

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem

Version: 4.3.0
Revision: 57726
Stand: 26.10.2018
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemSpec_HBA_ObjSys_G2.1

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung von P15.9

Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---------|----------|----------------|--|-------------|
| 4.0.0 | 21.04.17 | | Einarbeitung Anpassungen Kartengeneration G2.1 | gematik |
| 4.1.0 | 18.12.17 | | Einarbeitung Errata R1.6.4-2 | gematik |
| 4.2.0 | 14.05.18 | | Anpassung auf Grundlage von P 15.2 und P 15.3 | gematik |
| | 26.09.18 | | Einarbeitung P15.9 | gematik |
| 4.3.0 | 26.10.18 | | freigegeben | gematik |

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Einordnung des Dokumentes | 6 |
| 1.1 | Zielsetzung | 6 |
| 1.2 | Zielgruppe | 6 |
| 1.3 | Geltungsbereich | 6 |
| 1.4 | Abgrenzung des Dokuments | 7 |
| 1.5 | Methodik..... | 7 |
| 1.5.1 | Nomenklatur | 7 |
| 1.5.2 | Verwendung von Schlüsselworten | 9 |
| 1.5.3 | Komponentenspezifische Anforderungen | 9 |
| 2 | Optionen | 11 |
| 2.1 | Option_Erstellung_von_Testkarten..... | 11 |
| 3 | Lebenszyklus von Karte und Applikation | 12 |
| 4 | Anwendungsübergreifende Festlegungen | 13 |
| 4.1 | Mindestanzahl logischer Kanäle..... | 13 |
| 4.2 | Unterstützung RSA CV-Zertifikate | 13 |
| 4.3 | Unterstützung Onboard-RSA-Schlüsselgenerierung | 13 |
| 4.4 | Unterstützung optionaler Funktionspakete..... | 13 |
| 4.4.1 | USB-Schnittstelle (optional) | 13 |
| 4.4.2 | Kontaktlose Schnittstelle (optional) | 14 |
| 4.4.3 | Kryptobox (optional)..... | 15 |
| 4.4.4 | Symmetrischer Kryptographiealgorithmus DES (optional)..... | 15 |
| 4.5 | Attributstabellen | 15 |
| 4.5.1 | Attribute eines Ordners..... | 16 |
| 4.5.2 | Attribute einer Datei (EF) | 17 |
| 4.6 | Zugriffsregeln für besondere Kommandos..... | 17 |
| 4.7 | Attributswerte und Personalisierung | 18 |
| 4.8 | Kartenadministration..... | 19 |
| 5 | Spezifikation grundlegender Applikationen | 20 |
| 5.1 | Attribute des Objektsystems | 20 |
| 5.1.1 | ATR-Kodierung..... | 21 |
| 5.2 | Allgemeine Struktur..... | 22 |
| 5.3 | Root, die Wurzelapplikation MF | 22 |
| 5.3.1 | MF / EF.ATR..... | 24 |
| 5.3.2 | MF / EF.CardAccess (Option kontaktlose Schnittstelle) | 25 |
| 5.3.3 | MF / EF.DIR..... | 27 |
| 5.3.4 | MF / EF.GDO..... | 29 |

| | | |
|------------|---|------------|
| 5.3.5 | MF / EF.Version2..... | 31 |
| 5.3.6 | MF / EF.C.CA_HPC.CS.E256..... | 32 |
| 5.3.7 | MF / EF.C.HPC.AUTR_CVC.E256 | 34 |
| 5.3.8 | MF / EF.C.HPC.AUTD_SUK_CVC.E256 | 37 |
| 5.3.9 | MF / PIN.CH | 39 |
| 5.3.10 | MF / PrK.HPC.AUTR_CVC.E256..... | 42 |
| 5.3.11 | MF / PrK.HPC.AUTD_SUK_CVC.E256 | 44 |
| 5.3.12 | Sicherheitsanker zum Import von CV-Zertifikaten | 46 |
| 5.3.12.1 | MF / PuK.RCA.CS.E256..... | 46 |
| 5.3.13 | Asymmetrische Kartenadministration..... | 49 |
| 5.3.13.1 | MF / PuK.RCA.ADMINCMS.CS.E256..... | 49 |
| 5.3.14 | Symmetrische Kartenadministration | 52 |
| 5.3.14.1 | MF / SK.CMS.AES128..... | 52 |
| 5.3.14.2 | MF / SK.CMS.AES256..... | 54 |
| 5.3.14.3 | MF / SK.CUP.AES128..... | 56 |
| 5.3.14.4 | MF / SK.CUP.AES256..... | 58 |
| 5.3.15 | MF / SK.CAN (Option kontaktlose Schnittstelle) | 59 |
| 5.3.16 | Sicherheitsumgebungen auf MF-Ebene..... | 61 |
| 5.4 | Die Heilberufsanwendung DF.HPA..... | 61 |
| 5.4.1 | Dateistruktur und Dateinhalt..... | 61 |
| 5.4.2 | MF / DF.HPA (Health Professional Application) | 62 |
| 5.4.2.1 | MF / DF.HPA / EF.HPD (Health Professional Data)..... | 64 |
| 5.4.2.2 | Sicherheitsumgebungen | 65 |
| 5.5 | Die Anwendung für die qualifizierte elektronische Signatur (DF.QES)..... | 66 |
| 5.5.1 | Dateistruktur und Dateinhalt..... | 66 |
| 5.5.2 | MF / DF.QES (Qualified Electronic Signature Application) | 66 |
| 5.5.2.1 | MF / DF.QES / PrK.HP.QES.R2048 | 68 |
| 5.5.2.2 | MF / DF.QES / PIN.QES..... | 70 |
| 5.5.2.3 | MF / DF.QES / EF.SSEC..... | 73 |
| 5.5.2.4 | MF / DF.QES / EF.C.HP.QES.R2048 | 75 |
| 5.5.2.5 | MF / DF.QES / PrK.HP.QES.E256..... | 78 |
| 5.5.2.6 | MF / DF.QES / EF.C.HP.QES.E256 | 80 |
| 5.6 | Die ESIGN-Anwendung (DF.ESIGN) | 82 |
| 5.6.1 | Dateistruktur und Dateinhalt..... | 82 |
| 5.6.2 | MF / DF.ESIGN (Krypto-Anwendung ESIGN) | 82 |
| 5.6.2.1 | MF / DF.ESIGN / PrK.HP.AUT.R2048 | 84 |
| 5.6.2.2 | MF / DF.ESIGN / PrK.HP.ENC.R2048..... | 86 |
| 5.6.2.3 | MF / DF.ESIGN / EF.C.HP.AUT.R2048 | 88 |
| 5.6.2.4 | MF / DF.ESIGN / EF.C.HP.ENC.R2048..... | 90 |
| 5.6.2.5 | MF / DF.ESIGN / PrK.HP.AUT.E256 | 92 |
| 5.6.2.6 | MF / DF.ESIGN / PrK.HP.ENC.E256 | 94 |
| 5.6.2.7 | MF / DF.ESIGN / EF.C.HP.AUT.E256 | 96 |
| 5.6.2.8 | MF / DF.ESIGN/ EF.C.HP.ENC.E256..... | 98 |
| 5.6.2.9 | MF / DF.ESIGN / EF.C.HP.SIG.R2048 | 100 |
| 5.6.2.10 | MF / DF.ESIGN / EF.C.HP.SIG.E256 | 102 |
| 5.6.2.11 | MF / DF.ESIGN / PrK.HP.SIG.R2048 | 104 |
| 5.6.2.12 | MF / DF.ESIGN / PrK.HP.SIG.E256 | 105 |
| 5.6.3 | Sicherheitsumgebungen | 107 |
| 5.7 | Die kryptographischen Informationsanwendungen | 107 |
| 5.7.1 | MF / DF.CIA.QES (Cryptographic Information Applications) | 107 |
| 5.7.1.1 | MF / DF.CIA.QES / EF.CIA.CIAInfo | 109 |

| | | |
|------------|--|------------|
| 5.7.1.2 | MF / DF.CIA.QES / EF.OD | 111 |
| 5.7.1.3 | MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) | 112 |
| 5.7.1.4 | MF / DF.CIA.QES / EF.PrKD (Private Key Directory) | 114 |
| 5.7.1.5 | MF / DF.CIA.QES / EF.CD (Certificate Directory) | 116 |
| 5.7.2 | MF / DF.CIA.ESIGN (Cryptographic Information Applications) | 118 |
| 5.7.2.1 | MF / DF.CIA.ESIGN / EF.CIA.CIAInfo | 120 |
| 5.7.2.2 | MF / DF.CIA.ESIGN / EF.OD | 122 |
| 5.7.2.3 | MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) | 124 |
| 5.7.2.4 | MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory) | 125 |
| 5.7.2.5 | MF / DF.CIA.ESIGN / EF.CD (Certificate Directory) | 130 |
| 5.8 | Die Organisationsspezifische Authentisierungsanwendung | 133 |
| 5.8.1 | Dateistruktur und Dateinhalt | 134 |
| 5.8.2 | DF.AUTO (Organization-specific Authentication Application) | 134 |
| 5.8.2.1 | MF / DF.AUTO / PrK.HP.AUTO.R3072 | 136 |
| 5.8.2.2 | MF / DF.AUTO / PIN.AUTO | 138 |
| 5.8.2.3 | MF / DF.AUTO / PIN.SO | 141 |
| 5.8.2.4 | MF / DF.AUTO / EF.C.HP.AUTO1.R3072 und MF / DF.AUTO / EF.C.HP.AUTO2.R3072 | 144 |
| 5.8.2.5 | Sicherheitsumgebungen | 147 |
| 5.8.2.6 | Vorgaben für die Nutzung von DF.AUTO | 147 |
| 5.9 | Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des HBA | 149 |
| 6 | Anhang A – Verzeichnisse | 150 |
| 6.1 | - Abkürzungen | 150 |
| 6.2 | - Glossar | 153 |
| 6.3 | - Abbildungsverzeichnis | 154 |
| 6.4 | - Tabellenverzeichnis | 154 |
| 6.5 | - Referenzierte Dokumente | 158 |
| 6.5.1 | - Dokumente der gematik | 158 |
| 6.5.2 | - Weitere Dokumente | 159 |

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:

- Die EU-Verordnung Nr. 910/2014 (eIDAS)
- die DIN-Spezifikation für Chipkarten mit digitaler Signatur
- die ESIGN-Spezifikation für elektronische Signaturen
- die zugehörigen 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 |
|---|---|
| AUT(<code>oid_cvc_fl_cms</code> , '00010000000000') | <code>flagCMS.15</code> |
| AUT(<code>oid_cvc_fl_ti</code> , '00010000000000') OR AUT(<code>oid_cvc_fl_ti</code> , '00008000000000') | <code>flagTI.15</code> OR <code>flagTI.16</code> |
| PWD(PIN) AND [AUT(<code>oid_cvc_fl_cms</code> , '00010000000000') OR AUT(<code>oid_cvc_fl_ti</code> , '00008000000000')] | PWD(PIN) AND [<code>flagCMS.15</code> OR <code>flagTI.16</code>] |
| SmMac(<code>oid_cvc_fl_cms</code> , '00800000000000') | SmMac(<code>flagCMS.08</code>) |

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

- 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:
 - i. Falls eine Kommandonachricht keine Kommandodaten enthält, dann ist es zulässig den Term SmCmdEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
 - ii. 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:
 - i. Falls für eine Zugriffsart keine Kommandodaten existieren, dann ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmCmdEnc zu verwenden.
 - ii. Falls für eine Zugriffsart keine Antwortdaten existieren, dann ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmRspEnc zu verwenden.

1.5.2 Verwendung von Schlüsselworten

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <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 Option_Erstellung_von_Testkarten

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.
- Unterstützung von Onboard-RSA-Schlüsselgenerierung

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 RSA CV-Zertifikate

A_15175 - K_HBA: Vorhandensein asymmetrischer Kryptographiealgorithmus RSA für CV-Zertifikate

Für einen HBA KANN für das Objektsystem ein COS verwendet werden

1. das die Option_RSA_CVC implementiert hat.
2. das die Option_RSA_CVC nicht implementiert hat.[<=]

4.3 Unterstützung Onboard-RSA-Schlüsselgenerierung

Card-G2-A_3848 - K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung

Das COS eines HBA MUSS die Option_RSA_KeyGeneration implementieren.[<=]

4.4 Unterstützung optionaler Funktionspakete

4.4.1 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.

[<=]

4.4.2 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.

[<=]

4.4.3 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.

[<=]

4.4.4 Symmetrischer Kryptographiealgorithmus DES (optional)

Falls ein HBA den symmetrischen Algorithmus DES nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_DES implementiert hat.

Card-G2-A_3674 - K_HBA: Vorhandensein symmetrischer Kryptographiealgorithmus DES

Für einen HBA KANN für das Objektsystem ein COS verwendet werden,

1. das die Option_DES implementiert hat.
2. das die Option_DES nicht implementiert hat.

[<=]

4.5 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.

[<=]

4.5.1 Attribute eines Ordners

Card-G2-A_2033-01 - K_Initialisierung: Ordnerattribute

Enthält eine Tabelle mit Ordnerattributen einen oder mehrere applicationIdentifier (AID), dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen

[<=]

Card-G2-A_3624 - K_Initialisierung: Herstellerspezifischer ApplicationIdentifier

Enthält eine Tabelle mit Ordnerattributen keinen *applicationIdentifier* (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.

[<=]

Card-G2-A_3625 - K_Initialisierung: Fehlender FileIdentifier

Enthält eine Tabelle mit Ordnerattributen keinen *fileIdentifier* (FID), 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.

[<=]

Card-G2-A_3626 - K_Initialisierung: Herstellerspezifischer FileIdentifier

Enthält eine Tabelle mit Ordnerattributen keinen *fileIdentifier* (FID), so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden.

[<=]

4.5.2 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.

[<=]

4.6 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:

- Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.
- 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.
- 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.

[<=]

4.7 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 herstellersizifische Personalisierungsprozesse:

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

Zur Unterstützung herstellersizifischer 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.

[<=]

Für die Initialisierung und Personalisierung asymmetrischer Schlüssel gelten folgende Anforderungen:

Card-G2-A_3525 - K_Initialisierung: Schlüsselgenerierung auf der Karte

Der HBA MUSS die Generierung von asymmetrischen Schlüsselpaaren auf der Karte ermöglichen.

[<=]

Card-G2-A_3526 - K_Initialisierung: Weitere Verfahren zur Personalisierung von Schlüsseln

Der HBA KANN andere Verfahren als das in Card-G2-A_3525 genannte zur Personalisierung asymmetrischer Schlüsselpaare unterstützen.

[<=]

Card-G2-A_3523 - K_Personalisierung: Schlüsselgenerierung auf der Karte

Wenn ein privater Schlüssel für den HBA zu personalisieren ist, dann MUSS das Schlüsselpaar von der Smartcard selbst erzeugt werden. Es MUSS sichergestellt sein, dass der private Teil des Schlüssels die Smartcard nie verlässt.

[<=]

4.8 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 CUPs) und einer Karte beschrieben, die bei der Ausgabe der Karte angelegt werden müssen.

Card-G2-A_3005 - Absicherung der Kartenadministration

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

[<=]

Card-G2-A_3590 - Symmetrische Kartenadministration

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

[<=]

Card-G2-A_3591 - Schlüsselspeicherung

Der Kartenherausgeber MUSS sicherstellen, dass die Schlüssel zur Absicherung der Kartenadministration während der gesamten Nutzungsdauer des HBA sicher verwahrt werden und bei Bedarf an ein Kartenadministrationssystem (z.B. ein CUPs) übergeben werden können.

[<=]

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_2040-01 - 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_2044-01, Card-G2-A_3627, 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_2042-01 - K_Initialisierung: Inhalt persistentPublicKeyList

Das Attribut *persistentPublicKeyList* MUSS den Schlüssel 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 Signaturprüfchlüssel einer Root-CA mittels Linkzertifikaten persistent importierbar sind.

[<=]

Card-G2-A_3266-01 - K_Initialisierung: Wert von pointInTime

Der Hersteller des Objektsystems MUSS das Attribut *pointInTime* im Rahmen der Initialisierung auf den Wert von CED (Certificate Effective Date) aus dem selbst signierten CV-Zertifikat zu PuK.RCA.CS setzen.

[<=]

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_2044-01 - K_Personalisierung und K_Initialisierung: TC1 Byte im ATR

Der ATR SOLL ein TC1 Byte mit dem Wert 'FF' enthalten.

[<=]

Card-G2-A_3627 - K_Personalisierung und K_Initialisierung: T0 Byte im ATR

Wenn der ATR ein TC1 Byte mit dem Wert 'FF' enthält, 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

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

[<=]

5.2 Allgemeine Struktur

Abb_HBA_ObjSys_001 zeigt die allgemeine Struktur der Objekte eines HBA.

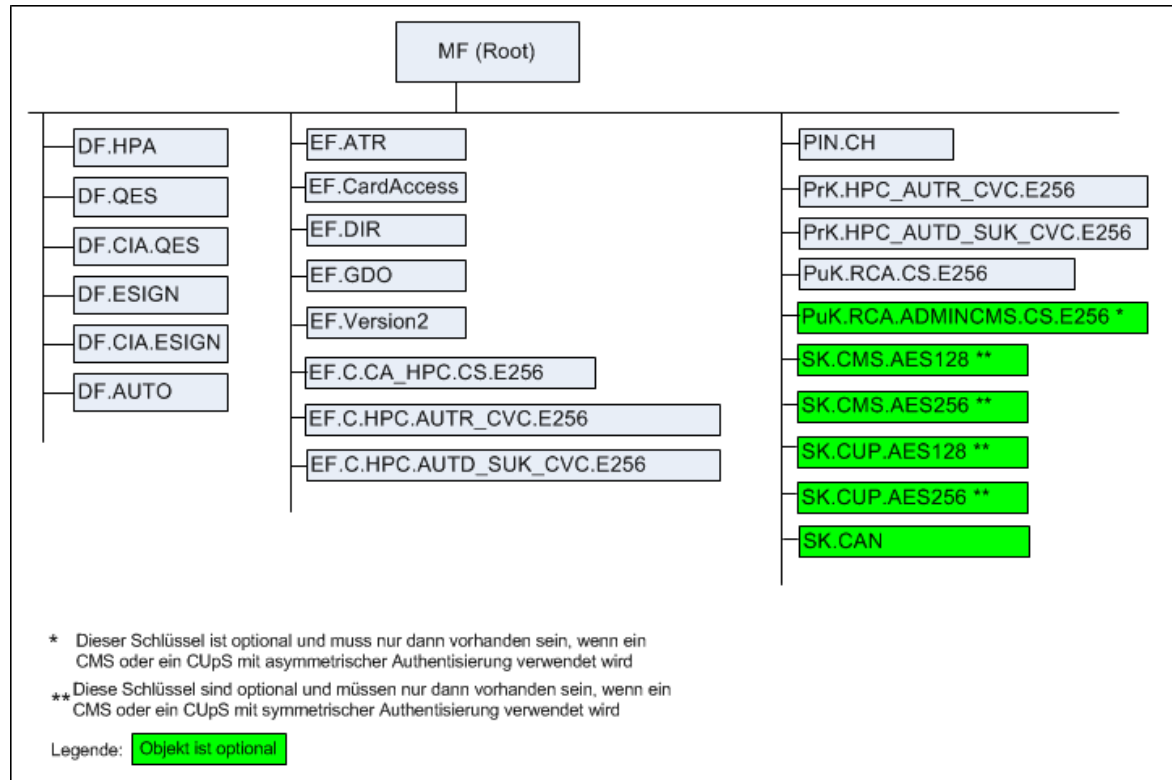


Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA

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 | |
| <i>applicationIdentifier</i> | 'D27600014601' | |
| <i>fileIdentifier</i> | '3F 00' | falls vorhanden |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |

| | | |
|---|----------------------|------------------|
| | | |
| <i>shareable</i> | 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_2048-01 - 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 |
|---|---|------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '2F 01' | siehe Hinweis 6: |
| <i>shortFileIdentifier</i> | '1D'= 29 | |
| <i>numberOfOctet</i> | herstellerspezifisch | |
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] | 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 | |
| <i>fileIdentifier</i> | '01 1C' | siehe Hinweis 6: |
| <i>shortFileIdentifier</i> | '1C' = 28 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>numberOfOctet</i> | passend zum Inhalt | |
| <i>positionLogicalEndOfFile</i> | passend zum Inhalt | |
| <i>shareable</i> | 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_3628 - K_Initialisierung: Inhalt der Records von EF.DIR

Für jede im Objektsystem vorhandene Anwendung MUSS die Datei einen eigenen Record besitzen, der den ApplicationIdentifier (AID) dieser Anwendung im Format '61-L₆₁-{4F-L_{4F}-AID}' enthält.

Zu jedem Record der Datei MUSS es auf der Karte eine Anwendung geben, deren AID durch diesen Record beschrieben ist.

Record 1 des EF.DIR MUSS den AID des MF enthalten.

[<=]

Card-G2-A_2055-01 - 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 | |
| <i>fileIdentifier</i> | '2F 00' | Siehe Hinweis 8: |
| <i>shortFileIdentifier</i> | '1E' = 30 | Siehe Hinweis 8: |
| <i>numberOfOctet</i> | '00 BE' Oktett = 190 Oktett | |
| <i>maxNumRecords</i> | 10 Records | |
| <i>maxRecordLength</i> | 32 Oktett | |
| <i>flagRecordLCS</i> | False | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>recordList</i> Record 1 Record 2 und folgende | '61- 08- (4F 06 D27600014601)' '61-L ₆₁ -{4F-L _{4F} -AID}' | AID.MF |

| | | |
|---|--|-------------------|
| | für alle Applikationen im Objektsystem | |
| 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 |
|--|---------------------------------|---------------------|
| Objektyp | 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_2058-01 - 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 |
|---------------------------------|--|-----------|
| <i>positionLogicalEndOfFile</i> | '00 0C' Oktett = 12 Oktett | |
| <i>body</i> | Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] | |

[<=]

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_G2.1] beschrieben.

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

Card-G2-A_2059-01 - 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 | |
| <i>fileIdentifier</i> | '2F 11' | |
| <i>shortFileIdentifier</i> | '11' = 17 | |
| <i>numberOfOctet</i> | '00 3C' Oktett = 60 Oktett | |
| <i>positionLogicalEndOfFile</i> | passend zum Inhalt | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] | |
| 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.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 10: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256

| Attribute | Wert | Bemerkung |
|----------------------------|-------------------------------|-----------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '2F 07' | |
| <i>shortFileIdentifier</i> | '07' = 7 | |

| | | |
|--|---------------------------------|---------------------|
| | | |
| <i>numberOfOctet</i> | '00 DC' Oktett = 220 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird 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 11: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256

| Attribute | Wert | Bemerkung |
|---|--|----------------------------------|
| <i>positionLogicalEndOfFile</i> | '00 DC' Oktett = 220 Oktett | |
| <i>body</i> | C.CA_HPC.CS.E256 gemäß [gemSpec_PKI#6.7.1] | siehe [gemSpec_COS] |
| <i>body</i> 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] |

[<=]

5.3.7 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 zugehörige 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 12: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF /
EF.C.HPC.AUTR_CVC.E256**

| Attribute | Wert | Bemerkung |
|---------------------------------|---------------------------------|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '2F 06' | |
| <i>shortFileIdentifier</i> | '06' = 6 | |
| <i>numberOfOctet</i> | '00 DE' Oktett = 222 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird 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 13: Tab_HBA_ObjSys_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|---|-----------|
| <i>positionLogicalEndOfFile</i> | '00 DE' Oktett = 222 Oktett | |
| <i>body</i> | C.HPC.AUTR_CVC.E256 gemäß [gemSpec_PKI] | |

[<=]

5.3.8 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/gSMC-KT 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 zugehörnde 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 14: Tab_HBA_ObjSys_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|---------------------------------|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '2F 09' | |
| <i>shortFileIdentifier</i> | '09'= 9 | |
| <i>numberOfOctet</i> | '00 DE' Oktett = 222 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird 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 15: 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 | |

[<=]

5.3.9 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 16: Tab_HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH

| Attribute | Wert | Bemerkung |
|-----------|----------------|-----------|
| Objektyp | Passwortobjekt | |

| <i>pwdIdentifier</i> | '01' = 1 | |
|---|---------------------------------|---------------------|
| <i>secret</i> | undefiniert | wird personalisiert |
| <i>minimumLength</i> | 6 | |
| <i>maximumLength</i> | 8 | |
| <i>startRetryCounter</i> | 3 | |
| <i>retryCounter</i> | 3 | |
| <i>transportStatus</i> | Transport-PIN | |
| <i>flagEnabled</i> | True | |
| <i>startSsec</i> | unendlich | |
| <i>PUK</i> | undefiniert | wird personalisiert |
| <i>pukUsage</i> | 10 | |
| <i>lifeCycleStatus</i> | „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 17: Tab_HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH

| Attribute | Wert | Bemerkung |
|------------------------|------------------------------------|---|
| <i>secret</i> | PIN-Wert gemäß [gemSpec_PINPUK_TI] | wird personalisiert |
| <i>transportStatus</i> | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis 22: |
| <i>PUK</i> | 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 den HBA

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

[<=]

5.3.10 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 18: 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)“ | |
| accessRuleSession keys | 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 19: Tab_HBA_ObjSys_099 Personalisierte Attribute von MF /
PrK.HPC.AUTR_CVC.E256**

| Attribute | Wert | Bemerkung |
|----------------------|--------------------|-----------|
| <i>keyAvailable</i> | True | |
| <i>privateElcKey</i> | keyData = Wildcard | |

[<=]

5.3.11 MF / PrK.HPC.AUTD_SUK_CVC.E256

PrK.HPC.AUTD_SUK_CVC.E256 ist der globale private Schlüssel für die Kryptographie
mit elliptischen Kurven für C2C-Authentisierungen zwischen HBA/gSMC-KT 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 20: Tab_HBA_ObjSys_024 Initialisierte Attribute von MF /
PrK.HPC.AUTD_SUK_CVC.E256**

| Attribute | Wert | Bemerkung |
|--------------------------------|---|---------------------|
| Objektyp | privates Schlüsselobjekt, ELC 256 | |
| <i>keyIdentifier</i> | '09' = 9 | |
| <i>privateElcKey</i> | domainparameter = brainpoolP256r1 | |
| <i>privateElcKey</i> | keyData = AttributNotSet | wird personalisiert |
| <i>keyAvailable</i> | Wildcard | |
| <i>listAlgorithmIdentifier</i> | Ein Wert aus der Menge {elcSessionkey4SM, elcAsynchronAdmin} | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |

| | | |
|---|----------------------|-------------------|
| | | |
| <i>numberScenarion</i> | 0 | |
| <i>accessRuleSessionkeys</i> | 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 21: Tab_HBA_ObjSys_101 Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256

| Attribute | Wert | Bemerkung |
|---------------|--------------------|-----------|
| keyAvailable | True | |
| privateElcKey | keyData = Wildcard | |

[<=]

5.3.12 Sicherheitsanker zum Import von CV-Zertifikaten

Ein Sicherheitsanker ist ein öffentliches Signaturprüfobjekt zum Import von CV-Zertifikaten und enthält den öffentlichen Schlüssel einer Root-CA für CV-Zertifikate der Telematikinfrastruktur.

5.3.12.1 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_2078-01 - 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 22: Tab_HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256

| Attribute | Wert | Bemerkung |
|--|--|-------------------|
| Objekttyp | öffentliches ELC Signaturprüfobjekt | |
| <p>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.</p> | | |
| <i>keyIdentifier</i> | E 256 Root-CA-Kennung (5 Bytes) Erweiterung (3 Bytes) | |
| <i>expirationDate</i> | 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 00E3' | siehe Hinweis 32: |
| <i>publicKey</i> | Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP#gemSpec_CVC_TSP#4.5] | |
| <p>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.</p> | | |
| <i>oid</i> | ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2} | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>accessRulesPublicSignatureVerificationObject</i> | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: Delete → ALWAYS AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS | |
| <i>accessRulesPublicAuthenticationObject</i> | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: Delete → ALWAYS External Authenticate → ALWAYS | siehe Hinweis 31: |
| 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 (32) 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_3327-01 - 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 23: Tab_HBA_ObjSys_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

| Attribute | Wert | Bemerkung |
|-----------------------|---|--|
| <i>publicKey</i> | Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-CVC-CA | personalisieren gemäß [gemSpec_TK#3.1.2] |
| <i>keyIdentifier</i> | E 256 Root-CA-Kennung (5 Bytes) Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels | |
| CHAT | <ul style="list-style-type: none"> OID_{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 00E3' | |
| <i>expirationDate</i> | Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels | |

[<=]

5.3.13 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.

5.3.13.1 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_3016-01 - 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 24: Tab_HBA_ObjSys_082 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

| Attribute | Wert | Bemerkung |
|--|---|---------------------|
| Objektyp | 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 | <ul style="list-style-type: none"> OID_{flags} = oid_cvc_fl_cms flagList = 'FF BFFF FFFF FFFF' | siehe Hinweis 34: |
| 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 | Für alle relevanten Interfacesarten und alle relevanten Werte von lifeCycleStatus gilt: Delete → AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS | |
| accessRulesPublicAuthenticationObject | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: Delete → ALWAYS | siehe Hinweis 31: |
| 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 (33) Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate

Hinweis (34) 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

Bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 MÜSSEN 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 25: Tab_HBA_ObjSys_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

| Attribute | Wert | Bemerkung |
|--|--|-----------|
| <i>publicKey</i> | Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] | |
| <i>publicKey</i> Option_Erstellung _von_Testkarten | Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-Admin-CVC-Root | |
| CHAT | <ul style="list-style-type: none"> 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 | |

[<=]

5.3.14 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.

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

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

5.3.14.1 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_2080-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128

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

Tabelle 26: 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 | |
| General Authenticate | ALWAYS | |
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 36: |
| 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 36: |
| 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 (35) 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 (36) 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 27: Tab_HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128

| Attribute | Wert | Bemerkung |
|---------------|---|-----------|
| <i>encKey</i> | Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4] | |
| <i>macKey</i> | Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4] | |

[<=]

5.3.14.2 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_2081-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256

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

Tabelle 28: Tab_HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256

| Attribute | Wert | Bemerkung |
|----------------------|--|---------------------|
| Objekttyp | Symmetrisches Authentisierungsobjekt | |
| <i>keyType</i> | AES-256 | |
| <i>keyIdentifier</i> | '18' = 24 | |
| <i>encKey</i> | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES- | wird personalisiert |

| | | |
|---|---|---------------------|
| | Schlüssel mit 256 Bit | |
| <i>macKey</i> | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| <i>numberScenario</i> | 0 | |
| <i>algorithmIdentifier</i> | aesSessionkey4SM, siehe [gemSpec_COS] | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>accessRuleSession keys</i> | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | |
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 36: |
| 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 36: |
| 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 | |

[<=]

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 29: Tab_HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256

| Attribute | Wert | Bemerkung |
|---------------|---|-----------|
| <i>encKey</i> | Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4] | |
| <i>macKey</i> | Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4] | |

[<=]

5.3.14.3 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_3293-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128

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

Tabelle 30: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128

| Attribute | Wert | Bemerkung |
|------------------------------|---|---------------------|
| Objektyp | Symmetrisches Authentisierungsobjekt | |
| <i>keyType</i> | AES-128 | |
| <i>keyIdentifier</i> | '03' = 3 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>encKey</i> | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| <i>macKey</i> | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| <i>numberScenario</i> | 0 | |
| <i>algorithmIdentifier</i> | aesSessionkey4SM, siehe [gemSpec_COS] | |
| <i>accessRuleSessionkeys</i> | irrelevant | |

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

| Zugriffsart | Zugriffsbedingung | Bemerkung |
|----------------------|-------------------|-----------|
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | |

| | | |
|---|----------------------|-------------------|
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 36: |
| 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 36: |
| 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 | |

[<=]

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 31: Tab_HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES128

| Attribute | Wert | Bemerkung |
|---------------|---|-----------|
| <i>encKey</i> | Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4] | |
| <i>macKey</i> | Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4] | |

[<=]

5.3.14.4 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_3295-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256

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

Tabelle 32: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256

| Attribute | Wert | Bemerkung |
|---|---|---------------------|
| Objektyp | Symmetrisches Authentisierungsobjekt | |
| keyType | AES-256 | |
| keyIdentifier | '04' = 4 | |
| lifeCycleStatus | „Operational state (activated)“ | |
| encKey | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| macKey | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| numberScenario | 0 | |
| algorithmIdentifier | aesSessionkey4SM, siehe [gemSpec_COS] | |
| accessRuleSessionkeys | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | |
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 36: |
| 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 36: |
| 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 | |

[<=]

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 33: Tab_HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES256

| Attribute | Wert | Bemerkung |
|---------------|---|-----------|
| <i>encKey</i> | Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4] | |
| <i>macKey</i> | Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4] | |

[<=]

5.3.15 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 34: Tab_HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN

| Attribute | Wert | Bemerkung |
|----------------------|---------------------------------------|-----------|
| Objekttyp | symmetrisches Kartenverbindungsobjekt | |
| <i>keyIdentifier</i> | '02' = 2 | |

| | | |
|---|--|-----------|
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| Can | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für ein Schlüsselobjekt SK.CAN | |
| <i>algorithmIdentifier</i> | id-PACE-ECDH-GM-AES-CBC-CMAC-128 | |
| <i>accessRuleSessionkeys</i> | 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 (37) 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 35: Tab_HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN

| Attribute | Wert | Bemerkung |
|------------|-------------------------------|------------------------|
| <i>can</i> | 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.

[<=]

5.3.16 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.

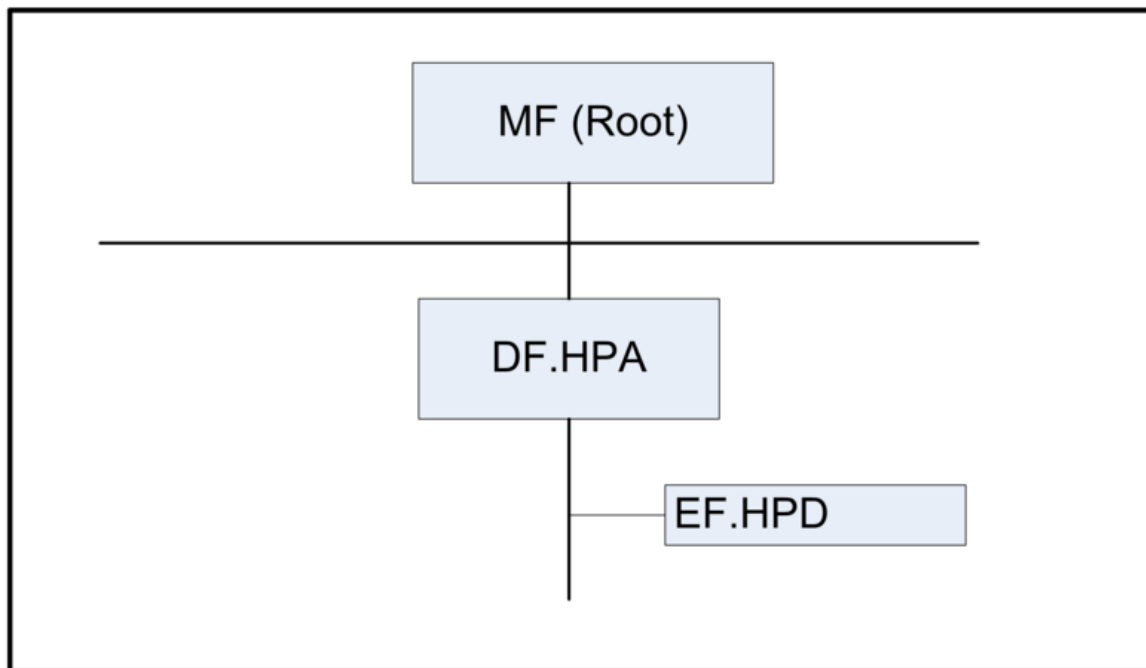


Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA

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 36: Tab_HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA

| Attribute | Wert | Bemerkung |
|---|---------------------------------|-----------|
| Objektyp | Ordner | |
| <i>applicationIdentifier</i> | 'D27600014602' | |
| <i>fileIdentifier</i> | – | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | 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 (38) 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 Heilberuf 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 37: Tab_HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD

| Attribute | Wert | Bemerkung |
|---|---------------------------------|-------------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'D0 01' | |
| <i>shortFileIdentifier</i> | '01' = 1 | |
| <i>numberOfOctet</i> | '08 00' Oktett = 2048 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | 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 | PWD(PIN.CH) | |

| | | |
|---|-----------------------------|-----------|
| WRITE BINARY | | |
| 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 (39) 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 Dateinhalt

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

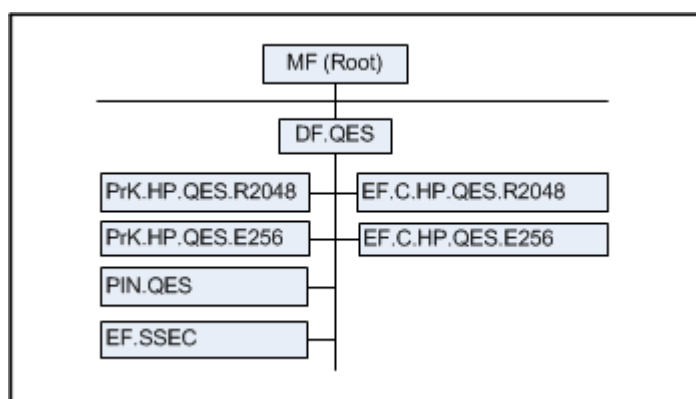


Abbildung 3 Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung

Die QES-Anwendung beinhaltet EFs für die X.509-QES-Zertifikate für die Kryptographie mit RSA und mit elliptischen Kurven. 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 38: Tab_HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES

| Attribute | Wert | Bemerkung |
|------------------------------|---------------------------------|-------------------|
| Objekttyp | Ordner | |
| <i>applicationIdentifier</i> | 'D276000066 01' | siehe Hinweis 40: |
| <i>fileIdentifier</i> | – | siehe Hinweis 41: |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |

| | | |
|---|----------------------|-------------------|
| | | |
| <i>shareable</i> | 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 (40) 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 (41) Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis (42) herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [ISO7816-4#8.1.1]

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_2085-01 - 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 39: Tab_HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048

| Attribute | Wert | Bemerkung |
|--|--|---------------------|
| Objektyp | privates Schlüsselobjekt RSA 2048 | |
| keyIdentifier | '04' = 4 | |
| privateKey | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit | wird personalisiert |
| keyAvailable | WildCard | |
| listAlgorithmIdentifier | alle Werte aus der Menge { signPSS } | |
| 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) | siehe Hinweis 48: |
| Delete | herstellerspezifisch | siehe Hinweis 46: |
| andere | NEVER | |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| PSO Comp Dig Sig | PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc | siehe Hinweis 47: |

| | | |
|---|--|-------------------|
| | AND SmRespEnc | |
| 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) | siehe Hinweis 48: |
| Delete | herstellerspezifisch | siehe Hinweis 46: |
| andere | NEVER | |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| PSO Compute Digital Signature | PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRspEnc | siehe Hinweis 47: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| 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) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Hinweis (46) Die konkrete Zugriffsregel muss durch den Objektsystemhersteller in Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS) festgelegt werden.

*Hinweis (47) Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115].
Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)*

*Hinweis (48) Modus für Einzel- oder Stapelsignatur ohne Geräteauthentisierung gemäß PIN.QES
Start Security Status Evaluation Counter.*

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

| Attribute | Wert | Bemerkung |
|---------------------|-----------------------|---------------------|
| <i>privateKey</i> | Moduluslänge 2048 Bit | wird personalisiert |
| <i>keyAvailable</i> | 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 Heilberufers (PrK.HP.QES.R2048) gemäß EU-Verordnung Nr. 910/2014 (eIDAS) 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_2088-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PIN.QES

PIN.QES MUSS die in Tab_HBA_ObjSys_037 dargestellten Werte besitzen.

Tabelle 41: Tab_HBA_ObjSys_037 Initialisierte Attribute von MF / DF.QES / PIN.QES

| Attribute | Wert | Bemerkung |
|--------------------------|----------------|---------------------|
| Objektyp | Passwortobjekt | |
| <i>pwdIdentifier</i> | '01' = 1 | |
| <i>secret</i> | undefiniert | wird personalisiert |
| <i>minimumLength</i> | 6 | |
| <i>maximumLength</i> | 8 | |
| <i>startRetryCounter</i> | 3 | |
| <i>retryCounter</i> | 3 | |

| | | |
|---|--|--------------------------------|
| <i>transportStatus</i> | Transport-PIN | |
| <i>flagEnabled</i> | True | |
| <i>Start Security Status Evaluation Counter</i> | SE # 1: $1 \leq \text{SSEC} \leq 250$ SE # 2: $1 \leq \text{SSEC} \leq 250$ | Werte wie in EF.SSEC angezeigt |
| PUK | undefiniert | wird personalisiert |
| <i>pukUsage</i> | 10 | |
| <i>lifeCycleStatus</i> | „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 42: Tab_HBA_ObjSys_111 Personalisierte Attribute von MF / DF.QES / PIN.QES

| Attribute | Wert | Bemerkung |
|------------------------|------------------------------------|---|
| <i>secret</i> | PIN-Wert gemäß [gemSpec_PINPUK_TI] | wird personalisiert |
| <i>transportStatus</i> | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis 50: |
| <i>PUK</i> | 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 43: Tab_HBA_ObjSys_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC

| Attribute | Wert | Bemerkung |
|---|---|-----------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'D0 05' | |
| <i>shortFileIdentifier</i> | '05' = 5 | |
| <i>numberOfOctet</i> | '002E' Oktett = 46 Oktett | |
| <i>positionLogical EndOfFile</i> | '002E' Oktett = 46 Oktett | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | Inhalt gemäß den Werten für <i>Start SecurityStatus Evaluation Counter</i> 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 SE#1, SE#2 | 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 | AUT_PACE | |
| 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_2090-01 - K_Initialisierung: Inhalt von EF.SSEC

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

Tabelle 44: 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' | 'xx' | SSEC-Maximalwert, z.B. 250 |
| | | 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.

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 Heilberufers PuK.HP.QES.R2048 für die qualifizierte elektronische Signatur gemäß EU-Verordnung Nr. 910/2014 (eIDAS). Das zugehörige private Schlüsselobjekt PrK.HP.QES.R2048 ist im Kapitel 5.5.2.1 definiert.

Card-G2-A_2091-01 - 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 45: Tab_HBA_ObjSys_040 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

| Attribute | Wert | Bemerkung |
|---|---------------------------------|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C0 00' | |
| <i>shortFileIdentifier</i> | '10' = 16 | |
| <i>numberOfOctet</i> | '07 6C' Oktett = 1900 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Delete | herstellerspezifisch | siehe Hinweis 53: |
| Read Binary | ALWAYS | |
| Erase Binary Set Logical EOF Update Binary Write Binary | herstellerspezifisch | siehe Hinweis 53: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| 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 53: |
| Read Binary | AUT_PACE | |
| Erase Binary Set Logical EOF Update Binary Write Binary | herstellerspezifisch | siehe Hinweis 53: |

| | | |
|--|----------------------------------|-------------------|
| andere | NEVER | |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Delete | herstellerspezifisch | siehe Hinweis 53: |
| Read Binary | SmMac(flagT1.55) AND SmRspEnc | |
| Erase Binary Set Logical EOF Update Binary Write Binary | herstellerspezifisch | siehe Hinweis 53: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| 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) Die konkrete Zugriffsregel muss durch den Objektsystemhersteller, der diese Option umsetzt, in Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS) 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 46: Tab_HBA_ObjSys_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-----------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>body</i> | 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 / PrK.HP.QES.E256

PrK.HP.QES.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven 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.E256 ist in C.HP.QES.E256 (siehe Kapitel 5.5.2.7) enthalten.

Card-G2-A_3629-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

PrK.HP.QES.E256 MUSS die in Tab_HBA_ObjSys_160 dargestellten initialisierten Attribute besitzen.

Tabelle 47: Tab_HBA_ObjSys_160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256

| Attribute | Wert | Bemerkung |
|--|---|---------------------|
| Objektyp | privates Schlüsselobjekt, ELC 256 | |
| keyIdentifier | '06' = 6 | |
| lifeCycleStatus | „Operational state (activated)“ | |
| privateElcKey | domainparameter = brainpoolP256r1 | wird personalisiert |
| privateElcKey | keyData = AttributNotSet | |
| keyAvailable | Wildcard | |
| listAlgorithmIdentifier | alle Werte aus der Menge, [gemSpec_COS] {signECDSA} | |
| | | |
| accessRuleSessionkeys | irrelevant | |
| 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) | siehe Hinweis 48: |
| Delete | herstellerspezifisch | siehe Hinweis 46: |
| andere | NEVER | |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| PSO Comp Dig Sig | PWD(PIN.QES) AND SmMac(flagT1.55) AND SmCmdEnc AND SmRespEnc | siehe Hinweis 47: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |

| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
|--|--|-------------------|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| 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) | siehe Hinweis 48: |
| Delete | herstellerspezifisch | siehe Hinweis 46: |
| andere | NEVER | |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| PSO Compute Digital Signature | PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRspEnc | siehe Hinweis 47: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER | |

[<=]

Card-G2-A_3630 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

Bei der Personalisierung von PrK.HP.QES.E256 MÜSSEN die in Tab_HBA_ObjSys_161 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 48: Tab_HBA_ObjSys_161 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

| Attribute | Wert | Bemerkung |
|----------------------|--------------------|-----------|
| <i>keyAvailable</i> | true | |
| <i>privateElcKey</i> | keyData = Wildcard | |

[<=]

5.5.2.6 MF / DF.QES / EF.C.HP.QES.E256

Die transparente Datei EF.C.HP.QES.E256 enthält das X.509-Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel des Heilberufers PuK.HP.QES.E256 für die qualifizierte elektronische Signatur gemäß EU-Verordnung Nr. 910/2014 (eIDAS). Das zugehörige private Schlüsselobjekt PrK.HP.QES.E256 ist im Kapitel 5.5.2.6 definiert.

Card-G2-A_3631 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

EF.C.HP.QES.E256 MUSS die in Tab_HBA_ObjSys_162 dargestellten initialisierten Attribute besitzen.

Tabelle 49: Tab_HBA_ObjSys_162 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

| Attribute | Wert | Bemerkung |
|--|---------------------------------|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C0 06' | |
| <i>shortFileIdentifier</i> | '06' = 6 | |
| <i>numberOfOctet</i> | '0B B8' Oktett = 3000 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | wird personalisiert |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Delete | herstellerspezifisch | siehe Hinweis 53: |
| Read Binary | ALWAYS | |
| Erase Binary Set Logical EOF Update Binary Write Binary | herstellerspezifisch | siehe Hinweis 53: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |

| Zugriffsart | Zugriffsbedingung | Bemerkung |
|--|----------------------------------|-------------------|
| 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 53: |
| Read Binary | AUT_PACE | |
| Erase Binary Set Logical EOF Update Binary Write Binary | herstellerspezifisch | siehe Hinweis 53: |
| andere | NEVER | |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Delete | herstellerspezifisch | siehe Hinweis 53: |
| Read Binary | SmMac(flagTI.55) AND SmRspEnc | |
| Erase Binary Set Logical EOF Update Binary Write Binary | herstellerspezifisch | siehe Hinweis 53: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |

[<=]

Hinweis (57) 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_3632 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

Bei der Personalisierung von EF.C.HP.QES.E256 MÜSSEN die in Tab_HBA_ObjSys_163 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 64: Tab_HBA_ObjSys_163 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-----------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>body</i> | C.HP.QES.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.QES.E256 | |

[<=]

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.

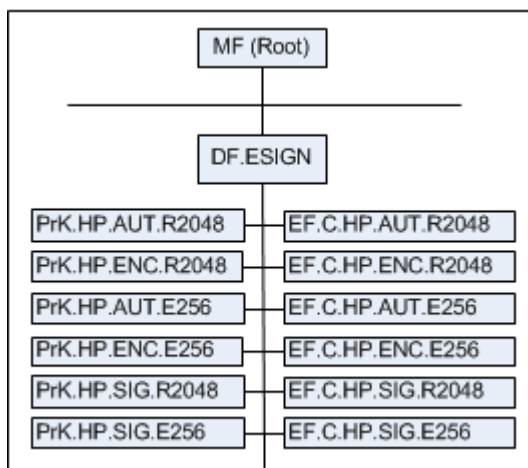


Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN

5.6.2 MF / DF.ESIGN (Krypto-Anwendung 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 50: Tab_HBA_ObjSys_045 Initialisierte Attribute von MF / DF.ESIGN

| Attribute | Wert | Bemerkung |
|-----------|--------|-----------|
| Objektyp | Ordner | |

| | | |
|---|---------------------------------|-------------------|
| | | |
| <i>applicationIdentifier</i> | 'A000000167 455349474E' | siehe Hinweis 59: |
| <i>fileIdentifier</i> | – | siehe Hinweis 60: |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | 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 (61) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.

Hinweis (62) Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis (63) herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1].

Hinweis (64) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.6 im Allgemeinen irrelevant.

Hinweis (65) 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_2098-01 - 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 51: 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 Modulslänge 2048 Bit | wird personalisiert |
| keyAvailable | WildCard | |
| listAlgorithmIdentifier | alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, 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 67: |
| 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 67: |
| 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 (66) 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 (67) 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 52: Tab_HBA_ObjSys_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

| Attribute | Wert | Bemerkung |
|---------------------|-----------------------|---------------------|
| <i>privateKey</i> | Moduluslänge 2048 Bit | wird personalisiert |
| <i>keyAvailable</i> | 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 53: Tab_HBA_ObjSys_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

| Attribute | Wert | Bemerkung |
|--|---|---|
| Objektyp | privates Schlüsselobjekt, RSA 2048 | |
| <i>keyIdentifier</i> | '03' = 3 | |
| <i>privateKey</i> | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| <i>keyAvailable</i> | Wildcard | |
| <i>listAlgorithmIdentifier</i> | alle Werte aus der Menge, siehe [gemSpec_COS] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5} | |
| <i>lifeCycleStatus</i> | „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 (68) 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 (69) 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 54: Tab_HBA_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

| Attribute | Wert | Bemerkung |
|---------------------|-----------------------|---------------------|
| <i>privateKey</i> | Moduluslänge 2048 Bit | wird personalisiert |
| <i>keyAvailable</i> | 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.HP.AUT.R2048. Das zugehörnde 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 55: Tab_HBA_ObjSys_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

| Attribute | Wert | Bemerkung |
|---------------------------------|-------------------------------|-----------|
| Objekttyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C5 00' | |
| <i>shortFileIdentifier</i> | '01' = 1 | |
| <i>numberOfOctet</i> | '07 6C' Oktett = 1900 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |

| | | |
|---|--------------------------------------|---------------------|
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird 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 (70) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (71) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

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

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-----------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>body</i> | 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.HP.ENC.R2048. Das zugehörnde private Schlüsselobjekt PrK.HP.ENC.R2048 ist im Kapitel 5.6.2.2 definiert.

Card-G2-A_2110-01 - 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 57: Tab_HBA_ObjSys_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

| Attribute | Wert | Bemerkung |
|---------------------------------|-------------------------------|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C2 00' | |
| <i>shortFileIdentifier</i> | '02' = 2 | |
| <i>numberOfOctet</i> | '07 6C' Oktett = 1900 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | wird personalisiert |
| <i>flagTransactionMode</i> | True | |

| | | |
|--|--------------------------------------|---------------------|
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 73: |
| Read Binary | ALWAYS | |
| Set Logical EOF Write Binary | AUT_CMS OR AUT_CUP | siehe Hinweis 73: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| 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 73: |
| Read Binary | AUT_PACE OR AUT_CMS OR AUT_CUP | |
| Set Logical EOF Write Binary | AUT_CMS OR AUT_CUP | siehe Hinweis 73: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |

[<=]

Hinweis (72) 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 (73) 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 58: Tab_HBA_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

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

[<=]

5.6.2.5 MF / DF.ESIGN / PrK.HP.AUT.E256

PrK.HP.AUT.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HP.AUT.E256 ist in C.HP.AUT.E256 (siehe Kapitel 5.6.2.7) enthalten.

Card-G2-A_3639-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

PrK.HP.AUT.E256 MUSS die in Tab_HBA_ObjSys_170 dargestellten initialisierten Attribute besitzen.

Tabelle 59: Tab_HBA_ObjSys_170 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

| Attribute | Wert | Bemerkung |
|--------------------------------|---|---------------------|
| Objektyp | privates Schlüsselobjekt, ELC 256 | |
| <i>keyIdentifier</i> | '06' = 6 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>privateElcKey</i> | <i>domainparameter</i> = <i>brainpoolP256r1</i> | wird personalisiert |
| <i>privateElcKey</i> | <i>keyData</i> = <i>AttributNotSet</i> | |
| <i>keyAvailable</i> | Wildcard | |
| <i>listAlgorithmIdentifier</i> | alle Werte aus der Menge, [gemSpec_COS] {signECDsa} | |
| | | |
| <i>accessRuleSessionkeys</i> | irrelevant | |

Zugriffsregeln für die Kontaktschnittstelle

| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
|---|-----------------------------|-------------------|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Compute Digital Signature | PWD(PIN.CH) | |
| Generate Asymmetric Key Pair P1='81' | ALWAYS | |
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 75: |
| 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 Compute Digital Signature | AUT_PACE AND PWD(PIN.CH) | |
| Generate Asymmetric Key Pair P1='81' | AUT_PACE | |
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 67: |
| 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 (74) 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 (75) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Card-G2-A_3640 - K_Personalisierung: Personalisierte MF / DF.ESIGN / PrK.HP.AUT.E256

Bei der Personalisierung von PrK.HP.AUT.E256 MÜSSEN die in Tab_HBA_ObjSys_171 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 60: Tab_HBA_ObjSys_171 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

| Attribute | Wert | Bemerkung |
|----------------------|--------------------|-----------|
| <i>keyAvailable</i> | true | |
| <i>privateElcKey</i> | keyData = Wildcard | |

[<=]

5.6.2.6 MF / DF.ESIGN / PrK.HP.ENC.E256

PrK.HP.ENC.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Der zugehörige öffentliche Schlüssel PuK.HP.ENC.E256 ist in C.HP.ENC.E256 (siehe Kapitel 5.6.2.8) enthalten.

Card-G2-A_3641-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

PrK.HP.ENC.E256 MUSS die in Tab_HBA_ObjSys_172 dargestellten initialisierten Attribute besitzen.

Tabelle 61: Tab_HBA_ObjSys_172 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

| Attribute | Wert | Bemerkung |
|---|--|---------------------|
| Objektyp | privates Schlüsselobjekt, ELC 256 | |
| <i>keyIdentifier</i> | '05' = 5 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>privateElcKey</i> | <i>domainparameter</i> = <i>brainpoolP256r1</i> | wird personalisiert |
| <i>privateElcKey</i> | <i>keyData</i> = <i>AttributNotSet</i> | |
| <i>keyAvailable</i> | Wildcard | |
| <i>listAlgorithmIdentifier</i> | alle Werte aus der Menge, [gemSpec_COS] {elcSharedSecretCalculation} | |
| | | |
| <i>accessRuleSessionkeys</i> | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |

| | | |
|---|-----------------------------|---|
| Delete | AUT_CMS OR AUT_CUP | siehe Hinweis 69: |
| 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 69: |
| 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 (76) 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 (77) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3642 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

Bei der Personalisierung von PrK.HP.ENC.E256 MÜSSEN die in Tab_HBA_ObjSys_173 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 62: Tab_HBA_ObjSys_173 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

| Attribute | Wert | Bemerkung |
|----------------------|--------------------|-----------|
| <i>keyAvailable</i> | true | |
| <i>privateElcKey</i> | keyData = Wildcard | |

[<=]

5.6.2.7 MF / DF.ESIGN / EF.C.HP.AUT.E256

Die Datei EF.C.HP.AUT.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.HP.AUT.E256. Das zugehörige private Schlüsselobjekt PrK.HP.AUT.E256 ist in Kapitel 5.6.2.5 definiert.

Card-G2-A_3643 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

EF.C.HP.AUT.E256 MUSS die in Tab_HBA_ObjSys_174 dargestellten initialisierten Attribute besitzen.

Tabelle 63: Tab_HBA_ObjSys_174 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|--|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C5 06' | |
| <i>shortFileIdentifier</i> | '06' = 6 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>numberOfOctet</i> | '0B B8' Oktett = 3000 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | wird personalisiert |
| <i>shareable</i> | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| <i>body</i> | 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 71: |

| | | |
|---|--------------------------------------|-------------------|
| Read Binary | ALWAYS | |
| Set Logical EOF Write Binary | AUT_CMS OR AUT_CUP | siehe Hinweis 71: |
| 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 71: |
| Read Binary | AUT_PACE OR AUT_CMS OR AUT_CUP | |
| Set Logical EOF Write Binary | AUT_CMS OR AUT_CUP | siehe Hinweis 71: |
| 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 (78) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (79) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3644 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

Bei der Initialisierung von EF.C.HP.AUT.E256 MÜSSEN die in Tab_HBA_ObjSys_175 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 64: Tab_HBA_ObjSys_175 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-----------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>body</i> | C.HP.AUT.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUT.E256 | |

[<=]

5.6.2.8 MF / DF.ESIGN/ EF.C.HP.ENC.E256

Die Datei EF.C.HP.ENC.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.HP.ENC.E256. Das zugehörnde private Schlüsselobjekt PrK.HP.ENC.E256 ist im Kapitel 5.6.2.6 definiert.

Card-G2-A_3645 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

EF.C.HP.ENC.E256 MUSS die in Tab_HBA_ObjSys_176 dargestellten initialisierten Attribute besitzen.

Tabelle 65: Tab_HBA_ObjSys_176 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|---|---------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C2 05' | |
| <i>shortFileIdentifier</i> | '05' = 5 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>numberOfOctet</i> | '0B B8' Oktett = 3000 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | wird personalisiert |
| <i>shareable</i> | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| <i>body</i> | 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 73: |
| Read Binary | ALWAYS | |
| Set Logical EOF Write Binary | AUT_CMS OR AUT_CUP | siehe Hinweis 73: |
| andere | NEVER | |

| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
|---|--------------------------------------|-------------------|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| 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 73: |
| Read Binary | AUT_PACE OR AUT_CMS OR AUT_CUP | |
| Set Logical EOF Write Binary | AUT_CMS OR AUT_CUP | siehe Hinweis 73: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |

[<=]

Hinweis (80) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (81) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3646 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

Bei der Initialisierung von EF.C.HP.ENC.E256 MÜSSEN die in Tab_HBA_ObjSys_177 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 66: Tab_HBA_ObjSys_177 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|---|-----------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>body</i> | C.HP.ENC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in | |

| | | |
|--|-----------------|--|
| | PrK.HP.ENC.E256 | |
|--|-----------------|--|

[<=]

5.6.2.9 MF / DF.ESIGN / EF.C.HP.SIG.R2048

Dieses EF enthält das Zertifikat zum Schlüssel PrK.HP.SIG.R2048.

A_15220 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

EF.C.HP.SIG.R2048 MUSS die in Tab_HBA_ObjSys_130 dargestellten Werte besitzen.

Tabelle 67: Tab_HBA_ObjSys_130 initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

| Attribute | Wert | Bemerkung |
|---|--|-----------|
| Objekttyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C0 00' | |
| <i>shortFileIdentifier</i> | '10' = 16 | |
| <i>numberOfOctet</i> | '0B B8' Oktett = 3000 Oktett | |
| <i>positionLogicalEndOfFile</i> | 0 | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | "Operational state (activated)" | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | |
| | Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| DELETE SET LOGICAL EOF WRITE BINARY | AUT_CMS OR AUT_CUP | |
| READ BINARY | ALWAYS | |
| | Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)" | |

| | | |
|--|--------------------|--|
| DELETE READ BINARY SET LOGICAL EOF WRITE BINARY | AUT_CMS OR AUT_CUP | |
| READ BINARY | AUT_PACE | |

[<=]

A_15221 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

Bei der Personalisierung von EF.C.HP.SIG.R2048 MÜSSEN die in Tab_HBA_ObjSys_136 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 68: Tab_HBA_ObjSys_136 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

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

[<=]

5.6.2.10 MF / DF.ESIGN / EF.C.HP.SIG.E256

Dieses EF enthält das Zertifikat zum Schlüssel PrK.HP.SIG.E256.

A_15222 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

EF.C.HP.SIG.E256 MUSS die in Tab_HBA_ObjSys_131 dargestellten Werte besitzen.

Tabelle 69: Tab_HBA_ObjSys_131 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|-------------------------------|-----------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'C0 07' | |
| <i>shortFileIdentifier</i> | '07' = 7 | |
| <i>numberOfOctet</i> | '0B B8' Oktett = 3000 Oktett | |
| <i>positionLogicalEndOfFile</i> | 0 | |

| | | |
|--|--|--|
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | "Operational state (activated)" | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | |
| | Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| DELETE SET LOIGCAL EOF WRITE BINARY | AUT_CMS OR AUT_CUP | |
| READ BINARY | ALWAYS | |
| | Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| DELETE READ BINARY SET LOIGCAL EOF WRITE BINARY | AUT_CMS OR AUT_CUP | |
| READ BINARY | AUT_PACE | |

[<=]

A_15223 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

Bei der Personalisierung von EF.C.HP.SIG.E256 MÜSSEN die in Tab_HBA_ObjSys_137 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 70: Tab_HBA_ObjSys_137 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-----------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | |
| <i>body</i> | C.HP.SIG.E2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.SIG.E2048 | |

[<=]

5.6.2.11 MF / DF.ESIGN / PrK.HP.SIG.R2048

Dieses Objekt enthält den privaten Signaturschlüssel für RSA-Signaturen.

A_15224 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048

PrK.HP.SIG.R2048 MUSS die in Tab_HBA_ObjSys_132 dargestellten Werte besitzen.

Tabelle 71: Tab_HBA_ObjSys_132 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048

| Attribute | Wert | Bemerkung |
|--|---|-----------|
| Objekttyp | privates Schlüsselobjekt, RSA 2048 | |
| <i>keyIdentifier</i> | '04' = 4 | |
| <i>lifeCycleStatus</i> | "Operational state (activated)" | |
| <i>privateKey</i> | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit | |
| <i>keyAvailable</i> | Wildcard | |
| <i>listAlgorithmIdentifier</i> | alle Werte aus der Menge, [gemSpec_COS] {signPSS} | |
| | Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| PSO Compute Digital Signature | PWD(PIN.CH) | |
| GENERATE ASYMMETRIC KEY PAIR (P1='81') | ALWAYS | |

| | | |
|--|--|--|
| DELETE | AUT_CMS OR AUT_CUP | |
| | Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| PSO Compute Digital Signature | AUT_PACE AND PWD(PIN.CH) | |
| GENERATE ASYMMETRIC KEY PAIR (P1='81') | AUT_PACE | |
| DELETE | AUT_CMS OR AUT_CUP | |

[<=]

A_15225 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

Bei der Personalisierung von PrK.HP.SIG.E256 MÜSSEN die in Tab_HBA_ObjSys_133 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 72: Tab_HBA_ObjSys_133 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

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

[<=]

5.6.2.12 MF / DF.ESIGN / PrK.HP.SIG.E256

Dieses Objekt enthält den privaten Signaturschlüssel für ECC-Signaturen.

A_15226 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

PrK.HP.SIG.E256 MUSS die in Tab_HBA_ObjSys_134 dargestellten Werte besitzen.

Tabelle 73: Tab_HBA_ObjSys_134 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

| Attribute | Wert | Bemerkung |
|------------------------|--|-----------|
| Objekttyp | privates Schlüsselobjekt, ELC 256 | |
| <i>keyIdentifier</i> | '07' = 7 | |
| <i>lifeCycleStatus</i> | "Operational state (activated)" | |
| <i>privateElcKey</i> | <ul style="list-style-type: none"> <i>domainparameter</i> = brainpoolP256r1 | |

| | | |
|--|--|--|
| | <ul style="list-style-type: none"> keyData = AttributeNotSet | |
| keyAvailable | Wildcard | |
| listAlgorithmIdentifier | alle Werte aus der Menge, [gemSpec_COS] {signECDSA} | |
| | Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| PSO Compute Digital Signature | PWD(PIN.CH) | |
| GENERATE ASYMMETRIC KEY PAIR (P1='81') | ALWAYS | |
| DELETE | AUT_CMS OR AUT_CUP | |
| | Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)" | |
| Zugriffsart | Zugriffsbedingung | |
| PSO Compute Digital Signature | AUT_PACE AND PWD(PIN.CH) | |
| GENERATE ASYMMETRIC KEY PAIR (P1='81') | AUT_PACE | |
| DELETE | AUT_CMS OR AUT_CUP | |

[<=]

A_15227 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

Bei der Personalisierung von PrK.HP.SIG.E256 MÜSSEN die in Tab_HBA_ObjSys_135 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 74: Tab_HBA_ObjSys_135 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

| Attribute | Wert | Bemerkung |
|---------------|--------------------|-----------|
| keyAvailable | True | |
| privateElcKey | keyData = WildCard | |

[<=]

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. Das jeweilige DF.CIA.x enthält dazu die Dateien Cryptographic Information Application (CIAInfo), Object Directory (OD), Authentication Object Directory (AOD), Private Key Directory (PrKD) und Certificate Directory (CD). Die verwendeten Objektattribute und die Dateiinhalte sind konform zu [ISO7816-15] und [ISO8825-1].

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

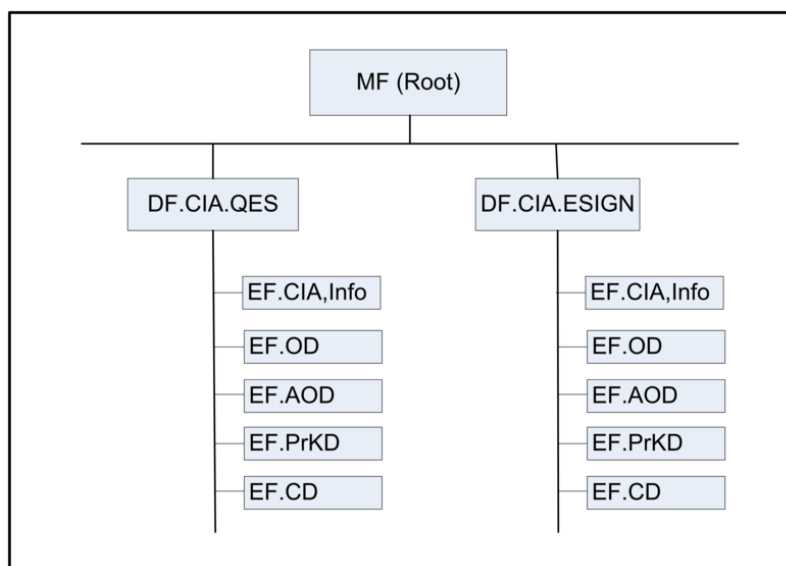


Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen

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 75: Tab_HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES

| Attribute | Wert | Bemerkung |
|-----------|--------|-----------|
| Objektyp | Ordner | |

| | | |
|---|---------------------------------|-------------------|
| | | |
| <i>applicationIdentifier</i> | "E828BD080F D27600006601" | siehe Hinweis 82: |
| <i>fileIdentifier</i> | – | siehe Hinweis 83: |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | 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_2119-01 - 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 76: Tab_HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info)

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-------------------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '50 32' | siehe Hinweis 83: |
| <i>shortFileIdentifier</i> | '12' = 18 | siehe Hinweis 83: |
| <i>numberOfOctet</i> | ' 00 A5' Oktett = 165 Oktett | |
| <i>positionLogicalEndOfFile</i> | ' 00 A5' Oktett = 165 Oktett | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | True | |
| <i>body</i> | <pre> 30 81 A2 02 01 01 80 1F 51 75 61 6C 69 66 69 65 64 20 53 69 67 6E 61 74 75 72 65 20 41 70 70 6C 69 63 61 74 69 6F 6E 03 02 05 60 30 0D 30 0B 02 01 01 04 06 D2 76 00 00 66 01 A2 69 30 49 02 01 01 02 01 43 30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 03 02 06 40 06 09 2A 86 48 86 F7 0D 01 01 0A </pre> | |

| | | |
|---|---|-----------|
| | 02 01 05 30 1C 02 01 02 02 04 80 00 00 05 05 00 03 02 06 40 06 08 2A 86 48 CE 3D 04 03 02 02 01 00 | |
| 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 (82) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (83) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in in [ISO7816-15] festgelegt.

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

Card-G2-A_2120-01 - 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 77: Tab_HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD

| Attribute | Wert | Bemerkung |
|---|---|-------------------|
| Objekttyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '50 31' | siehe Hinweis 85: |
| <i>shortFileIdentifier</i> | '11' = 17 | siehe Hinweis 85: |
| <i>numberOfOctet</i> | '00 18' Oktett = 24 Oktett | |
| <i>positionLogicalEndOfFile</i> | '00 18' Oktett = 24 Oktett | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |
| <i>body</i> | A8 06 30 04 04 02 50 34 A0 06 30 04 04 02 50 35 A4 06 30 04 04 02 50 38 | |
| 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 (84) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (85) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] [ISO7816-4] festgelegt.

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

Card-G2-A_2121-01 - 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 78: Tab_HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)

| Attribute | Wert | Bemerkung |
|--------------------------|-------------------------------|-----------|
| Objektyp | transparentes Elementary File | |
| fileIdentifier | '50 34' | |
| shortFileIdentifier | '14' = 20 | |
| numberOfOctet | '00 7C' Oktett = 124 Oktett | |
| positionLogicalEndOfFile | '00 7C' Oktett = 124 Oktett | |
| flagTransactionMode | False | |
| flagChecksum | True | |
| lifeCycleStatus | Operational state (activated) | |
| shareable | True | |

| | | |
|---|---|-----------|
| body | <pre> 30 3F 30 0C 0C 07 50 49 4E 2E 51 45 53 04 01 13 30 06 04 01 03 80 01 01 A1 27 30 25 03 03 04 4C 10 0A 01 04 02 01 06 02 01 08 02 01 08 80 01 81 04 01 FF 30 0C A1 0A 4F 06 D2 76 00 00 66 01 04 00 30 39 30 09 0C 07 50 55 4B 2E 51 45 53 30 06 04 01 13 80 01 01 A1 24 30 22 03 03 02 7E 04 0A 01 04 02 01 08 02 01 08 80 01 81 04 01 FF 30 0C A1 0A 4F 06 D2 76 00 00 66 01 04 00 </pre> | |
| 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 (86) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

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

Card-G2-A_2122-01 - 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.

Der initialisierte Wert des ASN.1 Elements *userConsent* (Oktett 26 des Attributs *body*, Zählweise beginnend mit 1) MUSS den Wert des SSEC für SE#1 aus MF / DF.QES / PIN.QES enthalten.

Tabelle 79: Tab_HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)

| Attribute | Wert | Bemerkung |
|---------------------------------|-------------------------------|-----------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '50 35' | |
| <i>shortFileIdentifier</i> | '15' = 21 | |
| <i>numberOfOctet</i> | '00 B2' Oktett = 178 Oktett | |
| <i>positionLogicalEndOfFile</i> | '00 B2' Oktett = 178 Oktett | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |
| <i>body</i> | 30 59 30 2C | |

| | | |
|---|--|-----------|
| | <pre> 53 0C 0A 50 72 4B 2E 48 50 2E 51 45 03 02 07 80 04 01 03 02 01 'xx' 30 14 30 12 03 02 02 24 A1 0C 04 01 03 30 07 03 02 05 20 02 01 01 30 13 04 01 84 03 02 05 20 03 02 03 B8 02 01 84 A1 03 02 01 01 A1 14 30 12 30 0C A1 0A 4F 06 D2 76 00 00 66 01 04 00 02 02 08 00 A0 55 30 2C 0C 0A 50 72 4B 2E 48 50 2E 51 45 53 03 02 07 80 04 01 03 02 01 01 30 14 30 12 03 02 02 24 A1 0C 04 01 03 30 07 03 02 05 20 02 01 01 30 13 04 01 86 03 02 05 20 03 02 03 B8 02 01 86 A1 03 02 01 02 A1 10 30 0E 30 0C A1 0A 4F 06 D2 76 00 00 66 01 04 00 </pre> | |
| 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 | | |
| 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.

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

Card-G2-A_2123-01 - 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 80: Tab_HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD (Certificate Directory)

| Attribute | Wert | Bemerkung |
|-----------------------|-------------------------------|-----------|
| Objekttyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '50 38' | |

| | | |
|---------------------------------|---|--|
| <i>shortFileIdentifier</i> | '16' = 22 | |
| <i>numberOfOctet</i> | '4E' Oktett = 78 Oktett | |
| <i>positionLogicalEndOfFile</i> | '4E' Oktett = 78 Oktett | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |
| <i>body</i> | <pre> 30 25 30 0A 0C 08 43 2E 48 50 2E 51 45 53 30 03 04 01 84 A1 12 30 10 30 0E A1 0C 4F 06 D2 76 00 00 66 01 04 02 C0 00 30 25 30 0A 0C 08 43 2E 48 50 2E 51 45 53 30 03 04 01 86 A1 12 30 10 30 0E A1 0C 4F 06 D2 76 00 00 66 01 04 02 C0 06 </pre> | |

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 (88) 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 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 81: Tab_HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN

| Attribute | Wert | Bemerkung |
|------------------------------|-----------------------------------|-------------------|
| Objektyp | Ordner | |
| <i>applicationIdentifier</i> | 'E828BD080F A000000167455349474E' | siehe Hinweis 82: |
| <i>fileIdentifier</i> | – | siehe Hinweis 83: |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | 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 (89) 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 (90) Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [ISO7816-15] sowie als PIX den applicationIdentifier von [ISO7816-4].

Hinweis (91) herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS# 8.1.1]

Hinweis (92) 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_3320-01 - 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 82: Tab_HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo (Cryptographic Information Application Info)

| Attribute | Wert | Bemerkung |
|--------------------------|---|-------------------|
| Objektyp | transparentes Elementary File | |
| fileIdentifier | '50 32' | siehe Hinweis 83: |
| shortFileIdentifier | '12' = 18 | siehe Hinweis 83: |
| numberOfOctet | '01 32' Oktett = 306 Oktett | |
| positionLogicalEndOfFile | '01 32' Oktett = 306 Oktett | |
| flagTransactionMode | False | |
| flagChecksum | True | |
| lifeCycleStatus | „Operational state (activated)“ | |
| shareable | True | |
| body | <pre> 30 82 01 2E 02 01 01 80 11 45 53 49 47 4E 20 41 70 70 6C 69 63 61 74 69 6F 6E 03 02 05 60 A2 82 01 10 30 49 02 01 01 02 01 43 30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 03 02 06 40 06 09 2A 86 48 86 F7 0D 01 01 0A 02 01 05 30 1A </pre> | |

| | | |
|--|---|------------------|
| | 02 01 02 02 01 01 05 00 03 02 06 40 06 09 2A 86 48 86 F7 0D 01 01 01 02 01 02 30 1A 02 01 04 02 01 01 05 00 03 02 02 04 06 09 2A 86 48 86 F7 0D 01 01 01 02 01 81 30 4C 02 01 05 02 04 80 00 00 02 30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 03 02 02 04 06 09 2A 86 48 86 F7 0D 01 01 07 02 01 85 30 1C 02 01 06 02 04 80 00 00 05 05 00 03 02 06 40 06 08 2A 86 48 CE 3D 04 03 02 02 01 00 30 1F 02 01 07 02 04 80 00 00 06 05 00 03 02 02 04 06 0B 04 00 7F 00 07 01 01 05 01 02 04 02 01 0B | |
| 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 | | |
| 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 (93) 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 (94) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.

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

Card-G2-A_3321-01 - 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 83: Tab_HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)

| Attribute | Wert | Bemerkung |
|--------------------------|-------------------------------|-------------------|
| Objektyp | transparentes Elementary File | |
| fileIdentifier | '50 31' | siehe Hinweis 85: |
| shortFileIdentifier | '11' = 17 | siehe Hinweis 85: |
| numberOfOctet | '0018' Oktett = 2 Oktett | |
| positionLogicalEndOfFile | '0018' Oktett = 2 Oktett | |
| flagTransactionMode | False | |

| | | |
|---|---|-----------|
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |
| <i>body</i> | A8 06 30 04 04 02 50 34 A0 06 30 04 04 02 50 35 A4 06 30 04 04 02 50 38 | |
| 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 (95) 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 (96) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.

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

Card-G2-A_3322-01 - 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 84: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)

| Attribute | Wert | Bemerkung |
|--------------------------|--|-----------|
| Objektyp | transparentes Elementary File | |
| fileIdentifier | '50 34' | |
| shortFileIdentifier | '14' = 20 | |
| numberOfOctet | '00 58' Oktett = 88 Oktett | |
| positionLogicalEndOfFile | '00 58' Oktett = 88 Oktett | |
| flagTransactionMode | False | |
| flagChecksum | True | |
| lifeCycleStatus | Operational state (activated) | |
| shareable | True | |
| body | <pre> 30 2D 30 0B 0C 06 50 49 4E 2E 43 48 04 01 12 30 03 04 01 02 A1 19 30 17 03 03 04 0C 10 0A 01 04 02 01 06 02 01 08 02 01 08 80 01 01 04 01 FF 30 27 30 08 0C 06 50 55 4B 2E 43 48 30 03 04 01 12 A1 16 30 14 03 03 02 3E 04 0A 01 04 02 01 08 02 01 08 80 01 01 04 01 FF </pre> | |

| | | |
|---|----------------------|-----------|
| | | |
| 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 (97) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

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

Card-G2-A_3323-01 - 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 85: Tab_HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

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

| | | |
|---------------------------------|-------------------------------|--|
| Objekttyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '50 35' | |
| <i>shortFileIdentifier</i> | '15' = 21 | |
| <i>numberOfOctet</i> | '02 11' Oktett = 529 Oktett | |
| <i>positionLogicalEndOfFile</i> | <i>numberOfOctet</i> | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |

| | | |
|------|--|--|
| body | <pre> 30 5B 30 27 0C 0A 50 72 4B 2E 48 50 2E 41 55 54 03 02 07 80 04 01 02 30 12 30 10 03 03 06 24 40 A1 09 04 01 02 30 04 03 02 05 20 30 16 04 01 82 03 02 05 20 03 02 03 B8 02 01 82 A1 06 02 01 01 02 01 02 A1 18 30 16 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 02 02 08 00 30 5A 30 26 0C 0A 50 72 4B 2E 48 50 2E 45 4E 43 03 02 07 80 04 01 02 30 11 30 0F 03 02 00 21 A1 09 04 01 02 30 04 03 02 05 20 30 16 04 01 83 03 02 06 40 03 02 03 B8 02 01 83 A1 06 02 01 04 02 01 05 A1 18 30 16 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 02 02 08 00 30 57 30 26 0C 0A 50 72 4B 2E 48 50 2E 53 49 47 03 02 07 80 04 01 02 30 11 30 0F </pre> | |
|------|--|--|

| | | |
|-------|----------------------------------|--|
| | 03 02 02 24 | |
| | A1 09 | |
| | 04 01 02 | |
| | 30 04 | |
| | 03 02 05 20 | |
| 30 13 | | |
| | 04 01 84 | |
| | 03 02 05 20 | |
| | 03 02 03 B8 | |
| | 02 01 84 | |
| | A1 03 | |
| | 02 01 01 | |
| A1 18 | | |
| 30 16 | | |
| 30 10 | | |
| | A1 0E | |
| | 4F 0A A0 00 00 01 67 | |
| | 45 53 49 47 4E | |
| | 04 00 | |
| | 02 02 08 00 | |
| A0 53 | | |
| 30 26 | | |
| | 0C 0A 50 72 4B 2E 48 50 2E 41 55 | |
| 54 | | |
| | 03 02 07 80 | |
| | 04 01 02 | |
| | 30 11 | |
| | 30 0F | |
| | 03 02 02 24 | |
| | A1 09 | |
| | 04 01 02 | |
| | 30 04 | |
| | 03 02 05 20 | |
| 30 13 | | |
| | 04 01 86 | |
| | 03 02 05 20 | |
| | 03 02 03 B8 | |
| | 02 01 86 | |
| | A1 03 | |
| | 02 01 06 | |
| A1 14 | | |
| 30 12 | | |
| 30 10 | | |
| | A1 0E | |
| | 4F 0A A0 00 00 01 67 | |
| | 45 53 49 47 4E | |
| | 04 00 | |
| A0 53 | | |
| 30 26 | | |
| | 0C 0A 50 72 4B 2E 48 50 2E 45 4E | |
| 43 | | |
| | 03 02 07 80 | |
| | 04 01 02 | |
| | 30 11 | |
| | 30 0F | |
| | 03 02 00 21 | |
| | A1 09 | |
| | 04 01 02 | |
| | 30 04 | |
| | 03 02 05 20 | |
| 30 13 | | |
| | 04 01 85 | |
| | 03 02 06 40 | |
| | 03 02 03 B8 | |
| | 02 01 85 | |
| | A1 03 | |

| | | |
|-------|----------------------------------|--|
| | 02 01 07 | |
| A1 14 | | |
| 30 12 | | |
| 30 10 | | |
| A1 0E | | |
| | 4F 0A A0 00 00 01 67 | |
| | 45 53 49 47 4E | |
| | 04 00 | |
| A0 53 | | |
| 30 26 | | |
| | 0C 0A 50 72 4B 2E 48 50 2E 53 49 | |
| 47 | | |
| | 03 02 07 80 | |
| | 04 01 02 | |
| 30 11 | | |
| 30 0F | | |
| | 03 02 02 24 | |
| A1 09 | | |
| | 04 01 02 | |
| 30 04 | | |
| | 03 02 05 20 | |
| 30 13 | | |
| | 04 01 87 | |
| | 03 02 05 20 | |
| | 03 02 03 B8 | |
| | 02 01 87 | |
| A1 03 | | |
| | 02 01 06 | |
| A1 14 | | |
| 30 12 | | |
| 30 10 | | |
| A1 0E | | |
| | 4F 0A A0 00 00 01 67 | |
| | 45 53 49 47 4E | |
| | 04 00 | |

| | | |
|---|----------------------|-----------|
| 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 (98) 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_3324-01 - 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 86: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)

| Attribute | Wert | Bemerkung |
|---------------------------------|--|-----------|
| Objektyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | '50 38' | |
| <i>shortFileIdentifier</i> | '16' = 22 | |
| <i>numberOfOctet</i> | '01 02' Oktett = 258 Oktett | |
| <i>positionLogicalEndOfFile</i> | numberOfOctett | |
| <i>flagTransactionMode</i> | False | |
| <i>flagChecksum</i> | True | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |
| <i>body</i> | <pre> 30 29 30 0A 0C 08 43 2E 48 50 2E 41 55 54 30 03 04 01 82 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C5 00 30 29 30 0A 0C 08 43 2E 48 50 2E 45 4E 43 30 03 04 01 83 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C2 00 30 29 </pre> | |

| | | |
|--|--|--|
| | <pre> 30 0A 0C 08 43 2E 48 50 2E 53 49 47 30 03 04 01 84 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C0 00 30 29 30 0A 0C 08 43 2E 48 50 2E 41 55 54 30 03 04 01 86 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C5 06 30 29 30 0A 0C 08 43 2E 48 50 2E 45 4E 43 30 03 04 01 85 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C2 05 30 29 30 0A 0C 08 43 2E 48 50 2E 53 49 47 30 03 04 01 87 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C0 07 </pre> | |
|--|--|--|

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 (99) 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.

5.8 Die Organisationsspezifische Authentisierungsanwendung

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.

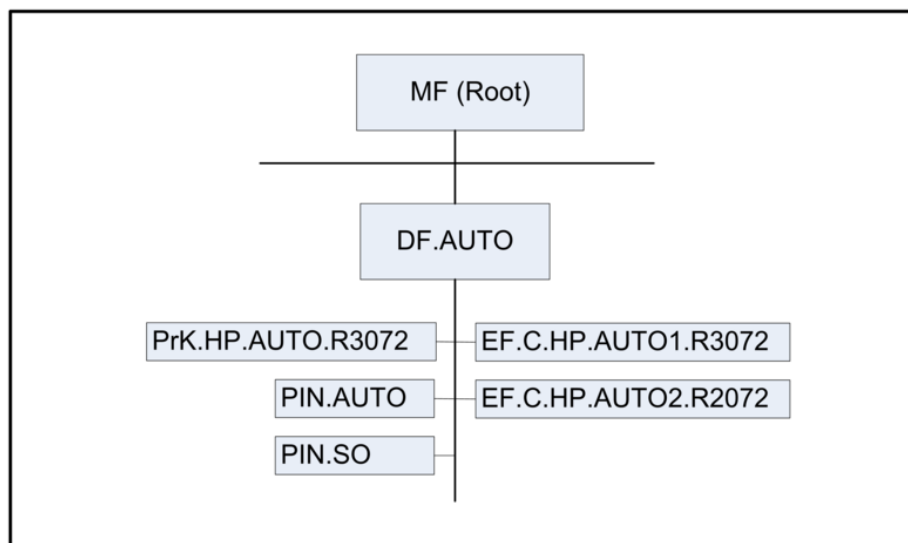


Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO

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 87: Tab_HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO

| Attribute | Wert | Bemerkung |
|------------------------------|---------------------------------|-------------------|
| Objektyp | Ordner | |
| <i>applicationIdentifier</i> | 'D27600014603' | siehe Hinweis 95: |
| <i>fileIdentifier</i> | – | siehe Hinweis 96: |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| <i>shareable</i> | 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 (100) 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 (101) Der Wert des Attributes applicationIdentifier ist in [ISO7816-4].

Hinweis (102) herstellerspezifisch; falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1]

Hinweis (103) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.8 im Allgemeinen irrelevant.

Hinweis (104) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

5.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R3072

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

Card-G2-A_2125-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

PrK.HP.AUTO.R3072 MUSS die in Tab_HBA_ObjSys_065 dargestellten Werte besitzen.

Tabelle 88: Tab_HBA_ObjSys_065 Initialisierte Attribute von MF / DF:AUTO / PrK.HP.AUTO.R3072

| Attribute | Wert | Bemerkung |
|---|--|---------------------|
| Objektyp | privates Schlüsselobjekt, RSA 3072 | |
| keyIdentifier | '02' = 2 | |
| privateKey | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit | wird personalisiert |
| keyAvailable | WildCard | |
| listAlgorithmIdentifier | alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, 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 (105) 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.R3072 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_3314-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

Bei der Personalisierung von PrK.HP.AUTO.R3072 MÜSSEN die in Tab_HBA_ObjSys_138 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 89: Tab_HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

| Attribute | Wert | Bemerkung |
|---------------------|-----------------------|---------------------|
| <i>privateKey</i> | Moduluslänge 3072 Bit | wird personalisiert |
| <i>keyAvailable</i> | 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 Heilberufers (PrK.HP.AUTO.R3072) 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 90: Tab_HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO

| Attribute | Wert | Bemerkung |
|--------------------------|--|---------------------|
| Objektyp | Passwortobjekt | |
| <i>pwdIdentifier</i> | '01' = 1 | |
| <i>secret</i> | undefiniert | wird personalisiert |
| <i>minimumLength</i> | 5 | |
| <i>maximumLength</i> | 8 | |
| <i>startRetryCounter</i> | 3 | |
| <i>retryCounter</i> | 3 | |
| <i>transportStatus</i> | ein Wert aus der Menge {Leer-PIN, Transport-PIN} | |

| | | |
|---|--|----------------------|
| <i>flagEnabled</i> | True | |
| <i>startSsec</i> | unendlich | |
| <i>PUK</i> | undefiniert | wird personalisiert |
| <i>pukUsage</i> | 10 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| CHANGE RD, P1=0 | ALWAYS | Hinweis 101: |
| CHANGE RD, P1=1 | ALWAYS | Hinweis 102: |
| | herstellerspezifisch | siehe Card-G2-A_3270 |
| 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 | Hinweis 101: |
| CHANGE RD, P1=1 | AUT_PACE | Hinweis 102: |
| | Herstellerspezifisch unter Verwendung von AUT_PACE | siehe Card-G2-A_3270 |

| | | |
|--|----------------------|-----------|
| 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 (106) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.

Hinweis (107) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

Hinweis (108) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN

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 herstellenspezifisch 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 91: Tab_HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO

| Attribute | Wert | Bemerkung |
|---------------|---------------|---|
| <i>secret</i> | Transport-PIN | Wird personalisiert, siehe Hinweis 103: |

| | | |
|-----|------------------------------------|--|
| PUK | PUK-Wert gemäß [gemSpec_PINPUK_TI] | |
|-----|------------------------------------|--|

[<=]

Hinweis (109) 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 92: Tab_HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO

| Attribute | Wert | Bemerkung |
|--------------------------|--|---------------------|
| Objektyp | Passwortobjekt | |
| <i>pwdIdentifier</i> | '03' = 3 | |
| <i>secret</i> | undefiniert | wird personalisiert |
| <i>minimumLength</i> | 6 | |
| <i>maximumLength</i> | 8 | |
| <i>startRetryCounter</i> | 3 | |
| <i>retryCounter</i> | 3 | |
| <i>transportStatus</i> | ein Wert aus der Menge {Leer-PIN, Transport-PIN} | |
| <i>flagEnabled</i> | True | |

| | | |
|---|--|----------------------|
| <i>startSsec</i> | unendlich | |
| <i>PUK</i> | undefiniert | wird personalisiert |
| <i>pukUsage</i> | 10 | |
| <i>lifeCycleStatus</i> | „Operational state (activated)“ | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| CHANGE RD, P1=0 | ALWAYS | Hinweis 105: |
| CHANGE RD, P1=1 | ALWAYS | Hinweis 106: |
| | herstellerspezifisch | siehe Card-G2-A_3271 |
| 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 | Hinweis 105: |
| CHANGE RD, P1=1 | AUT_PACE | Hinweis 106: |
| | Herstellerspezifisch unter Verwendung von AUT_PACE | siehe Card-G2-A_3271 |
| 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 (110) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.

Hinweis (111) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

Hinweis (112) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN

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 herstellerepezifisch 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 93: Tab_HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO

| Attribute | Wert | Bemerkung |
|---------------|------------------------------------|---|
| <i>secret</i> | Transport-PIN | Wird personalisiert, siehe Hinweis 107: |
| <i>PUK</i> | PUK-Wert gemäß [gemSpec_PINPUK_TI] | |

[<=]

Hinweis (113) 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.R3072 und MF / DF.AUTO / EF.C.HP.AUTO2.R3072

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

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

Card-G2-A_2130-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

EF.C.HP.AUTO1.R3072 MUSS die in Tab_HBA_ObjSys_070 dargestellten Werte besitzen.

Tabelle 94: Tab_HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

| Attribute | Wert | Bemerkung |
|---|-------------------------------|---------------------|
| Objektyp | transparentes Elementary File | |
| fileIdentifier | 'E0 01' | |
| shortFileIdentifier | '01' = 1 | |
| numberOfOctet | '0B B8' Oktett = 3000 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 (114) 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_3317-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

Bei der Personalisierung von EF.C.HP.AUTO1.R3072 MÜSSEN die in Tab_HBA_ObjSys_143 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 95: Tab_HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

| Attribute | Wert | Bemerkung |
|---------------------------------|---------------------------------------|---------------------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | wird personalisiert |

| | | |
|-------------|---|---------------------|
| <i>body</i> | C.HP.AUTO1.R3072 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUTO.R3072 | wird personalisiert |
|-------------|---|---------------------|

[<=]

Card-G2-A_2131-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

EF.C.HP.AUTO2.R3072 MUSS die in Tab_HBA_ObjSys_071 dargestellten Werte besitzen.

Tabelle 96: Tab_HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

| Attribute | Wert | Bemerkung |
|---------------------------------|-------------------------------|---------------------|
| Objekttyp | transparentes Elementary File | |
| <i>fileIdentifier</i> | 'E0 02' | |
| <i>shortFileIdentifier</i> | '02' = 2 | |
| <i>numberOfOctet</i> | '0B B8' Oktett = 3000 Oktett | |
| <i>positionLogicalEndOfFile</i> | '0' | |
| <i>flagTransactionMode</i> | True | |
| <i>flagChecksum</i> | False | |
| <i>lifeCycleStatus</i> | Operational state (activated) | |
| <i>shareable</i> | True | |
| <i>body</i> | kein Inhalt | wird 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 | |

[<=]

Card-G2-A_3318-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

Bei der Personalisierung von EF.C.HP.AUTO2.R3072 MÜSSEN die in Tab_HBA_ObjSys_144 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 97: Tab_HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

| Attribute | Wert | Bemerkung |
|---------------------------------|--|---------------------|
| <i>positionLogicalEndOfFile</i> | Zahl der tatsächlich belegten Oktette | wird personalisiert |
| <i>body</i> | C.HP.AUTO2.R3072 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUTO.R3072 | 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_2675-01 - K_Initialisierung: Initialisierte: Wert von PrK.HP.AUTO.R3072

PrK.HP.AUTO.R3072 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_2680-01 - K_Personalisierung: Inhalt von EF.C.HP.AUTO1.R3072

EF.C.HP.AUTO1.R3072 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_2681-01 - K_Personalisierung: Inhalt von EF.C.HP.AUTO2.R3072

EF.C.HP.AUTO2.R3072 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 (115) 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.

6 Anhang A – Verzeichnisse

6.1 - 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 Authorisation 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 |
| 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 |
| eIDAS | Verordnung über elektronische Identifizierung und Vertrauensdienste |
| 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) |
| ID | Identifizier |
| 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 (Fehlbedienungs-zähler) |
| 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 |
| 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 |
| 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 |

6.2 - Glossar

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

6.3 – Abbildungsverzeichnis

| | |
|---|-----|
| Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA | 22 |
| Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA | 62 |
| Abbildung 3: Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung | 66 |
| Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN | 82 |
| Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen | 107 |
| Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO..... | 134 |

6.4 – Tabellenverzeichnis

| | |
|--|----|
| Tabelle 1: Tab_HBA_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt..... | 9 |
| Tabelle 2: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten) | 21 |
| Tabelle 3: Tab_HBA_ObjSys_004 Initialisierte Attribute von MF | 22 |
| Tabelle 4: Tab_HBA_ObjSys_005 Initialisierte Attribute von MF / EF.ATR | 24 |
| Tabelle 5: Tab_HBA_ObjSys_083 Initialisierte Attribute von MF / EF.CardAccess | 25 |
| Tabelle 6: Tab_HBA_ObjSys_007 Initialisierte Attribute von MF / EF.DIR | 27 |
| Tabelle 7: Tab_HBA_ObjSys_008 Initialisierte Attribute von MF / EF.GDO | 29 |
| Tabelle 8: Tab_HBA_ObjSys_151 Personalisierte Attribute von MF / EF.GDO | 30 |
| Tabelle 9: Tab_HBA_ObjSys_009 Initialisierte Attribute von MF / EF.Version2..... | 31 |
| Tabelle 10: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256..... | 32 |
| Tabelle 11: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256..... | 34 |
| Tabelle 12: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256..... | 35 |
| Tabelle 13: Tab_HBA_ObjSys_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256..... | 37 |
| Tabelle 14: Tab_HBA_ObjSys_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256 | 37 |
| Tabelle 15: Tab_HBA_ObjSys_095 Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256 | 39 |
| Tabelle 16: Tab_HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH | 39 |
| Tabelle 17: Tab_HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH | 41 |
| Tabelle 18: Tab_HBA_ObjSys_021 Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256..... | 42 |

| | |
|---|----|
| Tabelle 19: Tab_HBA_ObjSys_099 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256..... | 44 |
| Tabelle 20: Tab_HBA_ObjSys_024 Initialisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256 | 44 |
| Tabelle 21: Tab_HBA_ObjSys_101 Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256 | 46 |
| Tabelle 22: Tab_HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256. | 47 |
| Tabelle 23: Tab_HBA_ObjSys_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten | 48 |
| Tabelle 24: Tab_HBA_ObjSys_082 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256..... | 50 |
| Tabelle 25: Tab_HBA_ObjSys_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256..... | 52 |
| Tabelle 26: Tab_HBA_ObjSys_029 Initialisierte Attribute von MF / SK.CMS.AES128..... | 52 |
| Tabelle 27: Tab_HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128 | 54 |
| Tabelle 28: Tab_HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256..... | 54 |
| Tabelle 29: Tab_HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256 | 56 |
| Tabelle 30: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128..... | 56 |
| Tabelle 31: Tab_HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES12857 | |
| Tabelle 32: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256..... | 58 |
| Tabelle 33: Tab_HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES25659 | |
| Tabelle 34: Tab_HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN..... | 59 |
| Tabelle 35: Tab_HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN | 61 |
| Tabelle 36: Tab_HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA | 62 |
| Tabelle 37: Tab_HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD ... | 64 |
| Tabelle 38: Tab_HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES..... | 66 |
| Tabelle 39: Tab_HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048..... | 68 |
| Tabelle 40: Tab_HBA_ObjSys_108 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048..... | 70 |
| Tabelle 41: Tab_HBA_ObjSys_037 Initialisierte Attribute von MF / DF.QES / PIN.QES.. | 70 |
| Tabelle 42: Tab_HBA_ObjSys_111 Personalisierte Attribute von MF / DF.QES / PIN.QES | 72 |
| Tabelle 43: Tab_HBA_ObjSys_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC. | 73 |
| Tabelle 44: Tab_HBA_ObjSys_039 Inhalt von EF.SSEC | 74 |
| Tabelle 45: Tab_HBA_ObjSys_040 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048..... | 75 |

| | |
|--|-----|
| Tabelle 46: Tab_HBA_ObjSys_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048..... | 77 |
| Tabelle 47: Tab_HBA_ObjSys_160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256..... | 78 |
| Tabelle 48: Tab_HBA_ObjSys_161 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256..... | 79 |
| Tabelle 49: Tab_HBA_ObjSys_162 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256..... | 80 |
| Tabelle 50: Tab_HBA_ObjSys_045 Initialisierte Attribute von MF / DF.ESIGN | 82 |
| Tabelle 51: Tab_HBA_ObjSys_046 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048 | 84 |
| Tabelle 52: Tab_HBA_ObjSys_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048 | 86 |
| Tabelle 53: Tab_HBA_ObjSys_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048..... | 86 |
| Tabelle 54: Tab_HBA_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048..... | 88 |
| Tabelle 55: Tab_HBA_ObjSys_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048..... | 88 |
| Tabelle 56: Tab_HBA_ObjSys_127 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048..... | 90 |
| Tabelle 57: Tab_HBA_ObjSys_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048..... | 90 |
| Tabelle 58: Tab_HBA_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048..... | 92 |
| Tabelle 59: Tab_HBA_ObjSys_170 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256 | 92 |
| Tabelle 60: Tab_HBA_ObjSys_171 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256 | 94 |
| Tabelle 61: Tab_HBA_ObjSys_172 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256..... | 94 |
| Tabelle 62: Tab_HBA_ObjSys_173 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256..... | 96 |
| Tabelle 63: Tab_HBA_ObjSys_174 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256 | 96 |
| Tabelle 64: Tab_HBA_ObjSys_175 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256 | 98 |
| Tabelle 65: Tab_HBA_ObjSys_176 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256..... | 98 |
| Tabelle 66: Tab_HBA_ObjSys_177 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256..... | 99 |
| Tabelle 67: Tab_HBA_ObjSys_130 initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048 | 101 |

| | |
|---|-----|
| Tabelle 68: Tab_HBA_ObjSys_136 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048 | 102 |
| Tabelle 69: Tab_HBA_ObjSys_131 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256 | 102 |
| Tabelle 70: Tab_HBA_ObjSys_137 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256 | 104 |
| Tabelle 71: Tab_HBA_ObjSys_132 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048 | 104 |
| Tabelle 72: Tab_HBA_ObjSys_133 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256 | 105 |
| Tabelle 73: Tab_HBA_ObjSys_134 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256 | 105 |
| Tabelle 74: Tab_HBA_ObjSys_135 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256 | 106 |
| Tabelle 75: Tab_HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES | 107 |
| Tabelle 76: Tab_HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info) | 109 |
| Tabelle 77: Tab_HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD | 111 |
| Tabelle 78: Tab_HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) | 112 |
| Tabelle 79: Tab_HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory) | 114 |
| Tabelle 80: Tab_HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD (Certificate Directory) | 116 |
| Tabelle 81: Tab_HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN | 118 |
| Tabelle 82: Tab_HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo (Cryptographic Information Application Info) | 120 |
| Tabelle 83: Tab_HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory) | 122 |
| Tabelle 84: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) | 124 |
| Tabelle 85: Tab_HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory) | 125 |
| Tabelle 86: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory) | 131 |
| Tabelle 87: Tab_HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO | 134 |
| Tabelle 88: Tab_HBA_ObjSys_065 Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072 | 136 |
| Tabelle 89: Tab_HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072 | 137 |
| Tabelle 90: Tab_HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO | 138 |

| | |
|---|-----|
| Tabelle 91: Tab_HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO..... | 140 |
| Tabelle 92: Tab_HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO | 141 |
| Tabelle 93: Tab_HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO | 143 |
| Tabelle 94: Tab_HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072 | 144 |
| Tabelle 95: Tab_HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072 | 145 |
| Tabelle 96: Tab_HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072 | 146 |
| Tabelle 97: Tab_HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072 | 147 |

6.5 - Referenzierte Dokumente

6.5.1 – 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_G2.1] | gematik: Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1 |
| [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 |

6.5.2 – Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|-----------------|---|
| [ALGCAT] | Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) in der aktuellen Fassung, siehe www.bundesnetzagentur.de |
| [DIN66291-1] | DIN V66291-1: 2000 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 1: Anwendungsschnittstelle |
| [EN14890-1] | EN 14890-1: 2008 Application Interface for smart cards used as secure signature creation devices, Part 1: Basic services |
| [EN1867] | EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers |
| [ISO3166-1] | ISO/IEC 3166-1: 2006 Codes for the representations of names of countries and their subdivisions – Part 1: Country codes |
| [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: 2016 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 |