Einführung der Gesundheitskarte

Spezifikation des elektronischen Heilberufsausweises

HBA-Objektsystem

|  |  |
| --- | --- |
| Version: | 4.1.0 |
| Revision: | \main\rel\_opb1\rel\_ors2\4 |
| Stand: | 18.12.2017 |
| Status: | freigegeben |
| Klassifizierung | öffentlich |
| Referenzierung: | [gemSpec\_HBA\_ObjSys\_G2.1] |

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung von Errata R1.6.4-2

Dokumentenhistorie

| **Version** | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | **Bearbeitung** |
| --- | --- | --- | --- | --- |
| 4.0.0 | 21.04.17 |  | Einarbeitung Anpassungen Kartengeneration G2.1 | gematik |
|  |  |  | Einarbeitung Errata R1.6.4-2 | gematik |
| 4.1.0 | 18.12.17 |  | freigegeben | gematik |
|  |  |  |  |  |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 6](#_Toc502657557)

[1.1 Zielsetzung 6](#_Toc502657558)

[1.2 Zielgruppe 6](#_Toc502657559)

[1.3 Geltungsbereich 7](#_Toc502657560)

[1.4 Abgrenzung des Dokuments 7](#_Toc502657561)

[1.5 Methodik 7](#_Toc502657562)

[1.5.1 Nomenklatur 7](#_Toc502657563)

[1.5.2 Verwendung von Schüsselworten 9](#_Toc502657564)

[1.5.3 Komponentenspezifische Anforderungen 10](#_Toc502657565)

[2 Optionen 11](#_Toc502657566)

[2.1 Option\_Erstellung\_von\_Testkarten 11](#_Toc502657567)

[3 Lebenszyklus von Karte und Applikation 12](#_Toc502657568)

[4 Anwendungsübergreifende Festlegungen 13](#_Toc502657569)

[4.1 Mindestanzahl logischer Kanäle 13](#_Toc502657570)

[4.2 Unterstützung RSA CV-Zertifikate 13](#_Toc502657571)

[4.3 Untestützung optionaler Funktionspakete 13](#_Toc502657572)

[4.3.1 USB-Schnittstelle (optional) 13](#_Toc502657573)

[4.3.2 Kontaktlose Schnittstelle (optional) 14](#_Toc502657574)

[4.3.3 Kryptobox (optional) 15](#_Toc502657575)

[4.3.4 Symmetrischer Kryptographiealgorithmus DES (optional) 15](#_Toc502657576)

[4.4 Attributstabellen 15](#_Toc502657577)

[4.4.1 Attribute eines Ordners 16](#_Toc502657578)

[4.4.2 Attribute einer Datei (EF) 17](#_Toc502657579)

[4.5 Zugriffsregeln für besondere Kommandos 17](#_Toc502657580)

[4.6 Attributswerte und Personalisierung 17](#_Toc502657581)

[4.7 Kartenadministration 19](#_Toc502657582)

[5 Spezifikation grundlegender Applikationen 20](#_Toc502657583)

[5.1 Attribute des Objektsystems 20](#_Toc502657584)

[5.1.1 ATR-Kodierung 21](#_Toc502657585)

[5.2 Allgemeine Struktur 22](#_Toc502657586)

[5.3 Root, die Wurzelapplikation MF 23](#_Toc502657587)

[5.3.1 MF / EF.ATR 24](#_Toc502657588)

[5.3.2 MF / EF.CardAccess (Option kontaktlose Schnittstelle) 26](#_Toc502657589)

[5.3.3 MF / EF.DIR 27](#_Toc502657590)

[5.3.4 MF / EF.GDO 29](#_Toc502657591)

[5.3.5 MF / EF.Version2 30](#_Toc502657592)

[5.3.6 MF / EF.C.CA\_HPC.CS.R2048 32](#_Toc502657593)

[5.3.7 MF / EF.C.CA\_HPC.CS.E256 34](#_Toc502657594)

[5.3.8 MF / EF.C.HPC.AUTR\_CVC.R2048 36](#_Toc502657595)

[5.3.9 MF / EF.C.HPC.AUTR\_CVC.E256 38](#_Toc502657596)

[5.3.10 MF / EF.C.HPC.AUTD\_SUK\_CVC.E256 40](#_Toc502657597)

[5.3.11 MF / PIN.CH 42](#_Toc502657598)

[5.3.12 MF / PrK.HPC.AUTR\_CVC.R2048 44](#_Toc502657599)

[5.3.13 MF / PrK.HPC.AUTR\_CVC.E256 46](#_Toc502657600)

[5.3.14 MF / PrK.HPC.AUTD\_SUK\_CVC.E256 48](#_Toc502657601)

[5.3.15 Sicherheitsanker zum Import von CV-Zertifikaten 50](#_Toc502657602)

[5.3.15.1 MF / PuK.RCA.CS.R2048 50](#_Toc502657603)

[5.3.15.2 MF / PuK.RCA.CS.E256 52](#_Toc502657604)

[5.3.16 Asymmetrische Kartenadministration 55](#_Toc502657605)

[5.3.16.1 MF / PuK.RCA.ADMINCMS.CS.E256 55](#_Toc502657606)

[5.3.17 Symmetrische Kartenadministration 57](#_Toc502657607)

[5.3.17.1 MF / SK.CMS.AES128 58](#_Toc502657608)

[5.3.17.2 MF / SK.CMS.AES256 60](#_Toc502657609)

[5.3.17.3 MF / SK.CUP.AES128 62](#_Toc502657610)

[5.3.17.4 MF / SK.CUP.AES256 63](#_Toc502657611)

[5.3.18 MF / SK.CAN (Option kontaktlose Schnittstelle) 65](#_Toc502657612)

[5.3.19 Sicherheitsumgebungen auf MF-Ebene 66](#_Toc502657613)

[5.4 Die Heilberufsanwendung DF.HPA 66](#_Toc502657614)

[5.4.1 Dateistruktur und Dateiinhalt 66](#_Toc502657615)

[5.4.2 MF / DF.HPA (Health Professional Application) 67](#_Toc502657616)

[5.4.2.1 MF / DF.HPA / EF.HPD (Health Professional Data) 68](#_Toc502657617)

[5.4.2.2 Sicherheitsumgebungen 70](#_Toc502657618)

[5.5 Die Anwendung für die qualifizierte elektronische Signatur (DF.QES) 70](#_Toc502657619)

[5.5.1 Dateistruktur und Dateiinhalt 70](#_Toc502657620)

[5.5.2 MF / DF.QES (Qualified Electronic Signature Application) 70](#_Toc502657621)

[5.5.2.1 MF / DF.QES / PrK.HP.QES.R2048 72](#_Toc502657622)

[5.5.2.2 MF / DF.QES / PIN.QES 74](#_Toc502657623)

[5.5.2.3 MF / DF.QES / EF.SSEC 77](#_Toc502657624)

[5.5.2.4 MF / DF.QES / EF.C.HP.QES.R2048 79](#_Toc502657625)

[5.5.2.5 MF / DF.QES / EF.C.HP.QES-AC1, MF / DF.QES / EF.C.HP.QES-AC2 und MF / DF.QES / EF.C.HP.QES-AC3 81](#_Toc502657626)

[5.5.2.6 MF / DF.QES / PrK.HP.QES.E256 87](#_Toc502657627)

[5.5.2.7 MF / DF.QES / EF.C.HP.QES.E256 89](#_Toc502657628)

[5.5.2.8 MF / DF.QES / EF.C.HP.QES-AC1.E256, MF / DF.QES / EF.C.HP.QES-AC2.E256 und MF / DF.QES / EF.C.HP.QES-AC3.E256 92](#_Toc502657629)

[5.6 Die ESIGN-Anwendung (DF.ESIGN) 97](#_Toc502657630)

[5.6.1 Dateistruktur und Dateiinhalt 97](#_Toc502657631)

[5.6.2 MF / DF.ESIGN (Krypto-Anwendung ESIGN) 98](#_Toc502657632)

[5.6.2.1 MF / DF.ESIGN / PrK.HP.AUT.R2048 99](#_Toc502657633)

[5.6.2.2 MF / DF.ESIGN / PrK.HP.ENC.R2048 101](#_Toc502657634)

[5.6.2.3 MF / DF.ESIGN / EF.C.HP.AUT.R2048 103](#_Toc502657635)

[5.6.2.4 MF / DF.ESIGN / EF.C.HP.ENC.R2048 105](#_Toc502657636)

[5.6.2.5 MF / DF.ESIGN / PrK.HP.AUT.E256 107](#_Toc502657637)

[5.6.2.6 MF / DF.ESIGN / PrK.HP.ENC.E256 109](#_Toc502657638)

[5.6.2.7 MF / DF.ESIGN / EF.C.HP.AUT.E256 111](#_Toc502657639)

[5.6.2.8 MF / DF.ESIGN/ EF.C.HP.ENC.E256 113](#_Toc502657640)

[5.6.3 Sicherheitsumgebungen 115](#_Toc502657641)

[5.7 Die kryptographischen Informationsanwendungen 115](#_Toc502657642)

[5.7.1 MF / DF.CIA.QES (Cryptographic Information Applications) 116](#_Toc502657643)

[5.7.1.1 MF / DF.CIA.QES / EF.CIA.CIAInfo 117](#_Toc502657644)

[5.7.1.2 MF / DF.CIA.QES / EF.OD 119](#_Toc502657645)

[5.7.1.3 MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) 120](#_Toc502657646)

[5.7.1.4 MF / DF.CIA.QES / EF.PrKD (Private Key Directory) 122](#_Toc502657647)

[5.7.1.5 MF / DF.CIA.QES / EF.CD (Certificate Directory) 124](#_Toc502657648)

[5.7.2 MF / DF.CIA.ESIGN (Cryptographic Information Applications) 127](#_Toc502657649)

[5.7.2.1 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo 128](#_Toc502657650)

[5.7.2.2 MF / DF.CIA.ESIGN / EF.OD 131](#_Toc502657651)

[5.7.2.3 MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) 132](#_Toc502657652)

[5.7.2.4 MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory) 134](#_Toc502657653)

[5.7.2.5 MF / DF.CIA.ESIGN / EF.CD (Certificate Directory) 137](#_Toc502657654)

[5.8 Die Organisationsspezifische Authentisierungsanwendung 139](#_Toc502657655)

[5.8.1 Dateistruktur und Dateiinhalt 139](#_Toc502657656)

[5.8.2 DF.AUTO (Organization-specific Authentication Application) 140](#_Toc502657657)

[5.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R3072 141](#_Toc502657658)

[5.8.2.2 MF / DF.AUTO / PIN.AUTO 143](#_Toc502657659)

[5.8.2.3 MF / DF.AUTO / PIN.SO 146](#_Toc502657660)

[5.8.2.4 MF / DF.AUTO / EF.C.HP.AUTO1.R3072 und MF / DF.AUTO / EF.C.HP.AUTO2.R3072 149](#_Toc502657661)

[5.8.2.5 Sicherheitsumgebungen 152](#_Toc502657662)

[5.8.2.6 Vorgaben für die Nutzung von DF.AUTO 152](#_Toc502657663)

[5.9 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des HBA 154](#_Toc502657664)

[6 Anhang A – Verzeichnisse 155](#_Toc502657665)

[6.1 A1 - Abkürzungen 155](#_Toc502657666)

[6.2 A2 - Glossar 158](#_Toc502657667)

[6.3 A3 – Abbildungsverzeichnis 158](#_Toc502657668)

[6.4 A4 – Tabellenverzeichnis 159](#_Toc502657669)

[6.5 A5 - Referenzierte Dokumente 162](#_Toc502657670)

[6.5.1 A5.1 – Dokumente der gematik 162](#_Toc502657671)

[6.5.2 A5.2 – Weitere Dokumente 163](#_Toc502657672)

# Einordnung des Dokumentes

Nach Inkrafttreten der eIDAS-Verordnung wurde die Anforderungslage der gematik entsprechend angepasst. Signaturgesetz (SigG) und -verordnung (SigV) sind weiterhin gültig und finden dort Anwendung, wo sie der eIDAS-Verordnung nicht widersprechen. SigG und SigV sollen zukünftig durch das deutsche Vertrauensdienstegesetz (VDG) abgelöst werden. Mit Verabschiedung des Vertrauensdienstegesetzes kann es in diesem Dokument daher zu Anpassungen und Konkretisierungen entsprechend der geänderten Rechtslage kommen.

## 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 zugehörenden ISO-Standards (speziell ISO/IEC 7816, Teile 1-4, 6, 8, 9 und 15)
* andere Quellen (z.B. Anforderungen der Trustcenter)

Die Spezifikation behandelt Anwendungen des elektronischen Heilberufsausweises (HBA) unter den folgenden, rein kartenorientierten Gesichtspunkten:

* Ordnerstruktur,
* Dateien,
* Sicherheitsmechanismen wie Zugriffsregeln.

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

## 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.

## 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.

## 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.

## Methodik

### 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(oid\_cvc\_fl\_cms,’00010000000000’) | flagCMS.15 |
| AUT(oid\_cvc\_fl\_ti, ‘00010000000000’) OR AUT(oid\_cvc\_fl\_ti, ‘00008000000000’) | flagTI.15 OR flagTI.16 |
| PWD(PIN) AND  [  AUT(oid\_cvc\_fl\_cms,’00010000000000’)  OR  AUT(oid\_cvc\_fl\_ti, ‘00008000000000’)  ] | PWD(PIN)   AND   [flagCMS.15 OR flagTI.16)] |
| SmMac(oid\_cvc\_fl\_cms, ’00800000000000’) | SmMac(flagCMS.08) |

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

|  |  |
| --- | --- |
| AUT\_CMS | {SmMac(SK.CMS.AES128)  OR SmMac(SK.CMS.AES256)  OR SmMac(flagCMS.08)}  AND SmCmdEnc  AND SmRspEnc |
| AUT\_CUP | {SmMac(SK.CUP.AES128)  OR SmMac(SK.CUP.AES256)  OR 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:

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

### Verwendung von Schüsselworten

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

Sie werden im Dokument wie folgt dargestellt:

**⌦ Card-G2-A\_0000 <Titel der Afo>**

Text / Beschreibung

**⌫**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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

### 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 |

# 

# Optionen

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

## 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.

**⌫**

# 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.

1. Die in diesem Kapitel verwendeten Begriffe "Vorbereitungsphase" und "Nutzungs­phase" werden in [gemSpec\_COS#4] definiert.

# 

# Anwendungsübergreifende Festlegungen

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

* Unterstützung von mindestens vier logischen Kanälen.
* Unterstützung der RSA CV-Zertifikate

## 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:

1. Die maximale Anzahl logischer Kanäle MUSS gemäß [ISO7816-4#Tab.88] in den Historical Bytes in EF.ATR angezeigt werden.
2. Der HBA MUSS mindestens vier logische Kanäle unterstützen. Das bedeutet, die in den Bits b3b2b1 gemäß [ISO7816-4#Tab.88] kodierte Zahl MUSS mindestens ‘011’ = 3 oder größer sein.
3. **⌫**

## Unterstützung RSA CV-Zertifikate

**⌦ Card-G2-A\_3673 K\_Personalisierung und K\_Initialisierung:Unterstützung RSA CV-Zertifikate**

Der HBA MUSS die Verwendung von RSA CV-Zertifikaten unterstützen.

**⌫**

## Untestützung optionaler Funktionspakete

### 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**

1. Falls ein HBA die Option\_USB\_Schnittstelle nicht nutzen will, KANN für das Objekt­sys­tem ein COS verwendet werden,
2. a) das die Option\_USB\_Schnittstelle implementiert hat.
3. b) das die Option\_USB\_Schnittstelle nicht implementiert hat.
4. **⌫**

### 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**

1. Falls ein HBA die Option\_kontaktlose\_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,
2. a) das die Option\_kontaktlose\_Schnittstelle implementiert hat.
3. b) das die Option\_kontaktlose\_Schnittstelle nicht implementiert hat.
4. **⌫**

**⌦ Card-G2-A\_3009 K\_HBA: Zusatzanforderungen für kontaktlose Schnittstelle**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_3010 K\_Initialisierung und K\_Personalisierung: Kontaktlose Schnittstelle wird nicht genutzt**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_3011 K\_Initialisierung: Kontaktlose Schnittstelle im COS nicht vorhanden**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_3012 K\_Personalisierung: Absicherung der kontaktlosen Schnitt­stelle**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_2038 K\_Personalisierung: Druck der CAN auf den HBA bei Verwendung der optionalen kontaktlosen Schnittstelle**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_3277 K\_Personalisierung und K\_Initialisierung: Konformität kontaktlose Schnittstelle**

1. 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.
2. **⌫**

### Kryptobox (optional)

**⌦ Card-G2-A\_3014 K\_HBA: Vorhandensein Kryptobox**

1. Für einen HBA KANN für das Objektsystem ein COS verwendet werden,
2. a) das die Option\_Kryptobox implementiert hat.

b) das die Option\_Kryptobox nicht implementiert hat.

**⌫**

### 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 Kryptographie-algorithmus DES**

1. Für einen HBA KANN für das Objektsystem ein COS verwendet werden,
2. a) das die Option\_DES implementiert hat.
3. b) das die Option\_DES nicht implementiert hat.
4. **⌫**

## 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**

1. 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.
2. **⌫**

**⌦ 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**

1. 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.
2. **⌫**

**⌦ 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.

**⌫**

### Attribute eines Ordners

**⌦ Card-G2-A\_2033-01 K\_Initialisierung: Ordnerattribute**

1. Enthält eine Tabelle mit Ordnerattributen einen oder mehrere applicationIdentifier (AID), dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen
2. **⌫**

**⌦ Card-G2-A\_3624 K\_Initialisierung: Herstellerspezifischer ApplicationIdentifier**

1. Enthält eine Tabelle mit Ordnerattributen keinen *applicationIdentifier* (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.
2. **⌫**

**⌦ Card-G2-A\_3625 K\_Initialisierung: Fehlender FileIdentifier**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_3626 K\_Initialisierung: Herstellerspezifischer FileIdentifier**

1. 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.
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.

**⌫**

## 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:

1. Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kom-mandos Get Challenge, List Public Key, Manage Security Environment und Select stets ALWAYS sein.
2. 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.
3. 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. **⌫**

## Attributswerte und Personalisierung

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

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

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

Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:

**⌦ Card-G2-A\_3325 K\_Initialisierung und K\_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung**

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

**⌫**

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.

**⌫**

## 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.ADMIN.CS für die asymmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.

**⌫**

**⌦ Card-G2-A\_3590 Symmetrische Kartenadministration**

1. Bei der Personalisierung KÖNNEN die Schlüssel (SK.CMS und SK.CUP) für die symmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.
2. **⌫**

**⌦ Card-G2-A\_3591 Schlüsselspeicherung**

1. 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.
2. **⌫**

# 

# 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.

## 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\_3015entsprechen.

**⌫**

**⌦ 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 sein.

**⌫**

**⌦ Card-G2-A\_2042 K\_Initialisierung: Inhalt persistentPublicKeyList**

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

**⌫**

**⌦ Card-G2-A\_3181 K\_Initialisierung: Größe persistentPublicKeyList**

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

**⌫**

**⌦ Card-G2-A\_3266-01 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.

**⌫**

### 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**

1. Wenn der ATR ein TC1 Byte mit dem Wert ‘FF’ enthält, MUSS T0 auf den Wert ‘Dx’ gesetzt werden.
2. **⌫**

**⌦ Card-G2-A\_3015 K\_Personalisierung und K\_Initialisierung: Historical Bytes im ATR**

1. Das Attribut answerToReset SOLL keine Historical Bytes enthalten.
2. **⌫**

**⌦ Card-G2-A\_2045 K\_Personalisierung und K\_Initialisierung: Vorgaben für Historical Bytes**

1. Falls answerToReset Historical Bytes enthält, dann MÜSSEN
   1. diese gemäß [ISO7816-4] kodiert sein.
   2. die dort getroffenen Angaben konsistent sein zu Angaben im EF.ATR.
   3. **⌫**

## Allgemeine Struktur

**⌦ Card-G2-A\_2046 K\_Personalisierung: Kompatibilität zu G1-Karten**

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

**⌫**



Abbildung 1: Abb\_HBA\_ObjSys\_001 Allgemeine Dateistruktur eines HBA

## Root, die Wurzelapplikation MF

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

**⌦ Card-G2-A\_2047 K\_Initialisierung: Initialisierte Attribute von MF**

MF MUSS die in Tab\_HBA\_ObjSys\_004 dargestellten Werte besitzen.

Tabelle 3: Tab\_HBA\_ObjSys\_004 Initialisierte Attribute von MF

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | | Bemerkung |
| Objekttyp | Ordner | |  |
| *applicationIdentifier* | ‘D27600014601’ | |  |
| *fileIdentifier* | ‘3F 00’ | | falls vorhanden |
| *lifeCycleStatus* | „Operational state (activated)“ | |  |
| *shareable* | True | |  |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| Fingerprint | Wildcard |  | |
| Get Random | ALWAYS |  | |
| Load Application | AUT\_CMS | siehe Hinweis 4: | |
| andere | NEVER |  | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| alle | herstellerspezifisch |  | |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| alle | herstellerspezifisch |  | |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| Get Random | ALWAYS |  | |
| Load Application | AUT\_CMS | siehe Hinweis 4: | |
| andere | NEVER |  | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| alle | herstellerspezifisch |  | |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| alle | herstellerspezifisch |  | |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.3 im Allgemeinen irrelevant.
3. Nur dann ausführbar, wenn ein CMS genutzt wird (optional), siehe Kapitel 4.9

### 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 |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 01’ | siehe Hinweis 6: |
| *shortFileIdentifier* | ‘1D’= 29 |  |
| *numberOfOctet* | herstellerspezifisch |  |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | Inhalt gemäß [gemSpec\_Karten\_Fach\_TIP\_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 |  |

**⌫**

1. 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.
2. Der Wert des Attributs fileIdentifier ist in [ISO7816-4] festgelegt.

**⌦ Card-G2-A\_3278 K\_Initialisierung: Initialisiertes Attribu*t 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.

**⌫**

### 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**

1. Falls die kontaktlose Schnittstelle für den HBA genutzt wird, MUSS EF.CardAccess vorhanden sein und die in Tab\_HBA\_ObjSys\_083 dargestellten Attribute besitzen.

Tabelle 5: Tab\_HBA\_ObjSys\_083 Initialisierte Attribute von MF / EF.CardAccess

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’01 1C’ | siehe Hinweis 6: |
| *shortFileIdentifier* | ‘1C’= 28 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *numberOfOctet* | passend zum Inhalt |  |
| *positionLogicalEndOfFile* | passend zum Inhalt |  |
| *shareable* | True |  |
| body | passend zu den Attributen von SK.CAN gemäß [TR-03110-3] |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Read Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos | | |
| alle | herstellerspezifisch |  |

2. **⌫**

### MF / EF.DIR

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

1. **⌦ Card-G2-A\_3628 K\_Initialisierung: Inhalt der Records von EF.DIR**
2. Für jede im Objektsystem vorhandene Anwendung MUSS die Datei einen eigenen Record besitzen, der den ApplicationIdentifier (AID) dieser Anwendung im Format ´61‑L61‑{4F‑L4F‑AID}´ enthält.
3. Zu jedem Record der Datei MUSS es auf der Karte eine Anwendung geben, deren AID durch diesen Record beschrieben ist.
4. 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 |  |
| *fileIdentifier* | | ‘2F 00’ | Siehe Hinweis 8: |
| *shortFileIdentifier* | | ‘1E’= 30 | Siehe Hinweis 8: |
| *numberOfOctet* | | ‘00 BE’ Oktett = 190 Oktett |  |
| *maxNumRecords* | | 10 Records |  |
| *maxRecordLength* | | 32 Oktett |  |
| *flagRecordLCS* | | False |  |
| *flagTransactionMode* | | True |  |
| *flagChecksum* | | True |  |
| *lifeCycleStatus* | | „Operational state (activated)“ |  |
| *shareable* | | True |  |
| *recordList*  Record 1  Record 2  und folgende | | ‘61- 08- (4F 06 D27600014601)’  ´61‑L61‑{4F‑L4F‑AID}´  für alle Applikationen im Objektsystem | AID.MF |
| 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 | |  |

**⌫**

1. 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.
2. Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

### MF / EF.GDO

In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte enthält. Die Kennnummer basiert auf [Beschluss 190].

**⌦ Card-G2-A\_2057 K\_Initialisierung: Initialisierte Attribute von MF / EF.GDO**

EF.GDO MUSS die in Tab\_HBA\_ObjSys\_008 dargestellten Werte besitzen.

Tabelle 7: Tab\_HBA\_ObjSys\_008 Initialisierte Attribute von MF / EF.GDO

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | | Wert | Bemerkung |
| Objekttyp | | transparentes Elementary File |  |
| *fileIdentifier* | | ‘2F 02’ |  |
| *shortFileIdentifier* | | ‘02’= 2 |  |
| *numberOfOctet* | | ‘00 0C’ Oktett = 12 Oktett |  |
| *positionLogicalEndOfFile* | | Wildcard |  |
| *flagTransactionMode* | | False |  |
| *flagChecksum* | | True |  |
| *lifeCycleStatus* | | „Operational state (activated)“ |  |
| *shareable* | | True |  |
| *body* | | Wildcard | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Read Binary | ALWAYS | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Read Binary | AUT\_PACE | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |

**⌫**

1. 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** |
| *positionLogicalEndOfFile* | ‘00 0C’ Oktett = 12 Oktett |  |
| *body* | Inhalt gemäß [gemSpec\_Karten\_Fach\_TIP\_G2.1] |  |

**⌫**

### 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 |  |
| *fileIdentifier* | ‘2F 11’ |  |
| *shortFileIdentifier* | ‘11’= 17 |  |
| *numberOfOctet* | ‘00 3C’ Oktett = 60 Oktett |  |
| *positionLogicalEndOfFile* | passend zum Inhalt |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | Inhalt gemäß [gemSpec\_Karten\_Fach\_TIP\_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 |  |

**⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

### MF / EF.C.CA\_HPC.CS.R2048

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

**⌦ Card-G2-A\_2060 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.CA\_HPC.CS.R2048**

EF.C.CA\_HPC.CS.R2048 MUSS die in Tab\_HBA\_ObjSys\_010 dargestellten Werte besitzen.

Tabelle 10: Tab\_HBA\_ObjSys\_010 Initialisierte Attribute von MF / EF.C.CA\_HPC.CS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 04’ |  |
| *shortFileIdentifier* | ‘04’= 4 |  |
| *numberOfOctet* | ‘01 4B’ Oktett = 331 Oktett |  |
| *positionLogicalEndOfFile* | ‘0’ |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 14: |
| Read Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 14: |
| Read Binary | AUT\_PACE |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

**⌦ Card-G2-A\_3281 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.CA\_HPC.CS.R2048**

Bei der Personalisierung von EF.C.CA\_HPC.CS.R2048 MÜSSEN die in Tab\_HBA\_ObjSys\_089 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 11: Tab\_HBA\_ObjSys\_089 Personalisierte Attribute von MF / EF.C.CA\_HPC.CS.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | ‘01 4B’ Oktett = 331 Oktett |  |
| *body* | C.CA\_HPC.CS.R2048 gemäß [gemSpec\_PKI] |  |
| *body*  Option\_Erstellung \_von\_Testkarten | C.CA\_HPC.CS.R2048 gemäß [gemSpec\_PKI]  aus Test-CVC-CA | Details siehe [gemSpec\_TK#3.1.2] |

**⌫**

### MF / EF.C.CA\_HPC.CS.E256

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

**⌦ Card-G2-A\_2061 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.CA\_HPC.CS.E256**

EF.C.CA\_HPC.CS.E256 MUSS die in Tab\_HBA\_ObjSys\_011 dargestellten Werte besitzen.

Tabelle 12: Tab\_HBA\_ObjSys\_011 Initialisierte Attribute von MF / EF.C.CA\_HPC.CS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 07’ |  |
| *shortFileIdentifier* | ‘07’= 7 |  |
| *numberOfOctet* | ‘00 DC’ Oktett = 220 Oktett |  |
| *positionLogicalEndOfFile* | ‘0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 14: |
| Read Binary | ALWAYS |  |
| Update Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis 14: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 14: |
| Read Binary | AUT\_PACE  OR AUT\_CMS  OR AUT\_CUP |  |
| Update Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis 14: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

**⌦ Card-G2-A\_3282 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.CA\_HPC.CS.E256**

Bei der Personalisierung von EF.C.CA\_HPC.CS.E256 MÜSSEN die in Tab\_HBA\_ObjSys\_090 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 13: Tab\_HBA\_ObjSys\_090 Personalisierte Attribute von MF / EF.C.CA\_HPC.CS.E256

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| *positionLogicalEndOfFile* | ‘00 DC’ Oktett = 220 Oktett |  |
| *body* | C.CA\_HPC.CS.E256 gemäß [gemSpec\_PKI#6.7.1] | siehe [gemSpec\_COS] |
| *body*  Option\_Erstellung \_von\_Testkarten | C.CA\_HPC.CS.E256 gemäß [gemSpec\_PKI#6.7.1] aus Test-CVC-CA | Details siehe [gemSpec\_TK#3.1.2] |

**⌫**

### MF / EF.C.HPC.AUTR\_CVC.R2048

EF.C.HPC.AUTR\_CVC.R2048 enthält das CV-Zertifikat des HBA für die Kryptographie mit RSA für rollenbasierte C2C-Authentisierung zwischen HBA und eGK und für die Auto­ri­sierung der SMC-B. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA\_HPC.CS.R2048 (siehe Tab\_HBA\_ObjSys\_010) prüfen. Das zugehörende pri­va­te Schlüsselobjekt PrK.HPC.AUTR\_CVC.R2048 ist im Kapitel 5.3.12 definiert.

**⌦ Card-G2-A\_2063 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.R2048**

EF.C.HPC.AUTR\_CVC.R2048 MUSS die in Tab\_HBA\_ObjSys\_013 dargestellten Werte besitzen.

Tabelle 14: Tab\_HBA\_ObjSys\_013 Initialisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 03’ |  |
| *shortFileIdentifier* | ‘03’= 3 |  |
| *numberOfOctet* | ‘01 55’ Oktett = 341 Oktett |  |
| *positionLogicalEndOfFile* | ‘0’ |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 16: |
| Read Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 16: |
| Read Binary | AUT\_PACE |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

**⌦ Card-G2-A\_3385 K\_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTR\_CVC.R2048**

Für die CHR in diesem Zertifikat MUSS CHR = ’00 10’ || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A\_2058].

**⌫**

**⌦ Card-G2-A\_3283 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.R2048**

Bei der Personalisierung von EF.C.HPC.AUTR\_CVC.R2048 MÜSSEN die in Tab\_HBA\_ObjSys\_092 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 15: Tab\_HBA\_ObjSys\_092 Personalisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | ‘01 55’ Oktett = 341 Oktett |  |
| *body* | C.HPC.AUTR\_CVC.R2048 passend zu dem privaten Schlüssel in PrK.HPC.AUTR\_CVC.R2048 [gemSpec\_PKI] | siehe [gemSpec\_COS] |

**⌫**

### MF / EF.C.HPC.AUTR\_CVC.E256

EF.C.HPC.AUTR\_CVC.E256 enthält das CV-Zertifikat des HBA für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen HBA und eGK und für die Autorisierung der SMC-B. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüs­sels aus EF.C.CA\_HPC.CS.E256 (siehe Tab\_HBA\_ObjSys\_011) prüfen. Das zu­ge­hörende private Schlüsselobjekt PrK.HPC.AUTR\_CVC.E256 ist im Kapitel 5.3.13 de­finiert.

**⌦ Card-G2-A\_2064 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.E256**

EF.C.HPC.AUTR\_CVC.E256 MUSS die in Tab\_HBA\_ObjSys\_014 dargestellten Werte besitzen.

Tabelle 16: Tab\_HBA\_ObjSys\_014 Initialisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.E256

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | transparentes Elementary File |  | |
| *fileIdentifier* | ‘2F 06’ |  | |
| *shortFileIdentifier* | ‘06’= 6 |  | |
| *numberOfOctet* | ‘00 DE’ Oktett = 222 Oktett |  | |
| *positionLogicalEndOfFile* | ‘0’ |  | |
| *flagTransactionMode* | True |  | |
| *flagChecksum* | False |  | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| *shareable* | True |  | |
| *body* | kein Inhalt | wird personalisiert | |
| Zugriffsregeln für die Kontaktschnittstelle | | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung | |
| Delete | AUT\_CMS OR AUT\_CUP | | siehe Hinweis 16: | |
| Read Binary | ALWAYS | |  | |
| Update Binary | AUT\_CMS OR AUT\_CUP | | siehe Hinweis 16: | |
| andere | NEVER | |  | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung | |
| alle | herstellerspezifisch | |  | |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung | |
| alle | herstellerspezifisch | |  | |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung | |
| Delete | AUT\_CMS OR AUT\_CUP | | siehe Hinweis 16: | |
| Read Binary | AUT\_PACE  OR AUT\_CMS  OR AUT\_CUP | |  | |
| Update Binary | AUT\_CMS OR AUT\_CUP | | siehe Hinweis 18: | |
| andere | NEVER | |  | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung | |
| alle | herstellerspezifisch | |  | |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung | |
| alle | herstellerspezifisch | |  | |

**⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

**⌦ Card-G2-A\_3386 K\_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTR\_CVC.E256**

Für die CHR in diesem Zertifikat MUSS CHR = ’00 06’ || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A\_2058].

**⌫**

**⌦ Card-G2-A\_3284 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.E256**

Bei der Personalisierung von EF.C.HPC.AUTR\_CVC.E256 MÜSSEN die in Tab\_HBA\_ObjSys\_093 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 17: Tab\_HBA\_ObjSys\_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | ‘00 DE’ Oktett = 222 Oktett |  |
| *body* | C.HPC.AUTR\_CVC.E256 gemäß [gemSpec\_PKI] |  |

**⌫**

### 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 zugehörende private Schlüsselobjekt PrK.HPC.AUTD\_SUK\_CVC.E256 ist im Ka­pi­tel 5.3.14 definiert.

**⌦ Card-G2-A\_2067 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTD\_SUK\_CVC.E256**

EF.C.HPC.AUTD\_SUK\_CVC.E256 MUSS die in Tab\_HBA\_ObjSys\_017 dargestellten Werte besitzen.

Tabelle 18: Tab\_HBA\_ObjSys\_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD\_SUK\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 09’ |  |
| *shortFileIdentifier* | ‘09’= 9 |  |
| *numberOfOctet* | ‘00 DE’ Oktett = 222 Oktett |  |
| *positionLogicalEndOfFile* | ‘0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird personalisiert |
| **Zugriffsregeln** | | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 16: |
| READ BINARY | ALWAYS |  |
| SELECT | ALWAYS |  |
| Update Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis 20: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 16: |
| READ BINARY | AUT\_PACE  OR AUT\_CMS  OR AUT\_CUP |  |
| Update Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis 20: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

**⌦ Card-G2-A\_3387 K\_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTD\_SUK\_CVC.E256**

Für die CHR in diesem Zertifikat MUSS CHR = ’00 09’ || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A\_2058].

**⌫**

**⌦ Card-G2-A\_3285 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTD\_SUK\_CVC.E256**

Bei der Personalisierung von EF.C.HPC.AUTD\_SUK\_CVC.E256 MÜSSEN die in Tab\_HBA\_ObjSys\_095 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 19: Tab\_HBA\_ObjSys\_095 Personalisierte Attribute von MF / EF.C.HPC.AUTD\_SUK\_CVC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| positionLogicalEndOfFile | ‘00 DE’ Oktett = 222 Oktett |  |
| body | C.HPC.AUTD\_SUK\_CVC.E256 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.HPC.AUTD\_SUK\_CVC.E256 |  |

**⌫**

### MF / PIN.CH

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

**⌦ Card-G2-A\_2069 K\_Initialisierung: Initialisierte Attribute von MF / PIN.CH**

PIN.CH MUSS die in Tab\_HBA\_ObjSys\_019 dargestellten Werte besitzen.

Tabelle 20: Tab\_HBA\_ObjSys\_019 Initialisierte Attribute von MF / PIN.CH

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘01’ = 1 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 6 |  |
| *maximumLength* | 8 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | Transport-PIN |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | undefiniert | wird personalisiert |
| *pukUsage* | 10 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Reset RC. P1 aus der Menge {0, 1} | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | AUT\_PACE |  |
| Get Pin Status | AUT\_PACE |  |
| Reset RC. P1 aus der Menge {0, 1} | AUT\_PACE |  |
| Verify | AUT\_PACE |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.

**⌦ Card-G2-A\_3286 K\_Personalisierung: Personalisierte Attribute von MF / PIN.CH**

Bei der Personalisierung von PIN.CH MÜSSEN die in Tab\_HBA\_ObjSys\_097 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 21: Tab\_HBA\_ObjSys\_097 Personalisierte Attribute von MF / PIN.CH

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis 22: |
| *PUK* | PUK-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |

**⌫**

1. 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.

**⌫**

### MF / PrK.HPC.AUTR\_CVC.R2048

PrK.HPC.AUTR\_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für C2C-Authentisierungen zwischen HBA/eGK. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTR\_CVC.R2048 ist in C.HPC.AUTR\_CVC.R2048 (siehe Kapitel 5.3.8) enthalten.

**⌦ Card-G2-A\_2071 K\_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR\_CVC.R2048**

PrK.HPC.AUTR\_CVC.R2048 MUSS die in Tab\_HBA\_ObjSys\_020 dargestellten Werte besitzen.

Tabelle 22: Tab\_HBA\_ObjSys\_020 Initialisierte Attribute von MF / PrK.HPC.AUTR\_CVC.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘10’ = 16 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge  {rsaRoleAuthentication} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *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 24: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘81’ | AUT\_PACE |  |
| Internal Authenticate | AUT\_PACE  AND PWD(PIN.CH) |  |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 24: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

**⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

**⌦ Card-G2-A\_3287 K\_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR\_CVC.R2048**

Bei der Personalisierung von PrK.HPC.AUTR\_CVC.R2048 MÜSSEN die in Tab\_HBA\_ObjSys\_098 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab\_HBA\_ObjSys\_098 Personalisierte Attribute von MF / PrK.HPC.AUTR\_CVC.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *privateKey* | Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | True |  |

**⌫**

### MF / PrK.HPC.AUTR\_CVC.E256

PrK.HPC.AUTR\_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für C2C-Authentisierungen zwischen HBA/eGK und HBA/CMS, und zur Autorisierung der SMC-B. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTR\_CVC.E256 ist in C.HPC.AUTR\_CVC.E256 (siehe Kapitel 5.3.9) ent­hal­ten.

**⌦ Card-G2-A\_2072 K\_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR\_CVC.E256**

PrK.HPC.AUTR\_CVC.E256 MUSS die in Tab\_HBA\_ObjSys\_021 dargestellten Werte besitzen.

Tabelle 24: Tab\_HBA\_ObjSys\_021 Initialisierte Attribute von MF / PrK.HPC.AUTR\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘06’ = 6 |  |
| *privateElcKey* | domainparameter = brainpoolP256r1 | wird personalisiert |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge  {elcRoleAuthentication} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *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 |  |

**⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

**⌦ Card-G2-A\_3288 K\_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR\_CVC.E256**

Bei der Personalisierung von PrK.HPC.AUTR\_CVC.E256 MÜSSEN die in Tab\_HBA\_ObjSys\_099 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 25: Tab\_HBA\_ObjSys\_099 Personalisierte Attribute von MF / PrK.HPC.AUTR\_CVC.E256

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

**⌫**

### 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 26: Tab\_HBA\_ObjSys\_024 Initialisierte Attribute von MF / PrK.HPC.AUTD\_SUK\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘09’ = 9 |  |
| *privateElcKey* | domainparameter = brainpoolP256r1 |  |
| *privateElcKey* | keyData = AttributNotSet | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | Ein Wert aus der Menge  {elcSessionkey4SM, elcAsynchronAdmin} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *numberScenarion* | 0 |  |
| *accessRuleSessionkeys* | irrelevant |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| General Authenticate | ALWAYS |  |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 28: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘81’ | AUT\_PACE |  |
| General Authenticate | ALWAYS |  |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 28: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

**⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

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

**⌦ Card-G2-A\_3289 K\_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTD\_SUK\_CVC.E256**

Bei der Personalisierung von PrK.HPC.AUTD\_SUK\_CVC.E256 MÜSSEN die in Tab\_HBA\_ObjSys\_101 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 27: Tab\_HBA\_ObjSys\_101 Personalisierte Attribute von MF / PrK.HPC.AUTD\_SUK\_CVC.E256

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

**⌫**

### Sicherheitsanker zum Import von CV-Zertifikaten

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

1. zwecks Abwärtskompatibilität zur Generation 1 Infrastruktur (PuK.RCA.CS.R2048),
2. zur unmittelbaren Ablösung der Generation 1 Algorithmen (PuK.RCA.CS.E256)

#### MF / PuK.RCA.CS.R2048

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

**⌦ Card-G2-A\_2077-01 K\_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.R2048**

PuK.RCA.CS.R2048 MUSS die in Tab\_HBA\_ObjSys\_026 dargestellten Werte besitzen.

Tabelle 28: Tab\_HBA\_ObjSys\_026 Initialisierte Attribute von MF / PuK.RCA.CS.R2048

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute | | Wert | | Bemerkung |
| Objekttyp | | öffentliches RSA Signaturprüfobjekt | |  |
| Für Echtkarten MÜSSEN die beiden folgenden Attribute mit den dort angegebenen Werten initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden. | | | | | |
| *keyIdentifier* | | RSA 2048 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes) | |  |
| *publicKey* | | Öffentlicher Schlüssel mit Moduluslänge 2048 Bit gemäß [gemSpec\_PKI#6.4.1.6] und gemäß [gemSpec\_CVC\_TSP#4.5] | |  |
| *oid* | | sigS\_ISO9796-2Withrsa\_sha256  ‘2B240304020204’ = {1.3.36.3.4.2.2.4} | |  |
| *lifeCycleStatus* | | „Operational state (activated)“ | |  |
| *accessRulesPublicSignatureVerificationObject* | | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt:  Delete 🡪 AUT\_CMS OR AUT\_CUP  PSO Verify Certificate 🡪 ALWAYS | |  |
| *accessRulesPublic AuthenticationObject* | | 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 | |  | |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.
3. Es ist möglich, dass importierte Authentisierungsschlüssel auch zum Aufbau eines Trusted Channels verwendet werden. Dabei wird das Kommando General Authenticate verwendet. Deshalb ist es erforderlich, dass importierte Authentisierungsschlüssel das Kommando General Authenticate unterstützen. Die Zugriffsart General Authenticate fehlt in der oben genannten Zugriffsregel, weil gemäß [gemSpec\_COS]] dabei lediglich für private Schlüssel, nicht aber für öffentliche Schlüssel Zugriffsregeln ausgewertet werden. Falls das herstellerspezifische COS im Rahmen eines General Authenticate Kommandos auch Zugriffsregeln für öffentliche Schlüssel auswertet, dann ist eine entsprechende Zugriffsart herstellerspezifisch mit der Zugriffsbedingung ALWAYS zu ergänzen.

**⌦ Card-G2-A\_3326 K\_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten**

Bei der Personalisierung von PuK.RCA.CS.R2048 für Testkarten MÜSSEN die in Tab\_HBA\_ObjSys\_152 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 29: Tab\_HBA\_ObjSys\_152 Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *publicKey* | Öffentlicher Schlüssel mit Moduluslänge 2048 Bit gemäß [gemSpec\_PKI#6.4.1.6] aus Test-CVC-Root | personalisieren gemäß [gemSpec\_TK#3.1.2] |
| *keyIdentifier* | RSA 2048 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels |  |

**⌫**

#### 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 30: Tab\_HBA\_ObjSys\_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256

| Attribute | Wert | Bemerkung |
| --- | --- | --- |
| Objekttyp | öffentliches ELC Signaturprüfobjekt |  |
| Für Echtkarten MÜSSEN die vier folgenden Attribute mit den unten angegebenen Werten initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die vier folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden. | | | |
| *keyIdentifier* | E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes) |  | |
| *expirationDate* | Jahr Monat Tag im Format YYMMDD gemäß [gemSpec\_PKI#6.7.2.6], Wert gemäß [gemSpec\_CVC\_Root#5.4.2] |  | |
| CHAT | OIDflags     = oid\_cvc\_fl\_ti  flagList     = ‘FF 0084 2006 00E3’ | siehe Hinweis 32: |
| *publicKey* | Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec\_PKI#6.7.2.3] und gemäß [gemSpec\_CVC\_TSP[gemSpec\_CVC\_TSP#4.5] |  | |
| Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden. | | | |
| *oid* | ecdsa-with-SHA256  ‘2A8648CE3D040302’ = {1.2.840.10045.4.3.2} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *accessRulesPublicSignatureVerificationObject* | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt:  Delete 🡪 ALWAYS AUT\_CMS OR AUT\_CUP  PSO Verify Certificate 🡪 ALWAYS |  |
| *accessRulesPublicAuthenticationObject* | 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 |  |

**⌫**

1. 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 31: Tab\_HBA\_ObjSys\_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| *publicKey* | Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec\_PKI#6.7.2.3] aus Test-CVC-CA | personalisieren gemäß [gemSpec\_TK#3.1.2] |
| *keyIdentifier* | E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels |  |
| CHAT | * OIDflags     = oid\_cvc\_fl\_ti * flagList     = ‘FF 0084 2006 00E3’ |  |
| *expirationDate* | Jahr Monat Tag im Format YYMMDD gemäß [gemSpec\_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels |  |

**⌫**

### 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.

#### 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**

1. PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab\_HBA\_ObjSys\_082 dargestellten Attribute besitzen.

Tabelle 32: Tab\_HBA\_ObjSys\_082 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | öffentliches Signaturprüfobjekt, ELC 256 |  |
| Für Echtkarten MÜSSEN die beiden folgenden Attribute mit den unten angegebenen Werten initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| CHAT | * OIDflags = 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate
2. 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 33: Tab\_HBA\_ObjSys\_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *publicKey* | Domainparameter = brainpoolP256r1 gemäß [gemSpec\_PKI#6.7.2.3] |  |
| *publicKey*  Option\_Erstellung \_von\_Testkarten | Domainparameter = brainpoolP256r1 gemäß [gemSpec\_PKI#6.7.2.3] aus Test-Admin-CVC-Root |  |
| CHAT | * OIDflags = oid\_cvc\_fl\_cms   flagList = ‘FF BFFF FFFF FFFF’ |  |
| expirationDate  Option\_Erstellung \_von\_Testkarten | Identisch zu „expirationDate“ des personalisierten PuK.RCA.CS.E256 |  |

**⌫**

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

#### 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 34: Tab\_HBA\_ObjSys\_029 Initialisierte Attribute von MF / SK.CMS.AES128

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-128 |  |
| *keyIdentifier* | ‘14’ = 20 |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *accessRuleSession keys* | irrelevant |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Mutual Authenticate | ALWAYS |  |
| 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 |  |

**⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

**⌦ Card-G2-A\_3291 K\_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES128 die in Tab\_HBA\_ObjSys\_104 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 35: Tab\_HBA\_ObjSys\_104 Personalisierte Attribute von MF / SK.CMS.AES128

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| *encKey* | Symmetrischer Schlüssel AES.128 gemäß [gemSpec\_Krypt#2.4] |  |
| *macKey* | Symmetrischer Schlüssel AES.128 gemäß [gemSpec\_Krypt#2.4] |  |

**⌫**

#### 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 36: Tab\_HBA\_ObjSys\_030 Initialisierte Attribute von MF / SK.CMS.AES256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-256 |  |
| *keyIdentifier* | ‘18’ = 24 |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *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 |  |

**⌫**

**⌦ Card-G2-A\_3292 K\_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256**

Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES256 die in Tab\_HBA\_ObjSys\_105 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 37: Tab\_HBA\_ObjSys\_105 Personalisierte Attribute von MF / SK.CMS.AES256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *encKey* | Symmetrischer Schlüssel AES.256 gemäß [gemSpec\_Krypt#2.4] |  |
| *macKey* | Symmetrischer Schlüssel AES.256 gemäß [gemSpec\_Krypt#2.4] |  |

**⌫**

#### 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 38: Tab\_HBA\_ObjSys\_147 Initialisierte Attribute von MF / SK.CUP.AES128

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-128 |  |
| *keyIdentifier* | ’03’ = 3 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *accessRuleSessionkeys* | irrelevant |  |
| Zugriffsregeln 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 39: Tab\_HBA\_ObjSys\_148 Personalisierte Attribute von MF / SK.CUP.AES128

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| *encKey* | Symmetrischer Schlüssel AES.128 gemäß [gemSpec\_Krypt#2.4] |  |
| *macKey* | Symmetrischer Schlüssel AES.128 gemäß [gemSpec\_Krypt#2.4] |  |

**⌫**

#### 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 40: Tab\_HBA\_ObjSys\_149 Initialisierte Attribute von MF / SK.CUP.AES256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-256 |  |
| *keyIdentifier* | ’04’ = 4 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *accessRuleSessionkeys* | irrelevant |  |
| Zugriffsregeln 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 41: Tab\_HBA\_ObjSys\_150 Personalisierte Attribute von MF / SK.CUP.AES256

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| *encKey* | Symmetrischer Schlüssel AES.256 gemäß [gemSpec\_Krypt#2.4] |  |
| *macKey* | Symmetrischer Schlüssel AES.256 gemäß [gemSpec\_Krypt#2.4] |  |

**⌫**

### 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**

1. Wird die kontaktlose Schnittstelle genutzt, dann MUSS SK.CAN vorhanden sein und die in Tab\_HBA\_ObjSys\_076 dargestellten Attribute besitzen.

Tabelle 42: Tab\_HBA\_ObjSys\_076 Initialisierte Attribute von MF / SK.CAN

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | symmetrisches Kartenverbindungsobjekt |  |
| *keyIdentifier* | ’02’ = 2 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Can | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für ein Schlüsselobjekt SK.CAN |  |
| *algorithmIdentifier* | id-PACE-ECDH-GM-AES-CBC-CMAC-128 |  |
| *accessRuleSessionkeys* | irrelevant |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| General Authenticate | ALWAYS |  |
| Delete | AUT\_CMS OR AUT\_CUP |  |
| Andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Alle | NEVER |  |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| General Authenticate | ALWAYS |  |
| Delete | AUT\_CMS OR AUT\_CUP |  |
| Andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Alle | NEVER |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit symmetrischen Kartenverbindungsobjekten arbeiten, sind: Activate; Deactivate; Delete, General Authenticate, Terminate.

**⌦ Card-G2-A\_3297 K\_Personalisierung: Personalisierte Attribute von MF / SK.CAN**

Bei der Personalisierung von SK.CAN MÜSSEN die in Tab\_HBA\_ObjSys\_106 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 43: Tab\_HBA\_ObjSys\_106 Personalisierte Attribute von MF / SK.CAN

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *can* | SK.CAN gemäß [gemSpec\_CAN\_TI] | siehe [Card-G2-A\_2869] |

**⌫**

**⌦** **Card-G2-A\_2869 K\_Personalisierung: Generierung der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle des HBA**

1. 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.
2. **⌫**

### 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.

## Die Heilberufsanwendung DF.HPA

### 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

### MF / DF.HPA (Health Professional Application)

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

**⌦ Card-G2-A\_2082 K\_Initialisierung: Initialisierte Attribute von MF / DF.HPA**

DF.HPA MUSS die in Tab\_HBA\_ObjSys\_031 dargestellten Werte besitzen.

Tabelle 44: Tab\_HBA\_ObjSys\_031 Initialisierte Attribute von MF / DF.HPA

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D27600014602’ |  |
| *fileIdentifier* | – |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load *Application*  (nach der HBA-Ausgabe) | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application  (nach der HBA-Ausgabe) | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.

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

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

**⌦ Card-G2-A\_2083 K\_Initialisierung: Initialisierte Attribute von MF / DF.HPA / EF.HPD**

EF.HPD MUSS die in Tab\_HBA\_ObjSys\_032 dargestellten Werte besitzen.

Tabelle 45: Tab\_HBA\_ObjSys\_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘D0 01’ |  |
| *shortFileIdentifier* | ‘01’= 1 |  |
| *numberOfOctet* | ‘08 00’ Oktett = 2048 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird später nachgeladen |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | AUT\_PACE |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.

#### Sicherheitsumgebungen

In DF.HPA wird das SE#1 verwendet.

## 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.

### Dateistruktur und Dateiinhalt

Die Abbildung Abb\_HBA\_ObjSys\_003 zeigt die prinzipielle Dateistruktur der QES-Anwendung, die in Überein­stimmung mit [DIN66291-1] definiert ist.



Abbildung 3: Abb\_HBA\_ObjSys\_003 Prinzipielle Struktur der QES-Anwendung

Die QES-Anwendung besitzt EFs für das X.509-QES-Zertifikat und maximal drei Attri­but­zer­tifikate, jeweils für die Kryptographie mit RSA und mit elliptischen Kurven. Zusätzlich ist ein EF zur Anzeige des unterstützten Maximal­wertes des SSEC angelegt.

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

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

**⌦ Card-G2-A\_2084 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES**

DF.QES MUSS die in Tab\_HBA\_ObjSys\_033 dargestellten Werte besitzen.

Tabelle 46: Tab\_HBA\_ObjSys\_033 Initialisierte Attribute von MF / DF.QES

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D276000066 01’ | siehe Hinweis 41: |
| *fileIdentifier* | – | siehe Hinweis 42: |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application | AUT\_CMS | Siehe Hinweis 43: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application | AUT\_CMS | Siehe Hinweis 43: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.
3. herstellerspezifisch; Falls un­ter­stützt, dann außerhalb des In­ter­valls [‘1000’, ‘FEFF’]; siehe [ISO7816-4#8.1.1]
4. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

#### 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 47: Tab\_HBA\_ObjSys\_034 Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt RSA 2048 |  |
| *keyIdentifier* | ‘04’ = 4 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 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  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 |  |

**⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.
3. Die konkrete Zugriffsregel muss durch den Objektsystemhersteller in Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS) festgelegt werden.
4. Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115]. Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)
5. 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 48: Tab\_HBA\_ObjSys\_108 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *privateKey* | Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | True |  |

**⌫**

#### MF / DF.QES / PIN.QES

PIN.QES ist eine DF-spezifische PIN, die nur zum Schutz des privaten Schlüssels für die qualifizierte elek­tro­ni­sche Signatur des Heilberuflers (PrK.HP.QES.R2048) gemäß 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 49: Tab\_HBA\_ObjSys\_037 Initialisierte Attribute von MF / DF.QES / PIN.QES

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘01’ = 1 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 6 |  |
| *maximumLength* | 8 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | Transport-PIN |  |
| *flagEnabled* | True |  |
| *Start Security Status Evaluation Counter* | SE # 1: 1 ≤ SSEC ≤ 250  SE # 2: 1 ≤ SSEC ≤ 250 | Werte wie in EF.SSEC angezeigt |
| PUK | undefiniert | wird personalisiert |
| *pukUsage* | 10 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Reset RC., P1=1 | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | SmMac(flagTI.54)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(flagTI.55) |  |
| Reset RC., P1=1 | SmMac(flagTI.54)  AND SmCmdEnc |  |
| Verify | SmMac(flagTI.54)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | AUT\_PACE |  |
| Get Pin Status | AUT\_PACE |  |
| Reset RC., P1=1 | AUT\_PACE |  |
| Verify | AUT\_PACE |  |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | SmMac(flagTI.54)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(flagTI.55) |  |
| Reset RC., P1=1 | SmMac(flagTI.54)  AND SmCmdEnc |  |
| Verify | SmMac(flagTI.54)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.

**⌦ Card-G2-A\_3299 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / PIN.QES**

Bei der Personalisierung von PIN.QES MÜSSEN die in Tab\_HBA\_ObjSys\_111 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 50: Tab\_HBA\_ObjSys\_111 Personalisierte Attribute von MF / DF.QES / PIN.QES

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis 50: |
| *PUK* | PUK-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |

**⌫**

1. 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.

#### MF / DF.QES / EF.SSEC

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

**⌦ Card-G2-A\_2089 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.SSEC**

EF.SSEC MUSS die in Tab\_HBA\_ObjSys\_038 dargestellten Werte besitzen.

Tabelle 51: Tab\_HBA\_ObjSys\_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘D0 05’ |  |
| *shortFileIdentifier* | ‘05’ = 5 |  |
| *numberOfOctet* | ‘002E’ Oktett = 46 Oktett |  |
| *positionLogical EndOfFile* | ‘002E’ Oktett = 46 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | Inhalt gemäß den Werten für *Start SecurityStatus Evaluation Counter* für SE#1 und für SE#2 in PIN.QES (siehe Kapitel 5.5.2.2) |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart 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 |  |

**⌫**

1. 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 52: Tab\_HBA\_ObjSys\_039 Inhalt von EF.SSEC

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

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

Die transparente Datei EF.C.HP.QES.R2048 enthält das X.509-Zertifikat für die Krypto­gra­phie mit RSA mit dem öffentlichen Schlüssel des Heilberuflers PuK.HP.QES.R2048 für die qualifizierte elektronische Signatur gemäß EU-Verordnung Nr. 910/2014 (eIDAS). Das zugehörende 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 53: Tab\_HBA\_ObjSys\_040 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C0 00’ |  |
| *shortFileIdentifier* | ‘10’= 16 |  |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart 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 |  |

**⌫**

1. 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.
2. 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 54: Tab\_HBA\_ObjSys\_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

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

**⌫**

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

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

**⌦ Card-G2-A\_2094-01 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1**

EF.C.HP.QES-AC1 MUSS die in Tab\_HBA\_ObjSys\_042 dargestellten Werte besitzen.

Tabelle 55: Tab\_HBA\_ObjSys\_042 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | | **Wert** | **Bemerkung** |
| Objekttyp | | transparentes Elementary File |  |
| *fileIdentifier* | | ‘C0 01’ |  |
| *shortFileIdentifier* | | ‘01’ = 1 |  |
| *numberOfOctet* | | ’06 40’ Oktett = 1600 Oktett |  |
| *positionLogicalEndOfFile* | | ’0’ |  |
| *flagTransactionMode* | | True |  |
| *flagChecksum* | | False |  |
| *lifeCycleStatus* | | Operational state (activated) |  |
| *shareable* | | True |  |
| *body* | | kein Inhalt |  |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | | |
| Zugriffsart SE#1, SE#2 | Zugriffsbedingung | | Bemerkung |
| Read Binary | ALWAYS | |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) | | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Zugriffsart SE#1 | Zugriffsbedingung | | Bemerkung |
| Read Binary | AUT\_PACE | |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) | | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER | |  |
| Zugriffsart SE#2 | Zugriffsbedingung | | Bemerkung |
| Read Binary | SmMac(flagTI.55)  AND SmRspEnc | |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH)  AND SmMac(flagTI.55))  AND SmCmdEnc | | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

**⌦ Card-G2-A\_3302 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1**

Bei der Personalisierung von EF.C.HP.QES-AC1 KÖNNEN die in Tab\_HBA\_ObjSys\_115 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 56: Tab\_HBA\_ObjSys\_115 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1

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

**⌫**

**⌦ Card-G2-A\_2095-01 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2**

EF.C.HP.QES-AC2 MUSS die in Tab\_HBA\_ObjSys\_043 dargestellten Werte besitzen.

Tabelle 57: Tab\_HBA\_ObjSys\_043 Initialisierte Attri7bute von MF / DF.QES / EF.C.HP.QES-AC2

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C0 02’ |  |
| *shortFileIdentifier* | ‘02’ = 2 |  |
| *numberOfOctet* | ’06 40’ Oktett = 1600 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 SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Read Binary | AUT\_PACE |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | SmMac(flagTI.55)  AND SmRspEnc |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH)  AND SmMac(flagTI.55))  AND SmCmdEnc | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

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\_3303 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2**

Bei der Personalisierung von EF.C.HP.QES-AC2 KÖNNEN die in Tab\_HBA\_ObjSys\_116 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 58: Tab\_HBA\_ObjSys\_116 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2

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

**⌫**

**⌦ Card-G2-A\_2096-01 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3**

EF.C.HP.QES-AC3 MUSS die in Tab\_HBA\_ObjSys\_044 dargestellten Werte besitzen.

Tabelle 59: Tab\_HBA\_ObjSys\_044 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | transparentes Elementary File |  | |
| *fileIdentifier* | ‘C0 03’ |  | |
| *shortFileIdentifier* | ‘03’ = 3 |  | |
| *numberOfOctet* | ’06 40’ Oktett = 1600 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 SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Read Binary | AUT\_PACE |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | SmMac(flagTI.55)  AND SmRspEnc |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH)  AND SmMac(flagTI.55))  AND SmCmdEnc | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. 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\_3304 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3**

Bei der Personalisierung von EF.C.HP.QES-AC3 KÖNNEN die in Tab\_HBA\_ObjSys\_117 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 60: Tab\_HBA\_ObjSys\_117 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3

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

**⌫**

#### 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 61: Tab\_HBA\_ObjSys\_160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | 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(flagTI.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 62: Tab\_HBA\_ObjSys\_161 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *keyAvailable* | true |  |
| *privateElcKey* | keyData = Wildcard |  |

**⌫**

#### 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 Heilberuflers PuK.HP.QES.E256 für die qualifizierte elektronische Signatur gemäß EU-Verordnung Nr. 910/2014 (eIDAS). Das zugehörende 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 63: Tab\_HBA\_ObjSys\_162 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | transparentes Elementary File |  | |
| *fileIdentifier* | ‘C0 06’ |  | |
| *shortFileIdentifier* | ‘06’= 6 |  | |
| *numberOfOctet* | ‘0B B8’ Oktett = 3000 Oktett |  | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert | |
| *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 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 |  |

**⌫**

1. 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** |
| *positionLogical EndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.HP.QES.E256 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.HP.QES.E256 |  |

**⌫**

#### MF / DF.QES / EF.C.HP.QES-AC1.E256, MF / DF.QES / EF.C.HP.QES-AC2.E256 und MF / DF.QES / EF.C.HP.QES-AC3.E256

Die transparenten Dateien EF.C.HP.QES-AC1.E256, EF.C.HP.QES-AC2.E256 und EF.C.HP.QES-AC3E.256 können X.509-Attributzertifikate enthalten, z. B. von einer Heilberufskammer (z. B. Ärzte-kammer, Apothekerkammer) oder von einer entsprechenden Organisation (z. B. einer Ärztevereinigung). Die charakteristischen Dateiattribute und Zugriffsregeln sind in den nachfolgenden Tabellen dargestellt. Bei Nutzung eines neuen Zertifikates (EF.C.HP.QES.E256) müssen die vorhandenen Attributzertifikate durch neue ersetzt werden, die an das neue Zertifikat gebunden sind.

**⌦ Card-G2-A\_3633 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.E256**

EF.C.HP.QES-AC1.E256 MUSS die in Tab\_HBA\_ObjSys\_164 dargestellten Werte besitzen.

Tabelle 64: Tab\_HBA\_ObjSys\_164 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C0 07’ |  |
| *shortFileIdentifier* | ‘07’ = 7 |  |
| *numberOfOctet* | ’06 40’ Oktett = 1600 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Read Binary | AUT\_PACE |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | SmMac(flagTI.55)  AND SmRspEnc |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH)  AND SmMac(flagTI.55))  AND SmCmdEnc | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

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\_3634 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.E256**

Bei der Personalisierung von EF.C.HP.QES-AC1.E256 KÖNNEN die in Tab\_HBA\_ObjSys\_165 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 65: Tab\_HBA\_ObjSys\_165 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | Attributs-Zertifikat zu C.HP.QES.E256 |  |

**⌫**

**⌦ Card-G2-A\_3635 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.E256**

EF.C.HP.QES-AC2.E256 MUSS die in Tab\_HBA\_ObjSys\_166 dargestellten Werte besitzen.

Tabelle 66: Tab\_HBA\_ObjSys\_166 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C0 08’ |  |
| *shortFileIdentifier* | ‘08’ = 8 |  |
| *numberOfOctet* | ’06 40’ Oktett = 1600 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Read Binary | AUT\_PACE |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | SmMac(flagTI.55)  AND SmRspEnc |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH)  AND SmMac(flagTI.55))  AND SmCmdEnc | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

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\_3636 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.E256**

Bei der Personalisierung von EF.C.HP.QES-AC2.E256 KÖNNEN die in Tab\_HBA\_ObjSys\_167 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 67: Tab\_HBA\_ObjSys\_167 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | Attributs-Zertifikat zu C.HP.QES.E256 |  |

**⌫**

**⌦ Card-G2-A\_3637 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.E256**

EF.C.HP.QES-AC3.E256 MUSS die in Tab\_HBA\_ObjSys\_168 dargestellten Werte besitzen.

Tabelle 68: Tab\_HBA\_ObjSys\_168 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C0 09’ |  |
| *shortFileIdentifier* | ‘09’ = 9 |  |
| *numberOfOctet* | ’06 40’ Oktett = 1600 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart SE#1, SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart SE#1 | Zugriffsbedingung | Bemerkung |
| Read Binary | AUT\_PACE |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_PACE  AND PWD(PIN.CH) | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsart SE#2 | Zugriffsbedingung | Bemerkung |
| Read Binary | SmMac(flagTI.55)  AND SmRspEnc |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.CH)  AND SmMac(flagTI.55))  AND SmCmdEnc | Zugriffsregel von PIN.CH ist auf MF-Ebene definiert |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

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\_3638 K\_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.E256**

Bei der Personalisierung von EF.C.HP.QES-AC3.E256 KÖNNEN die in Tab\_HBA\_ObjSys\_169 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 69: Tab\_HBA\_ObjSys\_169 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | Attributs-Zertifikat zu C.HP.QES.E256 |  |

**⌫**

## Die ESIGN-Anwendung (DF.ESIGN)

### 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

### 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 70: Tab\_HBA\_ObjSys\_045 Initialisierte Attribute von MF / DF.ESIGN

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘A000000167 455349474E’ | siehe Hinweis 62: |
| *fileIdentifier* | – | siehe Hinweis 63: |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application | AUT\_CMS | siehe Hinweis 65: |
| 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 65: |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.
3. herstellerspezifisch; Falls un­ter­stützt, dann außerhalb des In­ter­valls [‘1000’, ‘FEFF’]; siehe [gemSpec\_COS#8.1.1].
4. Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.6 im Allgemeinen irrelevant.
5. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.9.

#### 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 71: Tab\_HBA\_ObjSys\_046 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘02’ = 2 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  {rsaClientAuthentication, 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 |  |

**⌫**

1. 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
2. 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 72: Tab\_HBA\_ObjSys\_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *privateKey* | Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | True |  |

**⌫**

#### 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 73: Tab\_HBA\_ObjSys\_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘03’ = 3 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  {rsaDecipherOaep, rsaDecipherPKCS1\_V1\_5} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 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 |  |

**⌫**

1. 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
2. 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 74: Tab\_HBA\_ObjSys\_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *privateKey* | Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | True |  |

**⌫**

#### 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 zugehörende private Schlüssel­ob­jekt PrK.HP.AUT.R2048 ist in Kapitel 5.6.2.1 definiert.

**⌦ Card-G2-A\_2107 K\_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048**

EF.C.HP.AUT.R2048 MUSS die in Tab\_HBA\_ObjSys\_055 dargestellten Werte besitzen.

Tabelle 75: Tab\_HBA\_ObjSys\_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | | **Wert** | **Bemerkung** |
| Objekttyp | | transparentes Elementary File |  |
| *fileIdentifier* | | ‘C5 00’ |  |
| *shortFileIdentifier* | | ‘01’= 1 |  |
| *numberOfOctet* | | ‘07 6C’ Oktett = 1900 Oktett |  |
| *positionLogicalEndOfFile* | | ’0’ |  |
| *flagTransactionMode* | | True |  |
| *flagChecksum* | | False |  |
| *lifeCycleStatus* | | „Operational state (activated)“ |  |
| *shareable* | | True |  |
| *body* | | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | | siehe Hinweis 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 | |  |

**⌫**

1. 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.
2. 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 76: Tab\_HBA\_ObjSys\_127 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.HP.AUT.R2048 gemäß [gemSpec\_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.AUT.R2048 |  |

**⌫**

#### 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 zugehörende 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 77: Tab\_HBA\_ObjSys\_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C2 00’ |  |
| *shortFileIdentifier* | ‘02’= 2 |  |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 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 |  |

**⌫**

1. 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.
2. 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 78: Tab\_HBA\_ObjSys\_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.HP.ENC.R2048 gemäß [gemSpec\_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.ENC.R2048 |  |

**⌫**

#### 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 79: Tab\_HBA\_ObjSys\_170 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attribute** | | **Wert** | **Bemerkung** | | |
| Objekttyp | | 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 | 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 | | |  |

**⌫**

1. 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
2. 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 80: Tab\_HBA\_ObjSys\_171 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *keyAvailable* | true |  |
| *privateElcKey* | keyData = Wildcard |  |

**⌫**

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

PrK.HP.ENC.E256 ist der private Schlüssel für die Kryptographie mit ellptischen 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 81: Tab\_HBA\_ObjSys\_172 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  | |
| *keyIdentifier* | ‘05’ = 5 |  | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| *privateElcKey* | *domainparameter = brainpoolP256r1* | wird personalisiert | |
| *privateElcKey* | *keyData = AttributNotSet* |  | |
| *keyAvailable* | WildCard |  | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, [gemSpec\_COS] {elcSharedSecretCalculation} |  | |
|  |  |  | |
| *accessRuleSessionkeys* | 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 |  |

**⌫**

1. 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
2. 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 82: Tab\_HBA\_ObjSys\_173 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *keyAvailable* | true |  |
| *privateElcKey* | keyData = Wildcard |  |

**⌫**

#### 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 zugehörende 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 83: Tab\_HBA\_ObjSys\_174 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute | Wert | | Bemerkung | |
| Objekttyp | transparentes Elementary File | |  | |
| *fileIdentifier* | ‘C5 06’ | |  | |
| *shortFileIdentifier* | ‘06’= 6 | |  | |
| *lifeCycleStatus* | „Operational state (activated)“ | |  | |
| *flagTransactionMode* | True | |  | |
| *flagChecksum* | False | |  | |
| *numberOfOctet* | ‘0B B8’ Oktett = 3000 Oktett | |  | |
| *positionLogicalEndOfFile* | ’0’ | | wird personalisiert | |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch | |  | |
| *body* | kein Inhalt | | wird personalisiert | |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 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 |  | |

**⌫**

1. 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.
2. 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 84: Tab\_HBA\_ObjSys\_175 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.HP.AUT.E256 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUT.E256 |  |

**⌫**

#### 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 zugehörende 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 85: Tab\_HBA\_ObjSys\_176 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute | Wert | | Bemerkung | |
| Objekttyp | transparentes Elementary File | |  | |
| *fileIdentifier* | ‘C2 05’ | |  | |
| *shortFileIdentifier* | ‘05’= 5 | |  | |
| *lifeCycleStatus* | „Operational state (activated)“ | |  | |
| *flagTransactionMode* | True | |  | |
| *flagChecksum* | False | |  | |
| *numberOfOctet* | ‘0B B8’ Oktett = 3000 Oktett | |  | |
| *positionLogicalEndOfFile* | ’0’ | | wird personalisiert | |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch | |  | |
| *body* | kein Inhalt | | wird personalisiert | |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung | |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis 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 |  | |

**⌫**

1. 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.
2. 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 86: Tab\_HBA\_ObjSys\_177 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.HP.ENC.E256 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.HP.ENC.E256 |  |

**⌫**

### 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.

## 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

### 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 87: Tab\_HBA\_ObjSys\_057 Initialisierte Attribute von MF / DF.CIA.QES

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | | Bemerkung |
| Objekttyp | Ordner | |  |
| *applicationIdentifier* | ‘'E828BD080F D27600006601’ | | siehe Hinweis 90: |
| *fileIdentifier* | – | | siehe Hinweis 91: |
| *lifeCycleStatus* | „Operational state (activated)“ | |  |
| *shareable* | True | |  |
| Zugriffsregeln für die Kontaktschnittstelle | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Get Random | ALWAYS | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Get Random | ALWAYS | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | | |
| Zugriffsart | | Zugriffsbedingung | Bemerkung |
| alle | | herstellerspezifisch |  |

**⌫**

#### 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 88: Tab\_HBA\_ObjSys\_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info)

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘50 32’ | siehe Hinweis 83: |
| *shortFileIdentifier* | ‘12’= 18 | siehe Hinweis 83: |
| *numberOfOctet* | ’ 00 A5’ Oktett = 165 Oktett |  |
| *positionLogicalEndOfFile* | ’ 00 A5’ Oktett = 165 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | 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  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 |  |

**⌫**

1. 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.
2. Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in in [ISO7816-15] festgelegt.

#### 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 89: Tab\_HBA\_ObjSys\_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 31’ | siehe Hinweis 85: |
| *shortFileIdentifier* | ‘11’ = 17 | siehe Hinweis 85: |
| *numberOfOctet* | ’00 18’ Oktett = 24 Oktett |  |
| *positionLogicalEndOfFile* | ’00 18’ Oktett = 24 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | 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 |  |

**⌫**

1. 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.
2. Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] [ISO7816-4] festgelegt.

#### 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 90: Tab\_HBA\_ObjSys\_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 34’ |  |
| *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* | 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 |  |
| 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 |  |

**⌫**

1. 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.

#### 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 91: Tab\_HBA\_ObjSys\_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 35’ |  |
| *shortFileIdentifier* | ‘15’ = 21 |  |
| *numberOfOctet* | ’00 B2’ Oktett = 178 Oktett |  |
| *positionLogicalEndOfFile* | ’00 B2’ Oktett = 178 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | 30 59  30 2C  0C 0A 50 72 4B 2E 48 50 2E 51 45 53  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 |  |
| 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 |  |

**⌫**

1. 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.

#### 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 92: Tab\_HBA\_ObjSys\_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD (Certificate Directory)

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 38’ |  |
| *shortFileIdentifier* | ‘16’ = 22 |  |
| *numberOfOctet* | ’01 50’ Oktett = 336 Oktett |  |
| *positionLogicalEndOfFile* | ’01 50’ Oktett = 336 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | 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  A0 29  30 0E  0C 0C 43 2E 48 50 2E 51 45 53  2D 41 43 31  30 03  04 01 84  A1 12  30 10  30 0E  A1 0C  4F 06 D2 76 00 00 66 01  04 02 C0 01  A0 29  30 0E  0C 0C 43 2E 48 50 2E 51 45 53  2D 41 43 32  30 03  04 01 84  A1 12  30 10  30 0E  A1 0C  4F 06 D2 76 00 00 66 01  04 02 C0 02  A0 29  30 0E  0C 0C 43 2E 48 50 2E 51 45 53  2D 41 43 33  30 03  04 01 84  A1 12  30 10  30 0E  A1 0C  4F 06 D2 76 00 00 66 01  04 02 C0 03  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  A0 29  30 0E  0C 0C 43 2E 48 50 2E 51 45 53  2D 41 43 31  30 03  04 01 86  A1 12  30 10  30 0E  A1 0C  4F 06 D2 76 00 00 66 01  04 02 C0 07  A0 29  30 0E  0C 0C 43 2E 48 50 2E 51 45 53  2D 41 43 32  30 03  04 01 86  A1 12  30 10  30 0E  A1 0C  4F 06 D2 76 00 00 66 01  04 02 C0 08  A0 29  30 0E  0C 0C 43 2E 48 50 2E 51 45 53  2D 41 43 33  30 03  04 01 86  A1 12  30 10  30 0E  A1 0C  4F 06 D2 76 00 00 66 01  04 02 C0 09 |  |
| 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 |  |

**⌫**

1. 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.

### 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 93: Tab\_HBA\_ObjSys\_058 Initialisierte Attribute von MF / DF.CIA.ESIGN

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘E828BD080F A000000167455349474E’ | siehe Hinweis 90: |
| *fileIdentifier* | – | siehe Hinweis 91: |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [ISO7816-15] sowie als PIX den applicationIdentifier von [ISO7816-4].
3. herstellerspezifisch; Falls un­ter­stützt, dann außerhalb des In­ter­valls [‘1000’, ‘FEFF’]; siehe [gemSpec\_COS# 8.1.1]
4. Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.7 im Allgemeinen irrelevant.

#### 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 94: Tab\_HBA\_ObjSys\_145 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo (Cryptographic Information Application Info)

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘50 32’ | siehe Hinweis 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* | 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  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 |  |

**⌫**

1. 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.
2. Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.

#### 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 95: Tab\_HBA\_ObjSys\_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 31’ | siehe Hinweis 85: |
| *shortFileIdentifier* | ‘11’ = 17 | siehe Hinweis 85: |
| *numberOfOctet* | ’0018’ Oktett = 2 Oktett |  |
| *positionLogicalEndOfFile* | ’0018’ Oktett = 2 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | 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 |  |

**⌫**

1. 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.
2. Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.

#### 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 96: Tab\_HBA\_ObjSys\_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 34’ |  |
| *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* | 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 |  |
| 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 |  |

**⌫**

1. 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.

#### 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 97: Tab\_HBA\_ObjSys\_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 35’ |  |
| *shortFileIdentifier* | ‘15’ = 21 |  |
| *numberOfOctet* | ’01 63’ Oktett = 355 Oktett |  |
| *positionLogicalEndOfFile* | ’01 63’ Oktett = 355 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | 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  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 84  03 02 05 20  03 02 03 B8  02 01 84  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 |  |
| 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 |  |

**⌫**

1. 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.

#### 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 98: Tab\_HBA\_ObjSys\_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)

| **Attribute** | **Wert** | **Bemerkung** |
| --- | --- | --- |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ’50 38’ |  |
| *shortFileIdentifier* | ‘16’ = 22 |  |
| *numberOfOctet* | ’00 AC’ Oktett = 172 Oktett |  |
| *positionLogicalEndOfFile* | ’00 AC’ Oktett = 172 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | Operational state (activated) |  |
| *shareable* | True |  |
| *body* | 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  30 0A  0C 08 43 2E 48 50 2E 41 55 54  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 C5 04  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 |  |
| 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 |  |

**⌫**

1. 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.

## 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.

### 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

### 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 99: Tab\_HBA\_ObjSys\_064 Initialisierte Attribute von MF / DF.AUTO

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D27600014603’ | siehe Hinweis 101: |
| *fileIdentifier* | – | siehe Hinweis 102: |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application | AUT\_CMS | siehe Hinweis 104: |
| 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 104: |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier ist in [ISO7816-4].
3. herstellerspezifisch; falls un­ter­stützt, dann außerhalb des In­ter­valls [‘1000’, ‘FEFF’]; siehe [gemSpec\_COS#8.1.1]
4. Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.8 im Allgemeinen irrelevant.
5. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.9.

#### 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 100: Tab\_HBA\_ObjSys\_065 Initialisierte Attribute von MF / DF:AUTO / PrK.HP.AUTO.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  |
| *keyIdentifier* | ‘02’ = 2 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 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 |  |

**⌫**

1. 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 101: Tab\_HBA\_ObjSys\_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *privateKey* | Moduluslänge 3072 Bit | wird personalisiert |
| *keyAvailable* | True |  |

**⌫**

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

#### MF / DF.AUTO / PIN.AUTO

PIN.AUTO ist eine DF-spezifische PIN, die ausschließ­lich dem Schutz des privaten Authen­ti­sierungs­schlüs­sels für den organisationsspezifischen Authenti­sie­rungs­mecha­nis­mus des Heilberuf­lers (PrK.HP.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 102: Tab\_HBA\_ObjSys\_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘01’ = 1 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 5 |  |
| *maximumLength* | 8 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer–PIN, Transport–PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | undefiniert | wird personalisiert |
| *pukUsage* | 10 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | ALWAYS | Hinweis 107: |
| Change RD, P1=1 | ALWAYS | Hinweis 108: |
| 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 107: |
| Change RD, P1=1 | AUT\_PACE | Hinweis 108: |
| 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 |  |

**⌫**

1. 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.
2. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
3. 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 herstellerspezifisch umzusetzen.

**⌫**

**⌦ Card-G2-A\_3315 K\_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO**

Wenn der Wert des Attributes *transportStatus* von PIN.AUTO Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.AUTO die in Tab\_HBA\_ObjSys\_141 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 103: Tab\_HBA\_ObjSys\_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *secret* | Transport-PIN | Wird personalisiert, siehe Hinweis 109: |
| *PUK* | PUK-Wert gemäß [gemSpec\_PINPUK\_TI] |  |

**⌫**

1. 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.

#### 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:ATUO / PIN.SO**

PIN.SO MUSS die in Tab\_HBA\_ObjSys\_069 dargestellten Werte besitzen.

Tabelle 104: Tab\_HBA\_ObjSys\_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘03’ = 3 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 6 |  |
| *maximumLength* | 8 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer–PIN, Transport–PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | undefiniert | wird personalisiert |
| *pukUsage* | 10 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | ALWAYS | Hinweis 111: |
| Change RD, P1=1 | ALWAYS | Hinweis 112: |
| 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 111: |
| Change RD, P1=1 | AUT\_PACE | Hinweis 112: |
| 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 |  |

**⌫**

1. 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.
2. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
3. 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 herstellerspezifisch umzusetzen.

**⌫**

**⌦ Card-G2-A\_3316 K\_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.SO**

Wenn der Wert des Attributes *transportStatus* von PIN.SO Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.SO die in Tab\_HBA\_ObjSys\_142 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 105: Tab\_HBA\_ObjSys\_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *secret* | Transport-PIN | Wird personalisiert, siehe Hinweis 113: |
| *PUK* | PUK-Wert gemäß [gemSpec\_PINPUK\_TI] |  |

**⌫**

1. 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.

#### 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 Heil­beruflers für die Kryptographie mit RSA. Damit können dem Heilberufler zwei verschiedene Identitäten zur Verfügung stehen, die beide mit demselben privaten Schlüssel PrK.HP.AUTO.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 106: Tab\_HBA\_ObjSys\_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

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

**⌫**

1. 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 107: Tab\_HBA\_ObjSys\_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | wird personalisiert |
| *body* | 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 108: Tab\_HBA\_ObjSys\_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute | Wert | | Bemerkung | |
| Objekttyp | transparentes Elementary File | |  | |
| *fileIdentifier* | ‘E0 02’ | |  | |
| *shortFileIdentifier* | ‘02’ = 2 | |  | |
| *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 |  |

**⌫**

**⌦ 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 109: Tab\_HBA\_ObjSys\_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | wird personalisiert |
| *body* | C.HP.AUTO2.R3072 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUTO.R3072 | wird personalisiert |

**⌫**

#### Sicherheitsumgebungen

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

#### 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.

**⌫**

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

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

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien und EF.Version2) nach der Aus­gabe des HBA von einem Card Application Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

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

# 

# Anhang A – Verzeichnisse

## A1 - Abkürzungen

| **Kürzel** | **Erläuterung** |
| --- | --- |
| AID | Application Identifier (Anwendungskennung) |
| AOD | Authentication Object Directory |
| APDU | Application Protocol Data Unit |
| ASN.1 | Abstract Syntax Notation One |
| ASCII | American Standard Code for Information Interchange |
| AT | Authentication Template |
| ATR | Answer-to-Reset |
| AUT | Authentisierung |
| AUTD | CV-basierte Geräteauthentisierung |
| AUTR | CV-basierte Rollenauthentisierung |
| AUTO | Organisationsspezifische Authentisierung |
| BA | Berufsausweis |
| BCD | Binary Coded Decimal |
| BER | Basic Encoding Rules |
| BNA | Bundesnetzagentur |
| C | Zertifikat |
| C2C | Card to Card |
| CA | Certification Authority (Zertifizierungsdiensteanbieter) |
| CAR | Certification Authority Reference |
| CC | Cryptographic Checksum (kryptographische Prüfsumme) |
| CD | Certificate Directory |
| CER | Canonical Encoding Rules |
| CG | Cryptogram |
| CH | Cardholder (Karteninhaber) |
| CHAT | Certificate Holder Autorisation Template Liste von Rechten, die ein Zertifikatsinhaber besitzt |
| CHR | Certificate Holder Reference |
| CIA | Cryptographic Information Application |
| CIO | Cryptographic Information Objects |
| CLA | Class-Byte einer Kommando-APDU |
| CMS | Card Management System |
| COS | Card Operating System (Chipkartenbetriebssystem) |
| CPI | Certificate Profile Identifier |
| 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 | Identifier |
| IFSC | Information Field Size Card |
| IIN | Issuer Identification Number |
| INS | Instruction-Byte einer Kommando-APDU |
| KM | Komfortmerkmal |
| KT | Kartenterminal |
| LCS | Life Cycle Status |
| LSB | Least Significant Byte(s) |
| MAC | Message Authentication Code |
| MF | Master File |
| MII | Major Industry Identifier |
| MSE | Manage Security Environment |
| OCSP | Online Certificate Status Protocol |
| OD | Object Directory |
| OID | Object Identifier |
| OSIG | Organisationssignatur |
| PIN | Personal Identification Number |
| PIX | Proprietary Application Provider Extension |
| PK, PuK | Public Key |
| PKCS | Public Key Cryptography Standard (hier PKCS#1) |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure for X.509 Certificates (IETF) |
| PrK | Private Key |
| PSO | Perform Security Operation |
| PUK | Personal Unblocking Key (Resetting Code) |
| PV | Plain Value |
| P1 | Parameter P1 einer Kommando-APDU |
| P2 | Parameter P2 einer Kommando-APDU |
| QES | Qualifizierte Elektronische Signatur |
| RA | Registration Authority (Registrierungsinstanz) |
| RAM | Random Access Memory |
| RC | Retry Counter (Fehlbedienungszähler) |
| RCA | Root CA |
| RD | Referenzdaten |
| RF | Radio Frequency |
| RFC | Request für Comment |
| RFID | Radio Frequency Identification |
| RFU | Reserved for future use |
| RID | Registered Application Provider Identifier |
| 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 |

## A2 - Glossar

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

## A3 – Abbildungsverzeichnis

[Abbildung 1: Abb\_HBA\_ObjSys\_001 Allgemeine Dateistruktur eines HBA 21](#_Toc500841155)

[Abbildung 2: Abb\_HBA\_ObjSys\_002 Dateistruktur von DF.HPA 64](#_Toc500841156)

[Abbildung 3: Abb\_HBA\_ObjSys\_003 Prinzipielle Struktur der QES-Anwendung 67](#_Toc500841157)

[Abbildung 4: Abb\_HBA\_ObjSys\_004 Prinzipielle Struktur von DF.ESIGN 94](#_Toc500841158)

[Abbildung 5: Abb\_HBA\_ObjSys\_005 DF.CIA-Anwendungen und ihre Unterstrukturen 112](#_Toc500841159)

[Abbildung 6: Abb\_HBA\_ObjSys\_006 Prinzipielle Struktur von DF.AUTO 136](#_Toc500841160)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_HBA\_ObjSys\_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt 10](#_Toc500841162)

[Tabelle 2: Tab\_HBA\_ObjSys\_003 ATR-Kodierung (Sequenz von oben nach unten) 20](#_Toc500841163)

[Tabelle 3: Tab\_HBA\_ObjSys\_004 Initialisierte Attribute von MF 21](#_Toc500841164)

[Tabelle 4: Tab\_HBA\_ObjSys\_005 Initialisierte Attribute von MF / EF.ATR 23](#_Toc500841165)

[Tabelle 5: Tab\_HBA\_ObjSys\_083 Initialisierte Attribute von MF / EF.CardAccess 24](#_Toc500841166)

[Tabelle 6: Tab\_HBA\_ObjSys\_007 Initialisierte Attribute von MF / EF.DIR 25](#_Toc500841167)

[Tabelle 7: Tab\_HBA\_ObjSys\_008 Initialisierte Attribute von MF / EF.GDO 27](#_Toc500841168)

[Tabelle 8: Tab\_HBA\_ObjSys\_151 Personalisierte Attribute von MF / EF.GDO 28](#_Toc500841169)

[Tabelle 9: Tab\_HBA\_ObjSys\_009 Initialisierte Attribute von MF / EF.Version2 29](#_Toc500841170)

[Tabelle 10: Tab\_HBA\_ObjSys\_010 Initialisierte Attribute von MF / EF.C.CA\_HPC.CS.R2048 30](#_Toc500841171)

[Tabelle 11: Tab\_HBA\_ObjSys\_089 Personalisierte Attribute von MF / EF.C.CA\_HPC.CS.R2048 32](#_Toc500841172)

[Tabelle 12: Tab\_HBA\_ObjSys\_011 Initialisierte Attribute von MF / EF.C.CA\_HPC.CS.E256 32](#_Toc500841173)

[Tabelle 13: Tab\_HBA\_ObjSys\_090 Personalisierte Attribute von MF / EF.C.CA\_HPC.CS.E256 33](#_Toc500841174)

[Tabelle 14: Tab\_HBA\_ObjSys\_013 Initialisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.R2048 34](#_Toc500841175)

[Tabelle 15: Tab\_HBA\_ObjSys\_092 Personalisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.R2048 35](#_Toc500841176)

[Tabelle 16: Tab\_HBA\_ObjSys\_014 Initialisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.E256 36](#_Toc500841177)

[Tabelle 17: Tab\_HBA\_ObjSys\_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR\_CVC.E256 37](#_Toc500841178)

[Tabelle 18: Tab\_HBA\_ObjSys\_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD\_SUK\_CVC.E256 38](#_Toc500841179)

[Tabelle 19: Tab\_HBA\_ObjSys\_095 Personalisierte Attribute von MF / EF.C.HPC.AUTD\_SUK\_CVC.E256 40](#_Toc500841180)

[Tabelle 20: Tab\_HBA\_ObjSys\_019 Initialisierte Attribute von MF / PIN.CH 40](#_Toc500841181)

[Tabelle 21: Tab\_HBA\_ObjSys\_097 Personalisierte Attribute von MF / PIN.CH 41](#_Toc500841182)

[Tabelle 22: Tab\_HBA\_ObjSys\_020 Initialisierte Attribute von MF / PrK.HPC.AUTR\_CVC.R2048 42](#_Toc500841183)

[Tabelle 23: Tab\_HBA\_ObjSys\_098 Personalisierte Attribute von MF / PrK.HPC.AUTR\_CVC.R2048 44](#_Toc500841184)

[Tabelle 24: Tab\_HBA\_ObjSys\_021 Initialisierte Attribute von MF / PrK.HPC.AUTR\_CVC.E256 44](#_Toc500841185)

[Tabelle 25: Tab\_HBA\_ObjSys\_099 Personalisierte Attribute von MF / PrK.HPC.AUTR\_CVC.E256 46](#_Toc500841186)

[Tabelle 26: Tab\_HBA\_ObjSys\_024 Initialisierte Attribute von MF / PrK.HPC.AUTD\_SUK\_CVC.E256 46](#_Toc500841187)

[Tabelle 27: Tab\_HBA\_ObjSys\_101 Personalisierte Attribute von MF / PrK.HPC.AUTD\_SUK\_CVC.E256 48](#_Toc500841188)

[Tabelle 28: Tab\_HBA\_ObjSys\_026 Initialisierte Attribute von MF / PuK.RCA.CS.R2048 48](#_Toc500841189)

[Tabelle 29: Tab\_HBA\_ObjSys\_152 Personalisierte Attribute von MF / PuK.RCA.CS.R2048 für Testkarten 50](#_Toc500841190)

[Tabelle 30: Tab\_HBA\_ObjSys\_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256 50](#_Toc500841191)

[Tabelle 31: Tab\_HBA\_ObjSys\_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten 52](#_Toc500841192)

[Tabelle 32: Tab\_HBA\_ObjSys\_082 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 53](#_Toc500841193)

[Tabelle 33: Tab\_HBA\_ObjSys\_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 55](#_Toc500841194)

[Tabelle 34: Tab\_HBA\_ObjSys\_029 Initialisierte Attribute von MF / SK.CMS.AES128 56](#_Toc500841195)

[Tabelle 35: Tab\_HBA\_ObjSys\_104 Personalisierte Attribute von MF / SK.CMS.AES128 57](#_Toc500841196)

[Tabelle 36: Tab\_HBA\_ObjSys\_030 Initialisierte Attribute von MF / SK.CMS.AES256 58](#_Toc500841197)

[Tabelle 37: Tab\_HBA\_ObjSys\_105 Personalisierte Attribute von MF / SK.CMS.AES256 59](#_Toc500841198)

[Tabelle 38: Tab\_HBA\_ObjSys\_147 Initialisierte Attribute von MF / SK.CUP.AES128 59](#_Toc500841199)

[Tabelle 39: Tab\_HBA\_ObjSys\_148 Personalisierte Attribute von MF / SK.CUP.AES128 60](#_Toc500841200)

[Tabelle 40: Tab\_HBA\_ObjSys\_149 Initialisierte Attribute von MF / SK.CUP.AES256 61](#_Toc500841201)

[Tabelle 41: Tab\_HBA\_ObjSys\_150 Personalisierte Attribute von MF / SK.CUP.AES256 62](#_Toc500841202)

[Tabelle 42: Tab\_HBA\_ObjSys\_076 Initialisierte Attribute von MF / SK.CAN 62](#_Toc500841203)

[Tabelle 43: Tab\_HBA\_ObjSys\_106 Personalisierte Attribute von MF / SK.CAN 63](#_Toc500841204)

[Tabelle 44: Tab\_HBA\_ObjSys\_031 Initialisierte Attribute von MF / DF.HPA 64](#_Toc500841205)

[Tabelle 45: Tab\_HBA\_ObjSys\_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD 65](#_Toc500841206)

[Tabelle 46: Tab\_HBA\_ObjSys\_033 Initialisierte Attribute von MF / DF.QES 68](#_Toc500841207)

[Tabelle 47: Tab\_HBA\_ObjSys\_034 Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048 69](#_Toc500841208)

[Tabelle 48: Tab\_HBA\_ObjSys\_108 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048 71](#_Toc500841209)

[Tabelle 49: Tab\_HBA\_ObjSys\_037 Initialisierte Attribute von MF / DF.QES / PIN.QES 71](#_Toc500841210)

[Tabelle 50: Tab\_HBA\_ObjSys\_111 Personalisierte Attribute von MF / DF.QES / PIN.QES 73](#_Toc500841211)

[Tabelle 51: Tab\_HBA\_ObjSys\_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC 74](#_Toc500841212)

[Tabelle 52: Tab\_HBA\_ObjSys\_039 Inhalt von EF.SSEC 75](#_Toc500841213)

[Tabelle 53: Tab\_HBA\_ObjSys\_040 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048 76](#_Toc500841214)

[Tabelle 54: Tab\_HBA\_ObjSys\_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048 78](#_Toc500841215)

[Tabelle 55: Tab\_HBA\_ObjSys\_042 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1 79](#_Toc500841216)

[Tabelle 56: Tab\_HBA\_ObjSys\_115 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1 80](#_Toc500841217)

[Tabelle 57: Tab\_HBA\_ObjSys\_043 Initialisierte Attri7bute von MF / DF.QES / EF.C.HP.QES-AC2 81](#_Toc500841218)

[Tabelle 58: Tab\_HBA\_ObjSys\_116 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2 82](#_Toc500841219)

[Tabelle 59: Tab\_HBA\_ObjSys\_044 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3 82](#_Toc500841220)

[Tabelle 60: Tab\_HBA\_ObjSys\_117 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3 84](#_Toc500841221)

[Tabelle 61: Tab\_HBA\_ObjSys\_160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256 84](#_Toc500841222)

[Tabelle 62: Tab\_HBA\_ObjSys\_161 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256 86](#_Toc500841223)

[Tabelle 63: Tab\_HBA\_ObjSys\_162 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256 86](#_Toc500841224)

[Tabelle 64: Tab\_HBA\_ObjSys\_164 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.E256 89](#_Toc500841225)

[Tabelle 65: Tab\_HBA\_ObjSys\_165 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC1.E256 90](#_Toc500841226)

[Tabelle 66: Tab\_HBA\_ObjSys\_166 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.E256 90](#_Toc500841227)

[Tabelle 67: Tab\_HBA\_ObjSys\_167 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC2.E256 92](#_Toc500841228)

[Tabelle 68: Tab\_HBA\_ObjSys\_168 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.E256 92](#_Toc500841229)

[Tabelle 69: Tab\_HBA\_ObjSys\_169 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES-AC3.E256 94](#_Toc500841230)

[Tabelle 70: Tab\_HBA\_ObjSys\_045 Initialisierte Attribute von MF / DF.ESIGN 95](#_Toc500841231)

[Tabelle 71: Tab\_HBA\_ObjSys\_046 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048 96](#_Toc500841232)

[Tabelle 72: Tab\_HBA\_ObjSys\_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048 98](#_Toc500841233)

[Tabelle 73: Tab\_HBA\_ObjSys\_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048 98](#_Toc500841234)

[Tabelle 74: Tab\_HBA\_ObjSys\_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048 100](#_Toc500841235)

[Tabelle 75: Tab\_HBA\_ObjSys\_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048 100](#_Toc500841236)

[Tabelle 76: Tab\_HBA\_ObjSys\_127 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048 102](#_Toc500841237)

[Tabelle 77: Tab\_HBA\_ObjSys\_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048 102](#_Toc500841238)

[Tabelle 78: Tab\_HBA\_ObjSys\_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048 103](#_Toc500841239)

[Tabelle 79: Tab\_HBA\_ObjSys\_170 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256 104](#_Toc500841240)

[Tabelle 80: Tab\_HBA\_ObjSys\_171 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256 105](#_Toc500841241)

[Tabelle 81: Tab\_HBA\_ObjSys\_172 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256 106](#_Toc500841242)

[Tabelle 82: Tab\_HBA\_ObjSys\_173 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256 107](#_Toc500841243)

[Tabelle 83: Tab\_HBA\_ObjSys\_174 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256 108](#_Toc500841244)

[Tabelle 84: Tab\_HBA\_ObjSys\_175 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256 109](#_Toc500841245)

[Tabelle 85: Tab\_HBA\_ObjSys\_176 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256 109](#_Toc500841246)

[Tabelle 86: Tab\_HBA\_ObjSys\_177 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256 111](#_Toc500841247)

[Tabelle 87: Tab\_HBA\_ObjSys\_057 Initialisierte Attribute von MF / DF.CIA.QES 112](#_Toc500841248)

[Tabelle 88: Tab\_HBA\_ObjSys\_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info) 113](#_Toc500841249)

[Tabelle 89: Tab\_HBA\_ObjSys\_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD 115](#_Toc500841250)

[Tabelle 90: Tab\_HBA\_ObjSys\_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) 116](#_Toc500841251)

[Tabelle 91: Tab\_HBA\_ObjSys\_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory) 118](#_Toc500841252)

[Tabelle 92: Tab\_HBA\_ObjSys\_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD (Certificate Directory) 121](#_Toc500841253)

[Tabelle 93: Tab\_HBA\_ObjSys\_058 Initialisierte Attribute von MF / DF.CIA.ESIGN 123](#_Toc500841254)

[Tabelle 94: Tab\_HBA\_ObjSys\_145 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo (Cryptographic Information Application Info) 125](#_Toc500841255)

[Tabelle 95: Tab\_HBA\_ObjSys\_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory) 127](#_Toc500841256)

[Tabelle 96: Tab\_HBA\_ObjSys\_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) 128](#_Toc500841257)

[Tabelle 97: Tab\_HBA\_ObjSys\_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory) 130](#_Toc500841258)

[Tabelle 98: Tab\_HBA\_ObjSys\_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory) 133](#_Toc500841259)

[Tabelle 99: Tab\_HBA\_ObjSys\_064 Initialisierte Attribute von MF / DF.AUTO 136](#_Toc500841260)

[Tabelle 100: Tab\_HBA\_ObjSys\_065 Initialisierte Attribute von MF / DF:AUTO / PrK.HP.AUTO.R3072 137](#_Toc500841261)

[Tabelle 101: Tab\_HBA\_ObjSys\_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072 139](#_Toc500841262)

[Tabelle 102: Tab\_HBA\_ObjSys\_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO 140](#_Toc500841263)

[Tabelle 103: Tab\_HBA\_ObjSys\_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO 142](#_Toc500841264)

[Tabelle 104: Tab\_HBA\_ObjSys\_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO 142](#_Toc500841265)

[Tabelle 105: Tab\_HBA\_ObjSys\_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO 144](#_Toc500841266)

[Tabelle 106: Tab\_HBA\_ObjSys\_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072 145](#_Toc500841267)

[Tabelle 107: Tab\_HBA\_ObjSys\_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072 146](#_Toc500841268)

[Tabelle 108: Tab\_HBA\_ObjSys\_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072 146](#_Toc500841269)

[Tabelle 109: Tab\_HBA\_ObjSys\_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072 148](#_Toc500841270)

## A5 - Referenzierte Dokumente

### A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionen sind in den von der gematik veröffentlichten Produkttypsteckbriefen enthalten, in denen die vorliegende Version aufgeführt wird.

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
| --- | --- |
| [gemSpec\_COS] | gematik: Spezifikation COS - Spezifikation der elektrischen Schnittstelle |
| [gemSpec\_Karten\_Fach\_TIP\_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 |

### A5.2 – Weitere Dokumente

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