_CMS	siehe Hinweis 12:
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	

UPDATE BINARY SET LOGICAL EOF	AUT_CMS	siehe Hinweis 12:
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 11: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 12: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

5.3.6 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 K_Initialisierung: Initialisierte 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 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 04'	
shortFileIdentifier	'04'= 4	
numberOfOctet	'01 4B' Oktett = 331 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	kein Inhalt	wird personalisiert

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 14:
READ BINARY	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
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 14:
READ BINARY	AUT_PACE	
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 transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 14: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3281 K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_HPC.CS.R2048**

Bei der Personalisierung von EF.C.CA_HPC.CS.R2048 MÜSSEN die in Tab_HBA_ObjSys_089 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 11: Tab_HBA_ObjSys_089 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'01 4B' Oktett = 331 Oktett	
body	C.CA_HPC.CS.R2048 gemäß [gemSpec_PKI]	
body Option_Erstellung_von_Testkarten	C.CA_HPC.CS.R2048 gemäß [gemSpec_PKI] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]

⌫

5.3.7 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 K_Initialisierung: Initialisierte 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 12: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 07'	
shortFileIdentifier	'07'= 7	
numberOfOctet	'00 DC' Oktett = 220 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 14:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 14:

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 OR AUT_CUP	siehe Hinweis 14:
READ BINARY	AUT_PACE OR AUT_CMS OR AUT_CUP	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 14:
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_3282 K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256**

Bei der Personalisierung von EF.C.CA_HPC.CS.E256 MÜSSEN die in Tab_HBA_ObjSys_090 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 13: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	‘00 DC’ Oktett = 220 Oktett	
body	C.CA_HPC.CS.E256 gemäß [gemSpec_PKI#6.7.1]	siehe [gemSpec_COS]

body Option_Erstellung_von_Testkarten	C.CA_HPC.CS.E256 gemäß [gemSpec_PKI#6.7.1] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]

⌫

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

EF.C.HPC.AUTR_CVC.R2048 enthält das CV-Zertifikat des HBA für die Kryptographie mit RSA für rollenbasierte C2C-Authentisierung zwischen HBA 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 5.3.12 definiert.

⌦ **Card-G2-A_2063 K_Initialisierung: Initialisierte 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 14: Tab_HBA_ObjSys_013 Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 03’	
shortFileIdentifier	‘03’= 3	
numberOfOctet	‘01 55’ Oktett = 341 Oktett	
positionLogicalEndOfFile	‘0’	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 16:
READ BINARY	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
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 16:
READ BINARY	AUT_PACE	
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, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 16: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3385 K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTR_CVC.R2048**

Für die CHR in diesem Zertifikat MUSS CHR = '00 10' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2058].⌫

⌦ **Card-G2-A_3283 K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048**

Bei der Personalisierung von EF.C.HPC.AUTR_CVC.R2048 MÜSSEN die in Tab_HBA_ObjSys_092 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 15: Tab_HBA_ObjSys_092 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'01 55' Oktett = 341 Oktett	
body	C.HPC.AUTR_CVC.R2048 passend zu dem privaten Schlüssel in PrK.HPC.AUTR_CVC.R2048 [gemSpec_PKI]	siehe [gemSpec_COS]

⌫

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

EF.C.HPC.AUTR_CVC.E256 enthält das CV-Zertifikat des HBA für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen HBA 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 5.3.13 definiert.

⌦ **Card-G2-A_2064 K_Initialisierung: Initialisierte 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 16: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 06’	
shortFileIdentifier	‘06’= 6	
numberOfOctet	‘00 DE’ Oktett = 222 Oktett	
positionLogicalEndOfFile	‘0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 16:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	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 OR AUT_CUP	siehe Hinweis 16:
READ BINARY	AUT_PACE OR AUT_CMS OR AUT_CUP	
UPDATE BINARY	AUT_CMS OR AUT_CUP	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, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 18: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3386 K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTR_CVC.E256**

Für die CHR in diesem Zertifikat MUSS CHR = '00 06' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2058].⌫

⌦ **Card-G2-A_3284 K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256**

Bei der Personalisierung von EF.C.HPC.AUTR_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_093 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 17: Tab_HBA_ObjSys_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00 DE' Oktett = 222 Oktett	
body	C.HPC.AUTR_CVC.E256 gemäß [gemSpec_PKI]	

⌫

5.3.10 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 5.3.14 definiert.

⌦ **Card-G2-A_2067 K_Initialisierung: Initialisierte 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 18: Tab_HBA_ObjSys_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 09’	
shortFileIdentifier	‘09’= 9	
numberOfOctet	‘00 DE’ Oktett = 222 Oktett	
positionLogicalEndOfFile	‘0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 16:
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	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 OR AUT_CUP	siehe Hinweis 16:
READ BINARY	AUT_PACE OR AUT_CMS OR AUT_CUP	
UPDATE BINARY	AUT_CMS OR AUT_CUP	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, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 20: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3387 K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTD_SUK_CVC.E256**

Für die CHR in diesem Zertifikat MUSS CHR = '00 09' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2058].⌫

⌦ **Card-G2-A_3285 K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256**

Bei der Personalisierung von EF.C.HPC.AUTD_SUK_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_095 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 19: Tab_HBA_ObjSys_095 Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00 DE' Oktett = 222 Oktett	
body	C.HPC.AUTD_SUK_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HPC.AUTD_SUK_CVC.E256	

⌫

5.3.11 MF / PIN.CH

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

⌦ **Card-G2-A_2069 K_Initialisierung: Initialisierte Attribute von MF / PIN.CH**

PIN.CH MUSS die in Tab_HBA_ObjSys_019 dargestellten Werte besitzen.

Tabelle 20: Tab_HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	'01' = 1	
secret	undefiniert	wird personalisiert
minimumLength	6	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	Transport-PIN	
flagEnabled	True	
startSsec	unendlich	
PUK	undefiniert	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 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	AUT_PACE	
GET PIN STATUS	AUT_PACE	
RESET RC. P1 aus der Menge {0, 1}	AUT_PACE	
VERIFY	AUT_PACE	
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 Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

⌦ Card-G2-A_3286 K_Personalisierung: Personalisierte Attribute von MF / PIN.CH

Bei der Personalisierung von PIN.CH MÜSSEN die in Tab_HBA_ObjSys_097 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 21: Tab_HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH

Attribute	Wert	Bemerkung
secret	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
transportStatus	Transport-PIN	wird gegebenenfalls

		personalisiert, siehe Hinweis 22:
PUK	PUK-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert

⌫

Hinweis 22: Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

⌦ **Card-G2-A_2070 K_Personalisierung: Länge der PUK für des HBA**

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

5.3.12 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 HBA/eGK. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTR_CVC.R2048 ist in C.HPC.AUTR_CVC.R20485.5.2.4 (siehe Kapitel 5.3.8) enthalten.

⌦ **Card-G2-A_2071 K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048**

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

Tabelle 22: Tab_HBA_ObjSys_020 Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	‘10’ = 16	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge {rsaRoleAuthentication,	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	

INTERNAL AUTHENTICATE	PWD(PIN.CH)	
DELETE	AUT_CMS OR AUT_CUP	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	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	
INTERNAL AUTHENTICATE	AUT_PACE AND PWD(PIN.CH)	
DELETE	AUT_CMS OR AUT_CUP	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	NEVER	

⌫

Hinweis 23: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 24: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3287 K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048**

Bei der Personalisierung von PrK.HPC.AUTR_CVC.R2048 MÜSSEN die in Tab_HBA_ObjSys_098 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab_HBA_ObjSys_098 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

⌫

5.3.13 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 HBA/eGK und HBA/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 5.3.9) enthalten.

⌦ **Card-G2-A_2072 K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256**

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

Tabelle 24: Tab_HBA_ObjSys_021 Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	‘06’ = 6	
privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge {elcRoleAuthentication}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
INTERNAL AUTHENTICATE	PWD(PIN.CH)	

DELETE	AUT_CMS OR AUT_CUP	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	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	siehe Hinweis 26:
INTERNAL AUTHENTICATE	AUT_PACE AND PWD(PIN.CH)	
DELETE	AUT_CMS OR AUT_CUP	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	NEVER	

⌫

Hinweis 25: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 26: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

⌦ **Card-G2-A_3288 K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256**

Bei der Personalisierung von PrK.HPC.AUTR_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_099 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 25: Tab_HBA_ObjSys_099 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
privateElcKey	keyData = Wildcard	

⌫

5.3.14 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 HBA/SMC-B und HBA/gSMC-K für die Übertragung von PIN-Daten und der DTBS zum HBA. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTD_SUK_CVC.E256 ist in C.HPC.AUTD_SUK_CVC.E256 (siehe Kapitel 5.3.10) enthalten.

⌦ **Card-G2-A_2075 K_Initialisierung: Initialisierte 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 26: Tab_HBA_ObjSys_024 Initialisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	‘09’ = 9	
privateElcKey	domainparameter = brainpoolP256r1	
privateElcKey	keyData = AttributNotSet	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	Ein Wert aus der Menge {elcSessionkey4SM, elcAsynchronAdmin}	
lifeCycleStatus	„Operational state (activated)“	
numberScenarion	0	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	

DELETE	AUT_CMS OR AUT_CUP	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	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	
General Authenticate	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	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	NEVER	

⌫

Hinweis 27: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 28: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

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.

⌦ **Card-G2-A_3289 K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256**

Bei der Personalisierung von PrK.HPC.AUTD_SUK_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_101 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 27: Tab_HBA_ObjSys_101 Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
privateElcKey	keyData = Wildcard	

⌫

5.3.15 Sicherheitsanker zum Import von CV-Zertifikaten

In diesem Kapitel werden öffentliche Signaturprüfobjekte behandelt, die an der Wurzel eines PKI Baumes für CV-Zertifikate stehen. Diese werden auch Sicherheitsanker genannt und dienen dem Import von CV-Zertifikaten der zweiten Ebene. Derzeit ist jeweils ein Sicherheitsanker vorhanden,

a) zwecks Abwärtskompatibilität zur Generation 1 Infrastruktur (PuK.RCA.CS.R2048),

b) zur unmittelbaren Ablösung der Generation 1 Algorithmen (PuK.RCA.CS.E256)

5.3.15.1 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 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.R2048**

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

Tabelle 28: Tab_HBA_ObjSys_026 Initialisierte 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)	
publicKey	Öffentlicher Schlüssel mit Moduluslänge 2048 Bit gemäß [gemSpec_PKI#6.4.1.6] und gemäß [gemSpec_CVC_TSP#4.5]	
publicKey Option_Erstellung _von_Testkarten	Öffentlicher Schlüssel mit Moduluslänge 2048 Bit gemäß [gemSpec_PKI#6.4.1.6] aus Test-CVC-Root	wird personalisiert gemäß [gemSpec_TK#3.1.2]
oid	sigS_ISO9796-2Withrsa_sha256 '2B240304020204' = {1.3.36.3.4.2.2.4}	
lifeCycleStatus	„Operational state (activated)"	
accessRulesPublicSignatureVerificationObject.	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE → AUT_CMS OR AUT_CUP	

contact	PSO Verify Certificate → ALWAYS	
accessRulesPublic SignatureVerification Object. contactless		
accessRulesPublic AuthenticationObject contact	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE → AUT_CMS OR AUT_CUP EXTERNAL AUTHENTICATE → ALWAYS INTERNAL AUTHENTICATE → ALWAYS	
accessRulesPublicAuthenticationObject. contactless		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	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	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	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	NEVER	

⌫

Hinweis 29: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, PSO Verify Certificate, TERMINATE

Hinweis 30: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

⌦ **Card-G2-A_3326 K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten**

Bei der Personalisierung von PuK.RCA.CS.R2048 für Testkarten MÜSSEN die in Tab_HBA_ObjSys_152 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 29: Tab_HBA_ObjSys_152 Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten

Attribute	Wert	Bemerkung
publicKey	Öffentlicher Schlüssel mit Moduluslänge 2048 Bit	

⌫

5.3.15.2 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 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**

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

Tabelle 30: Tab_HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Signaturprüfobjekt	
Für Echtkarten MÜSSEN die vier folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die vier folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes)	
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß [gemSpec_CVC_Root#5.4.2]	
CHAT	OID_{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 07C3'	siehe Hinweis 31:
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP[gemSpec_CVC_TSP#4.5]	
Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		

oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
lifeCycleStatus	„Operational state (activated)"	
accessRulesPublicSignatureVerificationObject	Für alle Interfacearten und alle Werte von lifeCycleStatus gilt: DELETE --> AUT_CMS OR AUT_CUP PSO Verify Certificate --> ALWAYS	
accessRulesPublicAuthenticationObject	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE --> AUT_CMS OR AUT_CUP GENERAL AUTHENTICATE --> ALWAYS EXTERNAL AUTHENTICATE --> ALWAYS	
Zugriffsregeln		
accessRules	identisch zu PuK.RCA.CS.R2048	

⌫

Hinweis 31: Während gemäß den Tabellen in [gemSpec_PKI] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ‚0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ‚1' gesetzt.

⌦ **Card-G2-A_3327 K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten**

Bei der Personalisierung von PuK.RCA.CS.E256 für Testkarten MÜSSEN die in Tab_HBA_ObjSys_153 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Wenn die restlichen Attribute von PuK.RCA.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_HBA_ObjSys_027 personalisiert werden.

Tabelle 31: Tab_HBA_ObjSys_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Attribute	Wert	Bemerkung
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-CVC-CA	personalisieren gemäß [gemSpec_TK#3.1.2]
keyIdentifier	E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels	
CHAT	• OID_{flags} = oid_cvc_fl_ti • flagList = 'FF 0084 2006 07C3'	
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels	

⌫

5.3.16 Asymmetrische Kartenadministration

Die hier beschriebene Variante der Administration des HBA betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration des HBA.

Die Administration eines HBA erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels asymmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels symmetrischer Verfahren werden in 5.3.17 beschrieben.

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

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

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

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

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

⌦ **Card-G2-A_3016 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab_HBA_ObjSys_082 dargestellten Attribute besitzen.

Tabelle 32: Tab_HBA_ObjSys_082 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches Signaturprüfobjekt, ELC 256	
Für Echtkarten MÜSSEN die beiden folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
CHAT	▪ OID_{flags} = oid_cvc_fl_cms ▪ flagList = 'FF BFFF FFFF FFFF'	siehe Hinweis 33:
expirationDate	Identisch zu „expirationDate" von PuK.RCS.CS.E256	

Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	'0000 0000 0000 0013'	
lifeCycleStatus	„Operational state (activated)"	
publicKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Domainparameter = brainpoolP256r1	wird personalisiert
oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
accessRulesPublicSignatureVerificationObject.contact	Für alle Life Cycle State und in SE#1 gilt: DELETE --> AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublicSignatureVerificationObject.contactless		
accessRulesPublicAuthenticationObject.contact	Für alle Life Cycle State und in SE#1 gilt: DELETE --> AUT_CMS OR AUT_CUP GENERAL AUTHENTICATE → ALWAYS	
accessRulesPublicAuthenticationObject.contactless		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
PSO Verify Certificate	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
alle	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
PSO Verify Certificate	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
alle	NEVER	

⌫

Hinweis 32: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, PSO Verify Certificate, TERMINATE

Hinweis 33: Während gemäß den Tabellen in [gemSpec_COS]#H.4] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ‚0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ‚1' gesetzt.

⌦ **Card-G2-A_3290 K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 die in Tab_HBA_ObjSys_103 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Wenn die restlichen Attribute von PuK.RCA.ADMINCMS.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_HBA_ObjSys_082 personalisiert werden.

Tabelle 33: Tab_HBA_ObjSys_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
publicKey	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3]	
publicKey Option_Erstellung_von_Testkarten	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-Admin-CVC-Root	
CHAT	▪ OID_{flags} = oid_cvc_fl_cms ▪ flagList = 'FF BFFF FFFF FFFF'	
expirationDate Option_Erstellung_von_Testkarten	Identisch zu „expirationDate" des personalisierten PuK.RCA.CS.E256	

⌫

5.3.17 Symmetrische Kartenadministration

Die hier beschriebene Variante der Administration des HBA betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration des HBA.

Die Administration eines HBA erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels symmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels asymmetrischer Verfahren werden in 5.3.16 beschrieben.

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

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

Die Objekte müssen bei der Initialsierung angelegt werden. Bei der Personalisierung sind nur die Schlüssel zu personalisieren, die tatsächlich benötigt werden.

5.3.17.1 MF / SK.CMS.AES128

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

⌦ **Card-G2-A_2080 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128**

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

Tabelle 34: Tab_HBA_ObjSys_029 Initialisierte Attribute von MF / SK.CMS.AES128

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'14' = 20	
encKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)"	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
MUTUAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	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
alle	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
MUTUAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	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
alle	NEVER	

⌫

Hinweis 34: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GET SECURITY STATUS KEY, INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE, TERMINATE.

Hinweis 35: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

⌦ **Card-G2-A_3291 K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES128 die in Tab_HBA_ObjSys_104 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 35: Tab_HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128

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

⌫

5.3.17.2 MF / SK.CMS.AES256

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

⌦ **Card-G2-A_2081 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256**

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

Tabelle 36: Tab_HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	'18' = 22	
encKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)"	
accessRuleSession keys	irrelevant	
Zugriffsregeln		
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	

⌫

⌦ **Card-G2-A_3292 K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES256 die in Tab_HBA_ObjSys_105 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 37: Tab_HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256

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

⌫

5.3.17.3 MF / SK.CUP.AES128

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

⌦ **Card-G2-A_3293 K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128**

SK.CUP.AES128 MUSS die in Tab_HBA_ObjSys_147 dargestellten Initialisierten Attribute besitzen.

Tabelle 38: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128

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

⌫

⌦ **Card-G2-A_3294 K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CUP.AES128 die in Tab_HBA_ObjSys_148 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 39: Tab_HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES128

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

⌫

5.3.17.4 MF / SK.CUP.AES256

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

⌦ **Card-G2-A_3295 K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256**

SK.CUP.AES256 MUSS die in Tab_HBA_ObjSys_149 dargestellten Initialisierten Attribute besitzen.

Tabelle 40: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256

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

⌫

⌦ **Card-G2-A_3296 K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CUP.AES256 die in Tab_HBA_ObjSys_150 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 41: Tab_HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES256

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

⌫

5.3.18 MF / SK.CAN (Option kontaktlose Schnittstelle)

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

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

Wird die kontaktlose Schnittstelle genutzt, dann MUSS SK.CAN vorhanden sein und die in Tab_HBA_ObjSys_076 dargestellten Attribute besitzen.

Tabelle 42: Tab_HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN

Attribute	Wert	Bemerkung
Objekttyp	symmetrisches Kartenverbindungsobjekt	
keyIdentifier	'02' = 2	
lifeCycleStatus	„Operational state (activated)“	
Can	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für ein Schlüsselobjekt SK.CAN	
algorithmIdentifier	id-PACE-ECDH-GM-AES-CBC-CMAC-128	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
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	
DELETE	AUT_CMS OR AUT_CUP	
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 36: Kommandos, die gemäß [gemSpec_COS] mit symmetrischen Kartenverbindungsobjekten arbeiten, sind: ACTIVATE; DEACTIVATE; DELETE, GENERAL AUTHENTICATE, TERMINATE.

⌦ **Card-G2-A_3297 K_Personalisierung: Personalisierte Attribute von MF / SK.CAN**

Bei der Personalisierung von SK.CAN MÜSSEN die in Tab_HBA_ObjSys_106 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 43: Tab_HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN

Attribute	**Wert**	**Bemerkung**
can	SK.CAN gemäß [gemSpec_CAN_TI]	siehe [Card-G2-A_2869]

⌫

⌦ **Card-G2-A_2869 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 sechsstellige Ziffernfolge gemäß [gemSpec_CAN_TI] setzen⌫

5.3.19 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.

5.4 Die Heilberufsanwendung DF.HPA

5.4.1 Dateistruktur und Dateiinhalt

Die Abbildung Abb_HBA_ObjSys_002 zeigt die Dateistruktur von DF.HPA.

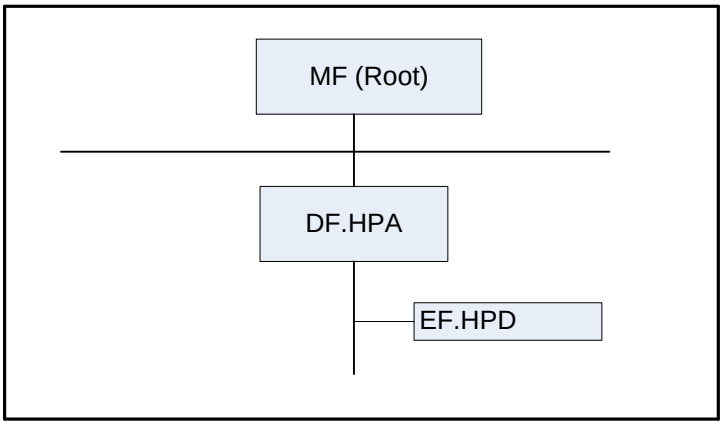

Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA

5.4.2 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 K_Initialisierung: Initialisierte Attribute von MF / DF.HPA**

DF.HPA MUSS die in Tab_HBA_ObjSys_031 dargestellten Werte besitzen.

Tabelle 44: Tab_HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D27600014602’	
fileIdentifier	–	

lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD *APPLICATION* (nach der HBA-Ausgabe)	AUT_CMS	
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
GET RANDOM	ALWAYS	
LOAD APPLICATION (nach der HBA-Ausgabe)	AUT_CMS	
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 37: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

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 5.9.

5.4.2.1 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 K_Initialisierung: Initialisierte Attribute von MF / DF.HPA / EF.HPD**

EF.HPD MUSS die in Tab_HBA_ObjSys_032 dargestellten Werte besitzen.

Tabelle 45: Tab_HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘D0 01’	
shortFileIdentifier	‘01’= 1	
numberOfOctet	‘08 00’ Oktett = 2048 Oktett	
positionLogicalEnd OfFile	’0’	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird später nachgeladen
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.CH)	
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	AUT_PACE	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	AUT_PACE AND PWD(PIN.CH)	
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 38: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

5.4.2.2 Sicherheitsumgebungen

In DF.HPA wird das SE#1 verwendet.

5.5 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.

5.5.1 Dateistruktur und Dateiinhalt

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

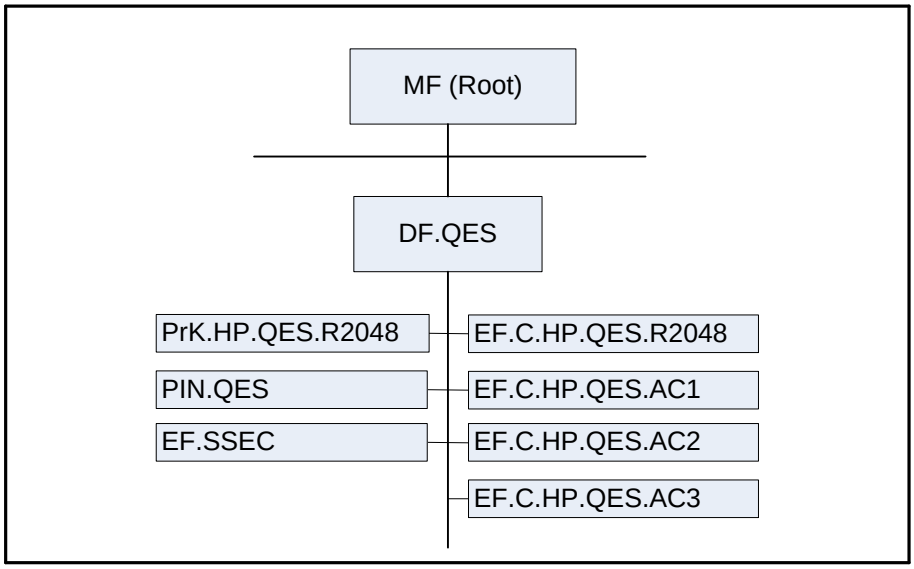

Abbildung 3: Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung

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.

5.5.2 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 K_Initialisierung: Initialisierte Attribute von MF / DF.QES**

DF.QES MUSS die in Tab_HBA_ObjSys_033 dargestellten Werte besitzen.

Tabelle 46: Tab_HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D276000066 01’	siehe Hinweis 40:
fileIdentifier	–	siehe Hinweis 41:
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	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
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	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
alle	herstellerspezifisch	

⌫

Hinweis 39: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 40: Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 41: herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [ISO7816-4#8.1.1]

Hinweis 42: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.5.2 im Allgemeinen irrelevant.

Hinweis 43: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

5.5.2.1 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 5.5.2.2 dargestellt. Der zugehörige öffentliche Schlüssel PuK.HP.QES.R2048 ist in C.HP.QES.R2048 (siehe Kapitel 5.5.2.4) enthalten.

⌦ **Card-G2-A_2085 K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048**

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

Tabelle 47: Tab_HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt RSA 2048	
keyIdentifier	‘04’ = 4	siehe Hinweis 45:
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	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 ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
PSO Comp Dig Sig	PWD(PIN.QES)	Modus Einzelsignatur
DELETE	herstellerspezifisch	siehe Hinweis 47:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
PSO Comp Dig Sig	PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRespEnc	siehe Hinweis 48:
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 (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	AUT_PACE	

PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.QES)	Modus Einzelsignatur
DELETE	herstellerspezifisch	siehe Hinweis 47:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
PSO Compute Digital Signature	PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRspEnc	siehe Hinweis 48:
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 44: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 45: Der Wert des Attributes keyIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 46: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Hinweis 47: Die konkrete Zugriffsregel muss durch den Objektsystemhersteller in Abstimmung mit dem jeweiligen ZDA gemäß SigG/SigV festgelegt werden.

Hinweis 48: Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115]. Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)

⌦ **Card-G2-A_3298 K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048**

Bei der Personalisierung von PrK.HP.QES.R2048 MÜSSEN die in Tab_HBA_ObjSys_108 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 48: Tab_HBA_ObjSys_108 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

⌫

5.5.2.2 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 K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PIN.QES**

PIN.QES MUSS die in Tab_HBA_ObjSys_037 dargestellten Werte besitzen.

Tabelle 49: Tab_HBA_ObjSys_037 Initialisierte Attribute von MF / DF.QES / PIN.QES

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	‘01’ = 1	
secret	undefiniert	wird personalisiert
minimumLength	6	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	Transport-PIN	
flagEnabled	True	
Start Security Status Evaluation Counter	SE # 1: SSEC = 1 SE # 2: 1 ≤ SSEC ≤ 250	Werte wie in EF.SSEC angezeigt
PUK	undefiniert	wird personalisiert

pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC., P1=1	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	SmMac(flagTI.54) AND SmCmdEnc	
GET PIN STATUS	SmMac(flagTI.55)	
RESET RC., P1=1	SmMac(flagTI.54) AND SmCmdEnc	
VERIFY	SmMac(flagTI.54) AND SmCmdEnc	
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 SE#1	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	AUT_PACE	
GET PIN STATUS	AUT_PACE	
RESET RC., P1=1	AUT_PACE	
VERIFY	AUT_PACE	
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	SmMac(flagTI.54) AND SmCmdEnc	
GET PIN STATUS	SmMac(flagTI.55)	
RESET RC., P1=1	SmMac(flagTI.54)	

	AND SmCmdEnc	
VERIFY	SmMac(flagTI.54) 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 49: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

⌦ **Card-G2-A_3299 K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PIN.QES**

Bei der Personalisierung von PIN.QES MÜSSEN die in Tab_HBA_ObjSys_111 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 50: Tab_HBA_ObjSys_111 Personalisierte Attribute von MF / DF.QES / PIN.QES

Attribute	Wert	Bemerkung
secret	PIN-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert
transportStatus	Transport-PIN	wird gegebenenfalls personalisiert, siehe Hinweis 50:
PUK	PUK-Wert gemäß [gemSpec_PINPUK_TI]	wird personalisiert

⌫

Hinweis 50: Für transportStatus wird der Wert „Transport-PIN" initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword" zu setzen.

5.5.2.3 MF / DF.QES / EF.SSEC

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

⌦ **Card-G2-A_2089 K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.SSEC**

EF.SSEC MUSS die in Tab_HBA_ObjSys_038 dargestellten Werte besitzen.

Tabelle 51: Tab_HBA_ObjSys_038 Initialisierte 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	
positionLogical EndOfFile	‘002E’ Oktett = 46 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß den Werten für *Start SecurityStatus Evaluation Counter* für SE#1 und für SE#2 in PIN.QES (siehe Kapitel 5.5.2.2)	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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 SE#1	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(SK.CAN) AND SmRspEnc	
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
READ BINARY	AUT_PACE	
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 51: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Der Inhalt von EF.SSEC (siehe Tab_HBA_ObjSys_038) wird während der Initialisierung gespeichert. Die externe Signaturanwendungskomponente kann den Inhalt der Datei lesen, um die Größe des Signaturstapels zu optimieren. Die Angaben in EF.SSEC müssen den implementierten SSEC-Maximalwerten entsprechen.

⌦ **Card-G2-A_2090 K_Initialisierung: Inhalt von EF.SSEC**

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

Tabelle 52: 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 Sicherheits-umgebungen 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.

5.5.2.4 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 5.5.2.1 definiert.

⌦ **Card-G2-A_2091 K_Initialisierung: Initialisierte 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 53: Tab_HBA_ObjSys_040 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'C0 00'	siehe Hinweis 53:
shortFileIdentifier	'10'= 16	
numberOfOctet	'07 6C' Oktett = 1900 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	herstellerspezifisch	siehe Hinweis 54:
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	herstellerspezifisch	siehe Hinweis 54:

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 SE#1	Zugriffsbedingung	Bemerkung
DELETE	herstellerspezifisch	siehe Hinweis 54:
READ BINARY	AUT_PACE	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	herstellerspezifisch	siehe Hinweis 54:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
DELETE	herstellerspezifisch	siehe Hinweis 54:
READ BINARY	SmMac(flagTI.55) AND SmRspEnc	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	herstellerspezifisch	siehe Hinweis 54:
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 52: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 53: Der Wert des Attributes fileIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 54: Die konkrete Zugriffsregel muss durch den Objektsystemhersteller, der diese Option umsetzt, in Abstimmung mit einer Bestätigungsstelle gemäß SigG/SigV festgelegt werden.

⌦ **Card-G2-A_3301 K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048**

Bei der Personalisierung von EF.C.HP.QES.R2048 MÜSSEN die in Tab_HBA_ObjSys_113 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 54: Tab_HBA_ObjSys_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

Attribute	Wert	Bemerkung
positionLogical EndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HP.QES.R2048 gemäß [gemSpec_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.QES.R2048	

⌫

5.5.2.5 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) müssen die vorhandenen Attributzertifikate durch neue ersetzt werden, die an das neue Zertifikat gebunden sind.

⌦ **Card-G2-A_2094 K_Initialisierung: Initialisierte 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 55: Tab_HBA_ObjSys_042 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C0 01’	siehe Hinweis 57:
shortFileIdentifier	‘01’ = 1	
numberOfOctet	’06 40’ Oktett = 1600 Oktett	
positionLogicalEndOfFile	’0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	kein Inhalt	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE 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 SE#1	Zugriffsbedingung	Bemerkung
READ BINARY	AUT_PACE	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	AUT_PACE AND PWD(PIN.CH)	Zugriffsregel von PIN.CH ist auf MF-Ebene definiert
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
READ BINARY	SmMac(flagTI.55) AND SmRspEnc	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.CH) AND SmMac(flagTI.55))	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 55: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_3302 K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1**

Bei der Personalisierung von EF.C.HP.QES-AC1 KÖNNEN die in Tab_HBA_ObjSys_115 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 56: Tab_HBA_ObjSys_115 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1

Attribute	Wert	Bemerkung
positionLogical EndOfFile	Zahl der tatsächlich belegten Oktette	
body	Attributs-Zertifikat zu C.HP.QES.R2048	

⌫

⌦ **Card-G2-A_2095 K_Initialisierung: Initialisierte 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 57: Tab_HBA_ObjSys_043 Initialisierte Attri7bute von MF / DF.QES / EF.C.HP.QES-AC2

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C0 02’	siehe Hinweis 57:
shortFileIdentifier	‘02’ = 2	
numberOfOctet	’06 40’ Oktett = 1600 Oktett	
positionLogicalEnd OfFile	’0’	
flagTransactionMod e	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln		
accessRules	identisch zu EF.C.HP.QES-AC1	

⌫

⌦ **Card-G2-A_3303 K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2**

Bei der Personalisierung von EF.C.HP.QES-AC2 KÖNNEN die in Tab_HBA_ObjSys_116 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 58: Tab_HBA_ObjSys_116 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2

Attribute	Wert	Bemerkung
positionLogical EndOfFile	Zahl der tatsächlich belegten Oktette	
body	‘Attributs-Zertifikat zu C.HP.QES.R2048	

⌫

⌦ **Card-G2-A_2096 K_Initialisierung: Initialisierte 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 59: Tab_HBA_ObjSys_044 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C0 03’	siehe Hinweis 57:
shortFileIdentifier	‘03’ = 3	
numberOfOctet	’06 40’ Oktett = 1600 Oktett	
positionLogicalEnd OfFile	’0’	
flagTransactionMod e	False	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln		
accessRules	identisch zu EF.C.HP.QES-AC1	

⌫

Hinweis 56: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 57: Der Wert des Attributes fileIdentifier ist in [ISO7816-4] festgelegt.

⌦ **Card-G2-A_3304 K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3**

Bei der Personalisierung von EF.C.HP.QES-AC3 KÖNNEN die in Tab_HBA_ObjSys_117 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 60: Tab_HBA_ObjSys_117 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3

Attribute	Wert	Bemerkung
positionLogical EndOfFile	Zahl der tatsächlich belegten Oktette	
body	Attributs-Zertifikat zu C.HP.QES.R2048	

⌫

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.

5.6 Die ESIGN-Anwendung (DF.ESIGN)

5.6.1 Dateistruktur und Dateiinhalt

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

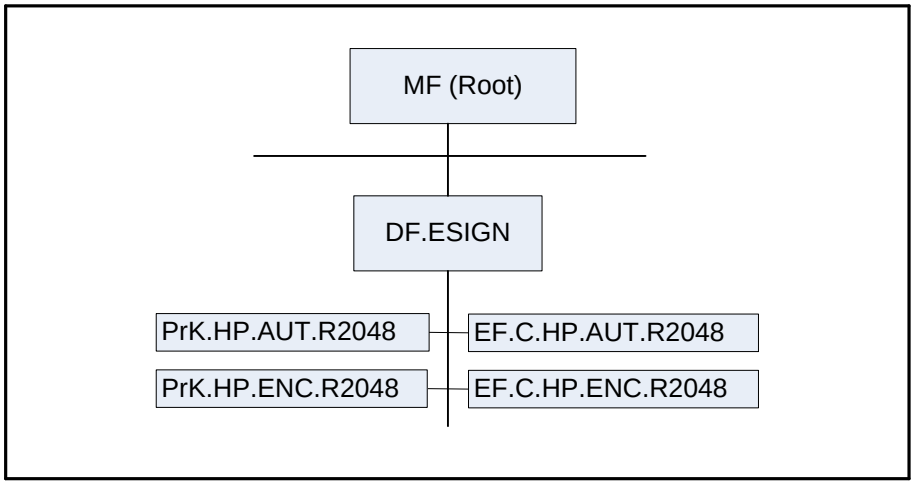

Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN

5.6.2 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 K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN**

DF.ESIGN MUSS die in Tab_HBA_ObjSys_045 dargestellten Werte besitzen.

Tabelle 61: Tab_HBA_ObjSys_045 Initialisierte Attribute von MF / DF.ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	'A000000167 455349474E'	siehe Hinweis 59:
fileIdentifier	–	siehe Hinweis 60:
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 62:
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
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 62:
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 58: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 59: Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis 60: herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1].

Hinweis 61: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.6 im Allgemeinen irrelevant.

Hinweis 62: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.9.

5.6.2.1 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 5.6.2.3) enthalten.

⌦ **Card-G2-A_2098 K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048**

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

Tabelle 62: Tab_HBA_ObjSys_046 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'02' = 2	
privateKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	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 AUTHENTICATE PSO Compute Digital Signature	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 64:
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 (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
INTERNAL AUTHENTICATE PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 64:
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 63: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 64: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

⌦ **Card-G2-A_3305 K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048**

Bei der Personalisierung von PrK.HP.AUT.R2048 MÜSSEN die in Tab_HBA_ObjSys_118 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 63: Tab_HBA_ObjSys_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

⌫

5.6.2.2 MF / DF.ESIGN / PrK.HP.ENC.R2048

PrK.HP.ENC.R2048 ist der private Schlüssel für die Kryptographie mit RSA für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Der zugehörige öffentliche Schlüssel PuK.HP.ENC.R2048 ist in C.HP.ENC.R2048 (siehe Kapitel 5.6.2.4) enthalten.

⌦ **Card-G2-A_2101 K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048**

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

Tabelle 64: Tab_HBA_ObjSys_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	‘03’ = 3	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	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
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 66:

PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	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	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 66:
PSO Decipher PSO Transcipher	AUT_PACE AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	
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 65: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 66: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116-1].

⌦ **Card-G2-A_3306 K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048**

Bei der Personalisierung von PrK.HP.ENC.R2048 MÜSSEN die in Tab_HBA_ObjSys_121 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 65: Tab_HBA_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

⌫

5.6.2.3 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 5.6.2.1 definiert.

⌦ **Card-G2-A_2107 K_Initialisierung: Initialisierte 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 66: Tab_HBA_ObjSys_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C5 00’	
shortFileIdentifier	‘01’= 1	
numberOfOctet	‘07 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 68:
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	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
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 68:
READ BINARY	AUT_PACE OR AUT_CMS OR AUT_CUP	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	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
alle	herstellerspezifisch	

⌫

Hinweis 67: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 68: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3307 K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048**

Bei der Personalisierung von EF.C.HP.AUT.R2048 MÜSSEN die in Tab_HBA_ObjSys_127 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 67: Tab_HBA_ObjSys_127 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HP.AUT.R2048 gemäß [gemSpec_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.AUT.R2048	

⌫

5.6.2.4 MF / DF.ESIGN / EF.C.HP.ENC.R2048

Die Datei EF.C.HP.ENC.R2048 enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.ENC.R2048. Das zugehörende private Schlüsselobjekt PrK.HP.ENC.R2048 ist im Kapitel 5.6.2.2 definiert.

⌦ **Card-G2-A_2110 K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048**

EF.C.HP.ENC.R2048 MUSS die in Tab_HBA_ObjSys_056 dargestellten Werte besitzen.

Tabelle 68: Tab_HBA_ObjSys_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C2 00’	
shortFileIdentifier	‘02’= 2	
numberOfOctet	‘07 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	wird personalisiert
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 70:
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 70:

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 OR AUT_CUP	siehe Hinweis 70:
READ BINARY	AUT_PACE OR AUT_CMS OR AUT_CUP	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 70:
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 69: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 70: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

⌦ **Card-G2-A_3308 K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048**

Bei der Personalisierung von EF.C.HP.ENC.R2048 MÜSSEN die in Tab_HBA_ObjSys_129 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 69: Tab_HBA_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HP.ENC.R2048 gemäß [gemSpec_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.ENC.R2048	

⌫

5.6.3 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 einem stationären HBA zu ermöglichen.

5.7 Die kryptographischen Informationsanwendungen

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. Die logischen File-Namen, File Identifier, Short File Identifier und die Dateiinhalte sind konform zu [ISO7816-15].

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

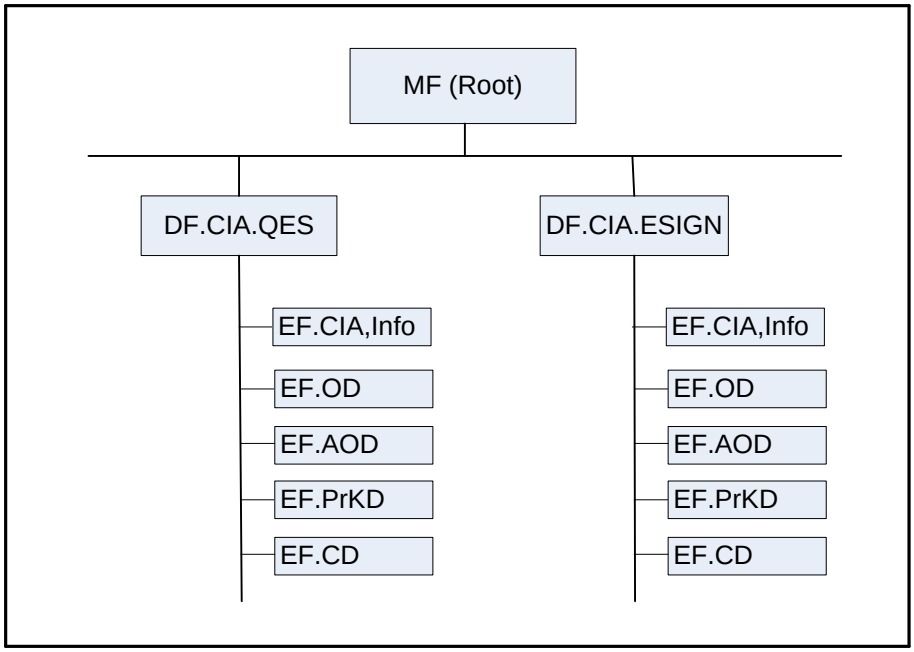

Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen

5.7.1 MF / DF.CIA.QES (Cryptographic Information Applications)

⌦ **Card-G2-A_2117 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES**

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

Tabelle 70: Tab_HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘‘E828BD080F D27600006601’	siehe Hinweis 82:
fileIdentifier	–	siehe Hinweis 83:
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	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
GET RANDOM	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	

⌫

5.7.1.1 MF / DF.CIA.QES / EF.CIA.CIAInfo

⌦ **Card-G2-A_2119 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo**

MF / DF.CIA.QES / EF.CIA.CIAInfo MUSS die in Tab_HBA_ObjSys_059 dargestellten Werte besitzen.

Tabelle 71: Tab_HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘50 32’	siehe Hinweis 72:
shortFileIdentifier	‘12’= 18	siehe Hinweis 72:
numberOfOctet	’01 99’ Oktett = 153 Oktett	
positionLogicalEndOfFile	’01 99’ Oktett = 153 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	30 8196 | 02 01 01 | 80 1f 5175616c69666965 64205369676e6174 757265204170706c 69636174696f6e | 03 02 0560 | 30 1a | | 30 0b | | | 02 01 01 | | | 04 06 d27600006601 | | 30 0b | | | 02 01 02 | | | 04 06 d27600006601 | 30 50 | | 30 18 | | | 02 01 01 | | | 04 02 0250 | | | 05 00 | | | 03 02 0102 | | | 06 09 608648016503040201 | | 30 17 | | | 02 01 03 | | | 04 01 43 | | | 05 00 | | | 03 02 0604 | | | 06 06 60864883770d | | | 02 01 05 | | 30 1b | | | 02 01 04	statischer Inhalt, da keine Administration der Schlüssel möglich ist

	| | | 04 04 80000001 | | | 05 00 | | | 03 02 0604 | | | 06 07 2b240304030204 | | | 02 01 07	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 71: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 72: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.1.2 **MF / DF.CIA.QES /** EF.OD

Card-G2-A_2120 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.OD (Object Directory)

MF / DF.CIA.QES / EF.OD MUSS die in Tab_HBA_ObjSys_060 dargestellten Werte besitzen.

Tabelle 72: Tab_HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	’50 31’	siehe Hinweis 74:
shortFileIdentifier	‘11’ = 17	siehe Hinweis 74:
numberOfOctet	’00 15’ Oktett = 21 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	’00 15’ Oktett = 21 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	`a8 05`
	`|  30 03`
	`|  |  04 01 14`
	`a0 05`
	`|  30 03`
	`|  |  04 01 15`
	`a4 05`
	`|  30 03`
	`|  |  04 01 16`
		statischer Inhalt, da keine Administration der Schlüssel möglich ist

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 73: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 74: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.1.3 MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)

⌦ **Card-G2-A_2121 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)**

MF / DF.CIA.QES / EF.AOD MUSS die in Tab_HBA_ObjSys_061 dargestellten Werte besitzen.

Tabelle 73: Tab_HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 34'	siehe Hinweis 76:
shortFileIdentifier	'14' = 20	siehe Hinweis 76:
numberOfOctet	'00 8E' Oktett = 142 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	'00 8E' Oktett = 142 Oktett	
flagTransactionMode	False	
flagChecksum	True	

lifeCycleStatus	Operational state (activated)	
shareable	True	
body	30 47 | 30 10 | | 0c 07 50494e2e514553 | | 03 02 0780 | | 04 01 13 | 30 0f | | 30 0d | | | 03 02 0520 | | | 30 07 | | | | 03 02 06c0 | | | | 02 01 02 | 30 03 | | 04 01 03 | a1 1d | | 30 1b | | | 03 03 044810 | | | 0a 01 04 | | | 02 01 06 | | | 02 01 00 | | | 02 01 08 | | | 80 01 81 | | | 30 05 | | | | 04 03 3f0004 30 43 | 30 0d | | 0c 07 50554b2e514553 | | 03 02 0780 | 30 0f | | 30 0d | | | 03 02 0520 | | | 30 07 | | | | 03 02 06c0 | | | | 02 01 02 | 30 03 | | 04 01 12 | a1 1c | | 30 13 | | | 03 02 017a | | | 0a 01 04 | | | 02 01 08 | | | 02 01 08 | | | 02 01 08 | | | 80 01 81 | | 30 05 | | | 04 03 3f0004	statischer Inhalt, da keine Administration der Schlüssel möglich ist
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 75: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 76: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.1.4 MF / DF.CIA.QES / EF.PrKD (Private Key Directory)

⌦ **Card-G2-A_2122 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)**

MF / DF.CIA.QES / EF.PrKD MUSS die in Tab_HBA_ObjSys_062 dargestellten Werte besitzen.

Tabelle 74: Tab_HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 35'	siehe Hinweis 78:
shortFileIdentifier	'15' = 21	siehe Hinweis 78:

numberOfOctet	’00 51’ Oktett = 81 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	‘0051’ Oktett = 81 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	<pre>30 4f
	| 30 35
	| | 0c 0a 50724b2e48502e514553
	| | 03 02 0780
	| | 04 01 03
	| | 30 20
	| | | 30 1e
	| | | | 03 02 0520
	| | | | a2 18
	| | | | | 04 01 03
	| | | | | 30 07
	| | | | | | 03 02 0520
	| | | | | | 02 01 01
	| | | | | 04 01 03
	| | | | | 30 07
	| | | | | | 03 02 0520
	| | | | | | 02 01 02
	| 30 0a
	| | 04 01 84
	| | 03 02 0520
	| | 02 01 84
	| a1 0a
	| | 30 08
	| | | 30 02
	| | | | 04 00
	| | | 02 02 0800</pre>
		statischer Inhalt, da keine Administration der Schlüssel möglich ist

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 77: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 78: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.1.5 **MF / DF.CIA.QES /** EF.CD (Certificate Directory)

⌦ **Card-G2-A_2123 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CD(Certificate Directory)**

MF / DF.CIA.QES / EF.CD MUSS die in Tab_HBA_ObjSys_063 dargestellten Werte besitzen.

Tabelle 75: Tab_HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD (Certificate Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	’50 38’	siehe Hinweis 80:
shortFileIdentifier	‘16’ = 22	siehe Hinweis 80:
numberOfOctet	’00 8C’ Oktett = 140 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	’00 8C’ Oktett = 140 Oktett	
flagTransactionMode	False	
flagChecksum	True	

lifeCycleStatus	Operational state (activated)	
shareable	True	
body	30 1e | 30 0e | | 0c 08 432e48502e514553 | | 03 02 0780 | 30 03 | | 04 01 84 | a1 07 | | 30 05 | | | 30 03 | | | | 04 01 10 30 22 | 30 12 | | 0c 0c 432e48502e5145532d414331 | | 03 02 0780 | 30 03 | | 04 01 84 | a1 07 | | 30 05 | | | 30 03 | | | | 04 01 01 30 22 | 30 12 | | 0c 0c 432e48502e5145532d414332 | | 03 02 0780 | 30 03 | | 04 01 84 | a1 07 | | 30 05 | | | 30 03 | | | | 04 01 02 30 22 | 30 12 | | 0c 0c 432e48502e5145532d414333 | | 03 02 0780 | 30 03 | | 04 01 84 | a1 07 | | 30 05 | | | 30 03 | | | | 04 01 03	statischer Inhalt, da keine Administration der Schlüssel möglich ist

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 79: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 80: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.2 MF / DF.CIA.ESIGN (Cryptographic Information Applications)

⌦ **Card-G2-A_2118 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN**

DF.CIA.ESIGN MUSS die in Tab_HBA_ObjSys_058 dargestellten Werte besitzen.

Tabelle 76: Tab_HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	'E828BD080F A000000167455349474E'	siehe Hinweis 82:
fileIdentifier	–	siehe Hinweis 83:
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	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
GET RANDOM	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 81: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 82: Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [ISO7816-15] sowie als PIX den applicationIdentifier von [ISO7816-4].

Hinweis 83: herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS# 8.1.1]

Hinweis 84: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.7 im Allgemeinen irrelevant.

5.7.2.1 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo

⌦ **Card-G2-A_3320 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo**

MF / DF.CIA.ESIGN / EF.CIA.CIAInfo MUSS die in Tab_HBA_ObjSys_145 dargestellten Werte besitzen.

Tabelle 77: Tab_HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo (Cryptographic Information Application Info)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘50 32’	siehe Hinweis 72:
shortFileIdentifier	‘12’= 18	siehe Hinweis 72:
numberOfOctet	’00 2F’ Oktett = 47 Oktett	
positionLogicalEndOfFile	’00 2F’ Oktett = 47 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	30 2d | 02 01 01 | 80 11 455349474e204170 706c69636174696f 6e | 03 02 0560 | 30 11 | | 30 0f | | | 02 01 01 | | | 04 0a a000000167455349474e	statischer Inhalt, da keine Administration der Schlüssel möglich ist
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 85: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 86: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.2.2 MF / DF.CIA.ESIGN / EF.OD

⌦ **Card-G2-A_3321 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)**

MF / DF.CIA.ESIGN / EF.OD MUSS die in Tab_HBA_ObjSys_146 dargestellten Werte besitzen.

Tabelle 78: Tab_HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 31'	siehe Hinweis 74:
shortFileIdentifier	'11' = 17	siehe Hinweis 74:
numberOfOctet	'0015' Oktett = 21 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	'0015' Oktett = 21 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	`a8 05`
	`| 30 03`
	`| | 04 01 14`
	`a0 05`
	`| 30 03`
	`| | 04 01 15`
	`a4 05`
	`| 30 03`
		statischer Inhalt, da keine Administration der Schlüssel möglich ist

	| | 04 01 16	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 87: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 88: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.2.3 MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)

⌦ **Card-G2-A_3322 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)**

MF / DF.CIA.ESIGN / EF.AOD MUSS die in Tab_HBA_ObjSys_147 dargestellten Werte besitzen.

Tabelle 79: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	’50 34’	siehe Hinweis 76:
shortFileIdentifier	‘14’ = 20	siehe Hinweis 76:
numberOfOctet	’00 5C’ Oktett = 92 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	’00 5C’ Oktett = 92 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	`30 2e`
	`| 30 0f`
	`| | 0c 06 50494e2e4348`
	`| | 03 02 0780`
	`| | 04 01 12`
	`| 30 03`
	`| | 04 01 02`
	`| a1 16`
	`| | 30 14`
	`| | | 03 03 040810`
	`| | | 0a 01 04`
	`| | | 02 01 05`
	`| | | 02 01 00`
	`| | | 02 01 08`
	`| | | 80 01 01`
	`30 2a`
	`| 30 0c`
	`| | 0c 06 50554b2e4348`
	`| | 03 02 0780`
	`| 30 03`
	`| | 04 01 12`
	`| a1 15`
	`| | 30 13`
	`| | | 03 02 013a`
	`| | | 0a 01 04`
	`| | | 02 01 08`
	`| | | 02 01 08`
	`| | | 02 01 08`
	`| | | 80 01 01`
		statischer Inhalt, da keine Administration der Schlüssel möglich ist

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 89: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 90: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.7.2.4 MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

⌦ **Card-G2-A_3323 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)**

MF / DF.CIA.ESIGN / EF.PrKD MUSS die in Tab_HBA_ObjSys_148 dargestellten Werte besitzen.

Tabelle 80: Tab_HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 35'	siehe Hinweis 78:
shortFileIdentifier	'15' = 21	siehe Hinweis 78:
numberOfOctet	'00 83' Oktett = 131 Oktett	Dateigröße an den unveränderlichen

		Inhalt angepasst
positionLogicalEndOfFile	’00 83’ Oktett = 131 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	30 40 | 30 26 | | 0c 0a 50724b2e48502e415554 | | 03 02 0780 | | 04 01 02 | | 30 11 | | | 30 0f | | | | 03 02 0520 | | | | a1 09 | | | | | 04 01 02 | | | | | 30 04 | | | | | | 03 02 0520 | 30 0a | | 04 01 82 | | 03 02 0410 | | 02 01 82 | a1 0a | | 30 08 | | | 30 02 | | | | 04 00 | | | 02 02 0800 30 3f | 30 25 | | 0c 09 50724b2e48502e4b45 | | 03 02 0780 | | 04 01 02 | | 30 11 | | | 30 0f | | | | 03 02 0520 | | | | a1 09 | | | | | 04 01 02 | | | | | 30 04 | | | | | | 03 02 0520 | 30 0a | | 04 01 83 | | 03 02 0204 | | 02 01 83 | a1 0a | | 30 08 | | | 30 02 | | | | 04 00 | | | 02 02 0800	statischer Inhalt, da keine Administration der Schlüssel möglich ist
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 91: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

5.7.2.5 MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)

⌦ **Card-G2-A_3324 K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)**

MF / DF.CIA.ESIGN / EF.CD MUSS die in Tab_HBA_ObjSys_149 dargestellten Werte besitzen.

Tabelle 81: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 38'	siehe Hinweis 80:

shortFileIdentifier	‘16’ = 22	siehe Hinweis 80:
numberOfOctet	’00 40’ Oktett = 64 Oktett	Dateigröße an den unveränderlichen Inhalt angepasst
positionLogicalEndOfFile	’00 40’ Oktett = 64 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	`30 1e`
	`|  30 0e`
	`|  |  0c 08 432e48502e415554`
	`|  |  03 02 0780`
	`|  30 03`
	`|  |  04 01 82`
	`|  a1 07`
	`|  |  30 05`
	`|  |  |  30 03`
	`|  |  |  |  04 01 01`
	`30 1e`
	`|  30 0e`
	`|  |  0c 08 432e48502e415554`
	`|  |  03 02 0780`
	`|  30 03`
	`|  |  04 01 83`
	`|  a1 07`
	`|  |  30 05`
	`|  |  |  30 03`
	`|  |  |  |  04 01 02`
		statischer Inhalt, da keine Administration der Schlüssel möglich ist

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	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	AUT_PACE	
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 92: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

Hinweis 93: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

5.8 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 HBA-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.

5.8.1 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.

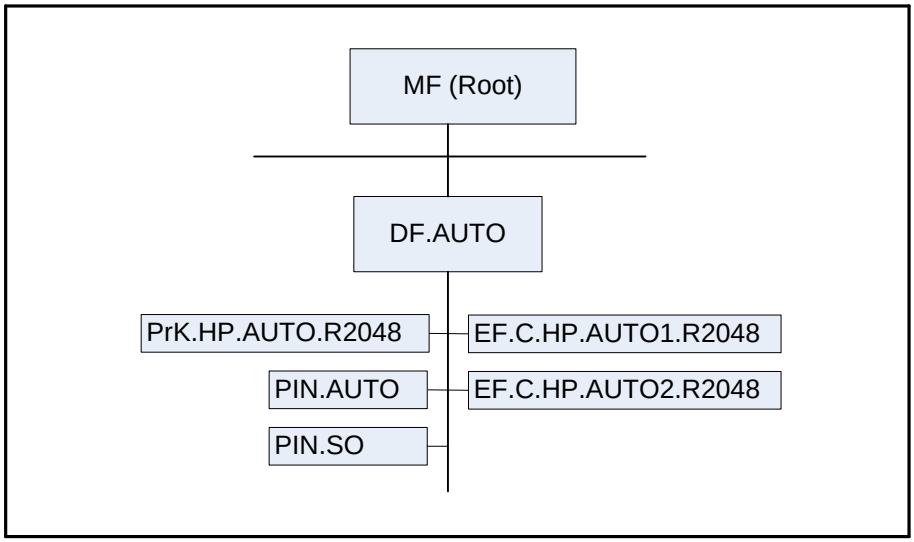

Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO

5.8.2 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 K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO**

DF.AUTO MUSS die in Tab_HBA_ObjSys_064 dargestellten Werte besitzen.

Tabelle 82: Tab_HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D27600014603’	siehe Hinweis 95:
fileIdentifier	–	siehe Hinweis 96:
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 98:
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
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 98:
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 94: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 95: Der Wert des Attributes applicationIdentifier ist in [ISO7816-4].

Hinweis 96: herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1]

Hinweis 97: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.8 im Allgemeinen irrelevant.

Hinweis 98: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

5.8.2.1 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 K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048**

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

Tabelle 83: Tab_HBA_ObjSys_065 Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'02' = 2	
privateKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	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 ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
INTERNAL AUTHENTICATE PSO Compute Digital Signature	PWD(PIN.AUTO)	
DELETE	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	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	
INTERNAL AUTHENTICATE PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.AUTO)	

DELETE	AUT_PACE 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	NEVER	

⌫

Hinweis 99: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Anmerkung – PrK.HP.AUTO.R2048 ist ein privates RSA-Objekt, welches gemäß Kapitel 9.6.3 in [gemSpec_COS] das Kommando GENERATE ASYMMETRIC KEY PAIR 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.

⌦ **Card-G2-A_3314 K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048**

Bei der Personalisierung von PrK.HP.AUTO.R2048 MÜSSEN die in Tab_HBA_ObjSys_138 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 84: Tab_HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

⌫

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116-1].

5.8.2.2 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) dient.

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 K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO**

PIN.AUTO MUSS die in Tab_HBA_ObjSys_068 dargestellten Werte besitzen.

Tabelle 85: Tab_HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	‘01’ = 1	
secret	undefiniert	wird personalisiert
minimumLength	5	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {Leer–PIN, Transport–PIN}	
flagEnabled	True	
startSsec	unendlich	
PUK	undefiniert	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	AUT_PACE	
GET PIN STATUS	AUT_PACE	
RESET RC., P1=1	AUT_PACE	
VERIFY	AUT_PACE	
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 100: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

⌦ Card-G2-A_3270 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AUTO

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

⌦ Card-G2-A_3315 K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO

Wenn der Wert des Attributes *transportStatus* von PIN.AUTO Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.AUTO die in Tab_HBA_ObjSys_141 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 86: Tab_HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO

Attribute	Wert	Bemerkung
secret	Transport-PIN	Wird personalisiert, siehe Hinweis 101:
PUK	PUK-Wert gemäß [gemSpec_PINPUK_TI]	

⌫

Hinweis 101: Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

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.

5.8.2.3 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 K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.SO**

PIN.SO MUSS die in Tab_HBA_ObjSys_069 dargestellten Werte besitzen.

Tabelle 87: Tab_HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	‘03’ = 3	
secret	undefiniert	wird personalisiert
minimumLength	6	
maximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {Leer–PIN, Transport–PIN}	
flagEnabled	True	
startSsec	unendlich	
PUK	undefiniert	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	AUT_PACE	
GET PIN STATUS	AUT_PACE	
RESET RC., P1=1	AUT_PACE	
VERIFY	AUT_PACE	
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 102: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

⌦ **Card-G2-A_3271 K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SO**

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

⌦ **Card-G2-A_3316 K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.SO**

Wenn der Wert des Attributes *transportStatus* von PIN.SO Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.SO die in Tab_HBA_ObjSys_142 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 88: Tab_HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO

Attribute	Wert	Bemerkung
secret	Transport-PIN	Wird personalisiert, siehe Hinweis 103:
PUK	PUK-Wert gemäß [gemSpec_PINPUK_TI]	

⌫

Hinweis 103: Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

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.

5.8.2.4 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 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 K_Initialisierung: Initialisierte 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 89: Tab_HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	

fileIdentifier	‘E0 01’	
shortFileIdentifier	‘01’ = 1	
numberOfOctet	‘07 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	PWD(PIN.SO)	
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE 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	AUT_PACE AND PWD(PIN.SO)	
READ BINARY	AUT_PACE	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	AUT_PACE 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	

⌫

Hinweis 104: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_3317 K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048**

Bei der Personalisierung von EF.C.HP.AUTO1.R2048 MÜSSEN die in Tab_HBA_ObjSys_143 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 90: Tab_HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048

Attribute	**Wert**	**Bemerkung**
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	wird personalisiert
body	C.HP.AUTO1.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUTO.R2048	wird personalisiert

⌫

⌦ **Card-G2-A_2131 K_Initialisierung: Initialisierte : MF / DF.AUTO / EF.C.HP.AUTO2.R2048**

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

Tabelle 91: Tab_HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘E0 02’	
shortFileIdentifier	‘02’ = 2	
numberOfOctet	‘07 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	kein Inhalt	wird personalisiert

Zugriffsregeln		
accessRules	identisch zu EF.C.HP.AUTO1.R2048	

⌫

⌦ **Card-G2-A_3318 K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R2048**

Bei der Personalisierung von EF.C.HP.AUTO2.R2048 MÜSSEN die in Tab_HBA_ObjSys_144 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 92: Tab_HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	wird personalisiert
body	C.HP.AUTO2.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUTO.R2048	wird personalisiert

⌫

5.8.2.5 Sicherheitsumgebungen

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

5.8.2.6 Vorgaben für die Nutzung von DF.AUTO

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

⌦ **Card-G2-A_2675 K_Initialisierung: Initialisierte : Wert von PrK.AUTO.R2048**

PrK.HP.AUTO.R2048 MUSS auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2676 K_Personalisierung: Wert von PIN.AUTO**

Falls das Attribut „*transportStatus*“ von PIN.AUTO auf einen Wert aus der Menge {regularPassword, Transport-PIN} gesetzt ist, MUSS PIN.AUTO auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2677 K_Personalisierung: Wert von PUK für PIN.AUTO**

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

⌦ **Card-G2-A_2678 K_Personalisierung: Wert von PIN.SO**

Falls das Attribut „*transportStatus*“ von PIN.SO auf einen Wert aus der Menge {regularPassword, Transport-PIN} gesetzt ist, MUSS PIN.SO auf einen kartenindividuellen Wert gesetzt werden.⌫

⌦ **Card-G2-A_2679 K_Personalisierung: Wert von PUK für PIN.SO**

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

⌦ **Card-G2-A_2680 K_Personalisierung: Inhalt von EF.C.HP.AUTO1.R2048**

EF.C.HP.AUTO1.R2048 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 K_Personalisierung: Inhalt von EF.C.HP.AUTO2. R2048**

EF.C.HP.AUTO2.R2048 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 K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.AUTO**

Falls die HBA-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 K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.SO**

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

Hinweis 105: 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.

5.9 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.Version2) 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)
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
CMS	Card Management System
COS	Card Operating System (Chipkartenbetriebssystem)
CPI	Certificate Profile Identifier

Kürzel	Erläuterung
CRL	Certificate Revocation List (Zertifikatssperrliste)
CS	CertSign (CertificateSigning)
CTA	Card Terminal Application (Kartenterminalanwendung)
CUP	Certificate Update
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
ELC	Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven
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
ICC	Integrated Circuit Card (Chipkarte)
ICCSN	ICC Serial Number (Chip-Seriennummer)
ICM	IC Manufacturer (Kartenhersteller)

Kürzel	Erläuterung
ID	Identifier
IFSC	Information Field Size Card
IIN	Issuer Identification Number
INS	Instruction-Byte einer Kommando-APDU
KM	Komfortmerkmal
KT	Kartenterminal
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
RD	Referenzdaten
RF	Radio Frequency
RFC	Request für Comment
RFID	Radio Frequency Identification
RFU	Reserved for future use
RID	Registered Application Provider Identifier

Kürzel	Erläuterung
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

Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA 21
Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA 61
Abbildung 3: Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung 65
Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN 80

Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen...90
Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO.....112

A4 – Tabellenverzeichnis

Tabelle 1: Tab_HBA_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt.....11
Tabelle 2: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten).....20
Tabelle 3: Tab_HBA_ObjSys_004 Initialisierte Attribute von MF.....21
Tabelle 4: Tab_HBA_ObjSys_005 Initialisierte Attribute von MF / EF.ATR 23
Tabelle 5: Tab_HBA_ObjSys_083 Initialisierte Attribute von MF / EF.CardAccess 24
Tabelle 6: Tab_HBA_ObjSys_007 Initialisierte Attribute von MF / EF.DIR 25
Tabelle 7: Tab_HBA_ObjSys_008 Initialisierte Attribute von MF / EF.GDO 27
Tabelle 8: Tab_HBA_ObjSys_151 Personalisierte Attribute von MF / EF.GDO.....28
Tabelle 9: Tab_HBA_ObjSys_009 Initialisierte Attribute von MF / EF.Version2.....29
Tabelle 10: Tab_HBA_ObjSys_010 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.R2048.....30
Tabelle 11: Tab_HBA_ObjSys_089 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.R2048.....32
Tabelle 12: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256.....32
Tabelle 13: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256.....33
Tabelle 14: Tab_HBA_ObjSys_013 Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048 34
Tabelle 15: Tab_HBA_ObjSys_092 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.R2048 35
Tabelle 16: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256.....36
Tabelle 17: Tab_HBA_ObjSys_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256.....37
Tabelle 18: Tab_HBA_ObjSys_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256 38
Tabelle 19: Tab_HBA_ObjSys_095 Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256 40
Tabelle 20: Tab_HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH.....40
Tabelle 21: Tab_HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH 41
Tabelle 22: Tab_HBA_ObjSys_020 Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048.....42
Tabelle 23: Tab_HBA_ObjSys_098 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.R2048.....44
Tabelle 24: Tab_HBA_ObjSys_021 Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256.....44
Tabelle 25: Tab_HBA_ObjSys_099 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256.....46
Tabelle 26: Tab_HBA_ObjSys_024 Initialisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256 46
Tabelle 27: Tab_HBA_ObjSys_101 Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256 48
Tabelle 28: Tab_HBA_ObjSys_026 Initialisierte Attribute von MF / PuK.RCA.CS.R2048 48
Tabelle 29: Tab_HBA_ObjSys_152 Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten 50

Tabelle 30: Tab_HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256 .50
Tabelle 31: Tab_HBA_ObjSys_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten 51
Tabelle 32: Tab_HBA_ObjSys_082 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 52
Tabelle 33: Tab_HBA_ObjSys_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 54
Tabelle 34: Tab_HBA_ObjSys_029 Initialisierte Attribute von MF / SK.CMS.AES128.....55
Tabelle 35: Tab_HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128 56
Tabelle 36: Tab_HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256.....57
Tabelle 37: Tab_HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256 57
Tabelle 38: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128 58
Tabelle 39: Tab_HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES12858
Tabelle 40: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256 59
Tabelle 41: Tab_HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES25659
Tabelle 42: Tab_HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN 60
Tabelle 43: Tab_HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN 60
Tabelle 44: Tab_HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA 61
Tabelle 45: Tab_HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD ...63
Tabelle 46: Tab_HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES 65
Tabelle 47: Tab_HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048.....67
Tabelle 48: Tab_HBA_ObjSys_108 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048.....69
Tabelle 49: Tab_HBA_ObjSys_037 Initialisierte Attribute von MF / DF.QES / PIN.QES..69
Tabelle 50: Tab_HBA_ObjSys_111 Personalisierte Attribute von MF / DF.QES / PIN.QES 71
Tabelle 51: Tab_HBA_ObjSys_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC.72
Tabelle 52: Tab_HBA_ObjSys_039 Inhalt von EF.SSEC 73
Tabelle 53: Tab_HBA_ObjSys_040 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048.....74
Tabelle 54: Tab_HBA_ObjSys_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048.....76
Tabelle 55: Tab_HBA_ObjSys_042 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.....76
Tabelle 56: Tab_HBA_ObjSys_115 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.....78
Tabelle 57: Tab_HBA_ObjSys_043 Initialisierte Attri7bute von MF / DF.QES / EF.C.HP.QES-AC2.....78
Tabelle 58: Tab_HBA_ObjSys_116 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.....79
Tabelle 59: Tab_HBA_ObjSys_044 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.....79
Tabelle 60: Tab_HBA_ObjSys_117 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.....80
Tabelle 61: Tab_HBA_ObjSys_045 Initialisierte Attribute von MF / DF.ESIGN 81
Tabelle 62: Tab_HBA_ObjSys_046 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048 82
Tabelle 63: Tab_HBA_ObjSys_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048 84

Tabelle 64: Tab_HBA_ObjSys_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048 84
Tabelle 65: Tab_HBA_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048 86
Tabelle 66: Tab_HBA_ObjSys_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048 86
Tabelle 67: Tab_HBA_ObjSys_127 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048 88
Tabelle 68: Tab_HBA_ObjSys_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048 88
Tabelle 69: Tab_HBA_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048 90
Tabelle 70: Tab_HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES 91
Tabelle 71: Tab_HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info) 92
Tabelle 72: Tab_HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD 94
Tabelle 73: Tab_HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) 95
Tabelle 74: Tab_HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory) 97
Tabelle 75: Tab_HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD (Certificate Directory) 99
Tabelle 76: Tab_HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN 101
Tabelle 77: Tab_HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo (Cryptographic Information Application Info) 103
Tabelle 78: Tab_HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory) 104
Tabelle 79: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) 106
Tabelle 80: Tab_HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory) 107
Tabelle 81: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory) 109
Tabelle 82: Tab_HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO 112
Tabelle 83: Tab_HBA_ObjSys_065 Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048 114
Tabelle 84: Tab_HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048 115
Tabelle 85: Tab_HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO 116
Tabelle 86: Tab_HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO 118
Tabelle 87: Tab_HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO 118
Tabelle 88: Tab_HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO 120
Tabelle 89: Tab_HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048 120
Tabelle 90: Tab_HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R2048 122
Tabelle 91: Tab_HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R2048 122

Tabelle 92: Tab_HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R2048 123

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: Spezifikation COS - Spezifikation der elektrischen Schnittstelle
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_PINPUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur
[gemSpec_CAN_TI]	gematik: Übergreifende Spezifikation CAN-Policy
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI
[gemSpec_CVC_Root]	gematik: Spezifikation CVC - Root
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_TK]	gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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
[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-03110-2]	Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) Version 2.10 vom 20.3.2012
[TR-03114]	BSI: TR 03114, Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007
[TR-03115]	BSI: TR-03115, Komfortsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007
[TR-03116-1]	Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur, Version 3.18 vom 30.01.2014