Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem

| | |
|---|---|
| Version: | 4.5.0 |
| Revision: | 167085 |
| Stand: | 02.10.2019 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | gemSpec_eGK_ObjSys_G2.1 |

# Dokumentinformationen

## Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

## Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---|---|---|---|---|
| 4.0.0 | 20.04.17 | | Erweiterungen und Änderungen für G2.1, Gesellschafterkommentierung | gematik |
| 4.1.0 | 18.12.17 | | Einarbeitung Errata R1.6.4-2 | gematik |
| 4.2.0 | 14.05.18 | | Einarbeitung P15.3 | gematik |
| 4.3.0 | 15.05.19 | | Einarbeitung P18.1 | gematik |
| 4.4.0 | 28.06.19 | | Einarbeitung P19.1 | gematik |
| | | | Einarbeitung P20.3 | gematik |
| 4.5.0 | 02.10.19 | | freigegeben | gematik |

# Inhaltsverzeichnis

**1 Einordnung des Dokuments ..... 6**
**1.1 Zielsetzung ..... 6**
**1.2 Zielgruppe ..... 6**
**1.3 Geltungsbereich ..... 6**
**1.4 Abgrenzung des Dokuments ..... 7**
**1.5 Methodik ..... 7**
1.5.1 Nomenklatur ..... 7
1.5.2 Verwendung von Schlüsselworten ..... 10
1.5.3 Komponentenspezifische Anforderungen ..... 11
**2 Optionen ..... 12**
**3 Lebenszyklus von Karte und Applikation ..... 13**
**4 Anwendungsübergreifende Festlegungen ..... 14**
**4.1 Unterstützung optionaler Funktionspakete ..... 14**
4.1.1 USB-Schnittstelle (optional) ..... 14
4.1.2 Logische Kanäle (optional) ..... 14
4.1.3 Kryptobox (optional) ..... 15
4.1.4 RSA CV-Zertifikate (optional) ..... 15
4.1.5 Symmetrischer Kryptographiealgorithmus DES (optional) ..... 15
4.1.6 Onboard-RSA-Schlüsselgenerierung (optional) ..... 15
**4.2 Reservierung Speicherplatz ..... 16**
**4.3 Attributstabellen ..... 16**
4.3.1 Attribute einer Datei (EF) ..... 17
**4.4 Zugriffsregeln für besondere Kommandos ..... 17**
**4.5 Attributswerte und Personalisierung ..... 17**
**5 Spezifikation grundlegender Applikationen ..... 19**
**5.1 Attribute des Objektsystems ..... 19**
5.1.1 Answer To Reset ..... 20
**5.2 Allgemeine Struktur ..... 21**
**5.3 Root, die Wurzelapplikation (MF) ..... 22**
5.3.1 MF / EF.ATR ..... 23
5.3.2 MF / EF.CardAccess ..... 25
5.3.3 MF / EF.C.CA_eGK.CS.E256 ..... 26
5.3.4 MF / EF.C.eGK.AUT_CVC.E256 ..... 29
5.3.5 MF / EF.DIR ..... 31
5.3.6 MF / EF.GDO ..... 33

5.3.7 MF / EF.Version @deprecated ..... 35
5.3.8 MF / EF.Version2 ..... 37
5.3.9 Passwortobjekte und Multireferenz-Passwortobjekte ..... 39
*5.3.9.1 MF / PIN.CH ..... 39*
*5.3.9.2 MF / MRPIN.home ..... 41*
*5.3.9.3 MF / MRPIN.NFD ..... 43*
*5.3.9.4 MF / MRPIN.DPE ..... 44*
*5.3.9.5 MF / MRPIN.GDD ..... 46*
*5.3.9.6 MF / MRPIN.NFD_READ ..... 48*
*5.3.9.7 MF / MRPIN.OSE ..... 49*
*5.3.9.8 MF / MRPIN.AMTS ..... 51*
*5.3.9.9 MF / PIN.AMTS_REP ..... 53*
5.3.10 MF / PrK.eGK.AUT_CVC.E256 ..... 55
5.3.11 Sicherheitsanker zum Import von CV-Zertifikaten ..... 57
*5.3.11.1 MF / PuK.RCA.CS.E256 ..... 57*
5.3.12 Asymmetrische Kartenadministration ..... 60
*5.3.12.1 MF / PuK.RCA.ADMINCMS.CS.E256 ..... 61*
5.3.13 Symmetrische Kartenadministration ..... 63
*5.3.13.1 MF / SK.CMS.AES128 ..... 64*
*5.3.13.2 MF / SK.CMS.AES256 ..... 66*
*5.3.13.3 MF / SK.VSD.AES128 ..... 68*
*5.3.13.4 MF/ SK.VSD.AES256 ..... 70*
5.3.14 MF / SK.CAN ..... 71

**5.4 Gesundheitsanwendung, Health Care Application (DF.HCA) ..... 73**
5.4.1 MF / DF.HCA / EF.Einwilligung ..... 76
5.4.2 MF / DF.HCA / EF.GVD ..... 78
5.4.3 MF / DF.HCA / EF.Logging ..... 80
5.4.4 MF / DF.HCA / EF.PD ..... 82
5.4.5 MF / DF.HCA / EF.Prüfungsnachweis ..... 84
5.4.6 MF / DF.HCA / EF.Standalone ..... 85
5.4.7 MF / DF.HCA / EF.StatusVD ..... 87
5.4.8 MF / DF.HCA / EF.VD ..... 89
5.4.9 MF / DF.HCA / EF.Verweis ..... 90
5.4.10 Anwendung Notfalldatensatz (DF.NFD) ..... 92
*5.4.10.1 MF / DF.HCA / DF.NFD / EF.NFD ..... 95*
*5.4.10.2 MF / DF.HCA / DF.NFD / EF.StatusNFD ..... 97*
5.4.11 Anwendung Datensatz Persönliche Erklärungen (DF.DPE) ..... 99
*5.4.11.1 MF / DF.HCA / DF.DPE / EF.DPE ..... 102*
*5.4.11.2 MF / DF.HCA / DF.DPE / EF.StatusDPE ..... 104*
5.4.12 Anwendung Gesundheitsdatendienst (GDD) ..... 106
*5.4.12.1 MF / DF.HCA / DF.GDD / EF.EinwilligungGDD ..... 108*
*5.4.12.2 MF / DF.HCA / DF.GDD / EF.VerweiseGDD ..... 110*
5.4.13 Anwendung Organspendeerklärung (DF.OSE) ..... 112
*5.4.13.1 MF / DF.HCA / DF.OSE / EF.OSE ..... 115*
*5.4.13.2 MF / DF.HCA / DF.OSE / EF.StatusOSE ..... 117*
5.4.14 Anwendung AMTS Datenmanagement (DF.AMTS) ..... 119
*5.4.14.1 MF / DF.HCA / DF.AMTS / EF.AMTS ..... 121*
*5.4.14.2 MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS ..... 123*
*5.4.14.3 MF / DF.HCA / DF.AMTS / EF.StatusAMTS ..... 126*
*5.4.14.4 MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256 ..... 128*

**5.5 DF.ESIGN (Krypto-Anwendung ESIGN) ..... 130**
5.5.1 MF / DF.ESIGN / EF.C.CH.AUT.R2048 ..... 132
5.5.2 MF / DF.ESIGN / EF.C.CH.AUTN.R2048 ..... 134
5.5.3 MF / DF.ESIGN / EF.C.CH.ENC.R2048 ..... 136
5.5.4 MF / DF.ESIGN / EF.C.CH.ENCV.R2048 ..... 138
5.5.5 MF / DF.ESIGN / PrK.CH.AUT.R2048 ..... 141
5.5.6 MF / DF.ESIGN / PrK.CH.AUTN.R2048 ..... 143
5.5.7 MF / DF.ESIGN / PrK.CH.ENC.R2048 ..... 145
5.5.8 MF / DF.ESIGN / PrK.CH.ENCV.R2048 ..... 147
5.5.9 MF / DF.ESIGN / EF.C.CH.AUT.E256 ..... 149
5.5.10 MF / DF.ESIGN / EF.C.CH.AUTN.E256 ..... 151
5.5.11 MF / DF.ESIGN / EF.C.CH.ENC.E256 ..... 153
5.5.12 MF / DF.ESIGN / EF.C.CH.ENCV.E256 ..... 154
5.5.13 MF / DF.ESIGN / PrK.CH.AUT.E256 ..... 157
5.5.14 MF / DF.ESIGN / PrK.CH.AUTN. E256 ..... 158
5.5.15 MF / DF.ESIGN / PrK.CH.ENC.E256 ..... 161
5.5.16 MF / DF.ESIGN / PrK.CH.ENCV.E256 ..... 162

**6 Qualifizierte elektronische Signatur ..... 165**

**6.1 DF.QES (QES-Anwendung komplett angelegt und nutzbar) ..... 165**
6.1.1 MF / DF.QES / EF.C.CH.QES.R2048 ..... 167
6.1.2 MF / DF.QES / PIN.QES ..... 169
6.1.3 MF / DF.QES / PrK.CH.QES.R2048 ..... 172
6.1.4 MF / DF.QES / EF.C.CH.QES.E256 ..... 174
6.1.5 MF / DF.QES / PrK.CH.QES.E256 ..... 176

**6.2 Optionen für unvollständige QES-Anwendung ..... 178**

**7 Anhang A – Verzeichnisse ..... 179**

**7.1 Abkürzungen ..... 179**

**7.2 Glossar ..... 180**

**7.3 Abbildungsverzeichnis ..... 180**

**7.4 Tabellenverzeichnis ..... 181**

**7.5 Referenzierte Dokumente ..... 186**
7.5.1 Dokumente der gematik ..... 186
7.5.2 Weitere Dokumente ..... 187

# 1 Einordnung des Dokuments

## 1.1 Zielsetzung

Dieses Dokument spezifiziert die anwendungsspezifischen Strukturen der eGK und beschreibt die Strukturen der Anwendungen, die bei der Initialisierung und Personalisierung in die eGK geladen werden. Außerdem werden in diesem Teil die Zugriffsrechte auf Elemente der eGK festgelegt.

Die Spezifikation behandelt Anwendungen der elektronischen Gesundheitskarte (eGK) unter den folgenden, rein kartenorientierten Gesichtspunkten:

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

Somit stellt dieses Dokument auf unterster technischer Ebene eine Reihe von Datencontainern bereit, die etwa mit Versichertenstammdaten, Notfalldaten etc. befüllbar sind. 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 1.4).

## 1.2 Zielgruppe

Das Dokument richtet sich an

- Hersteller, welche die hier spezifizierten Anwendungen herstellerspezifisch für ein bestimmtes Chipkartenbetriebssystem umsetzen,
- Kartenherausgeber, die anhand der hier spezifizierten Anwendungen die elektrische Personalisierung einer eGK planen,
- Hersteller von Systemen, die Programme entwickeln, welche unmittelbar mit der Chipkarte kommunizieren.

## 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

**Schutzrechts-/Patentrechtshinweis**

*Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.*

## 1.4 Abgrenzung des Dokuments

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

## 1.5 Methodik

### 1.5.1 Nomenklatur

| **‘1D’** | **Hexadezimale Zahlen und Oktettstrings werden in Hochkommata eingeschlossen.** |
|---|---|
| x \|\| y | Das Symbol \|\| steht für die Konkatenierung von Oktettstrings oder Bitstrings: ‘1234’ \|\| ‘5678’ = ‘12345678’. |

In [gemSpec_COS] wurde ein objektorientierter Ansatz für die Beschreibung der Funktionalität des Betriebssystems gewählt. Deshalb wurde dort der Begriff "Passwortobjekt" verwendet, wenn Instanzen für eine Benutzerverifikation besprochen wurden. Da in diesem Dokument lediglich numerische Ziffernfolgen als Verifikationsdaten eines Benutzers verwendet werden, wird hier statt Passwortobjekt vielfach der Begriff PIN gewählt, wenn keine Gefahr besteht, dass es zu Verwechslungen kommt zwischen den Verifikationsdaten und der Instanz des Objektes, in denen sie enthalten sind (zur Erinnerung: ein Passwortobjekt enthält neben den Verifikationsdaten auch einen Identifier, eine Zugriffsregel, eine PUK, …).

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

Externe Authentisierung für CV-Zertifikate der Generation 1 mit einer Rolle CHA (informativ)

Gemäß [gemSpec_COS#10.2] wird die Notwendigkeit einer externen Authentisierung für Karten der Generation 1 mit einer Rolle CHA.1 wie folgt dargestellt: AUT(*CHA.1*). Wegen der häufigen ODER-Verknüpfung von Rollen in Zugriffsregeln, wird in diesem Dokument

abweichend davon, aus Gründen der Übersichtlichkeit, folgende Notation synonym verwendet:

- C.1 entspricht Rollenauthentisierung mittels CV-Zertifikaten mit der Rolle CHA.1.
- C.1.2 entspricht Rollenauthentisierung mittels CV-Zertifikaten mit der Rolle CHA.1 oder (boolesches oder) CHA.2. In komplexeren Ausdrücken bindet dieses ODER genauso wie jedes andere ODER auch und damit schwächer als UND.

Die Zugriffsrechte in dieser Notation werden nur noch informativ in den Tabellen mit den Zugriffsrechten aufgeführt, um deutlich zu machen, welche Profile Zugriffsrechte haben. Diese Zugriffrechte werden in eGKs der Generation 2 nicht mehr umgesetzt, da zugreifende Karten (HBA, SMC-B) ausschließlich Generation 2-Karten sein werden.

Die Angabe dieser informativen Zugriffsrechte beschränkt sich aus Gründen der Übersichtlichkeit jeweils nur auf die Anteile der Zugriffsregel, die einem Profil zuzuordnen sind.

Beispiel:

| **Zugriffsregel** | **Informative Darstellung** |
|---|---|
| PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.40]<br>OR [PWD(PIN.CH) AND flagTI.33] | *(informativ: OR [PWD(MRPIN.GDD) AND (C.1.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND C.1.10])* |

Externe Authentisierung für CV-Zertifikate der Generation 2 mit einer Flaglist

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 Dokumentes genau ein Bit gesetzt ist. Abkürzend wird deshalb in diesem Dokument lediglich die Nummer des gesetzten Bits angegeben in Verbindung mit der OID. Ein gesetztes Bit i in Verbindung mit der oid_cvc_fl_cms wird im Folgenden mit flagCMS.i angegeben und ein gesetztes Bit j in Verbindung mit der oid_cvc_fl_ti wird im Folgenden mit flagTI.j angegeben.

Beispiele:

| **Langform** | **Kurzform** |
|---|---|
| Informativ: AUT( CHA.1 ) | C.1 |
| Informativ: AUT( CHA.7 ) | C.7 |

| | |
|---|---|
| Informativ: AUT( CHA.2 ) OR AUT( CHA.3 ) | C.2.3 |
| Informativ: PWD(PIN) AND [AUT( CHA.2 ) OR AUT( CHA.3 )] | PWD(PIN) AND [C.2.3] |
| AUT(oid_cvc_fl_cms,'00010000000000') | flagCMS.15 |
| AUT(oid_cvc_fl_ti, '00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000') | flagTI.15 OR flagTI.16 |
| PWD(PIN) AND<br>[<br>AUT(oid_cvc_fl_cms,'00010000000000')<br>OR<br>AUT(oid_cvc_fl_ti, '00008000000000')<br>] | PWD(PIN) AND [flagCMS.15 OR flagTI.16)] |
| SmMac(oid_cvc_fl_cms, '00800000000000') | SmMac(flagCMS.08) |

Für die Authentisierung der Zugriffe durch ein CMS oder ein VSDM auf die dafür vorgesehenen Objekte können entweder symmetrische Verfahren mit AES-Schlüsseln oder alternativ asymmetrische Verfahren mit CV-Zertifikaten verwendet werden. Für beide Verfahren sind die Schlüsselobjekte in dieser Spezifikation spezifiziert. Um die Zugriffsregeln für administrative Zugriffe in den einzelnen Tabellen übersichtlich darstellen zu können, werden folgende Abkürzungen verwendet:

| | |
|---|---|
| AUT_CMS | {SmMac(SK.CMS.AES128)<br>OR SmMac(SK.CMS.AES256)<br>OR SmMac(flagCMS.08)}<br>AND SmCmdEnc<br>AND SmRspEnc |
| AUT_VSD | {SmMac(SK.VSD.AES128)<br>OR SmMac(SK.VSD.AES256)<br>OR SmMac(flagCMS.09)}<br>AND SmCmdEnc<br>AND SmRspEnc |
| AUT_PACE | SmMac(SK.CAN)<br>AND SmCmdEnc<br>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(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:
   a. Falls eine Kommandonachricht keine Kommandodaten enthält, ist es zulässig, den Term SmCmdEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
   b. Falls eine Antwortnachricht keine Antwortdaten enthält, 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:
   a. Falls für eine Zugriffsart keine Kommandodaten existieren, ist es für den Prüfling zulässig, in der zugehörigen Zugriffsregel den Term SmCmdEnc zu verwenden.
   b. Falls für eine Zugriffsart keine Antwortdaten existieren, ist es für den Prüfling zulässig, in der zugehörigen Zugriffsregel den Term SmRspEnc zu verwenden.

An der Benutzerschnittstelle werden für Benutzergeheimnisse andere Bezeichnungen verwendet, als in technischen Dokumenten. Tab_eGK_ObjSys_001 listet die Zuordnung.

**Tabelle 1: Tab_eGK_ObjSys_001: Zuordnung der Bezeichnungen für PINs**

| Bezeichnung Benutzerschnittstelle | Bezeichnung in technischen Dokumenten |
|---|---|
| Praxis PIN | PIN.CH |
| Privat PIN | MRPIN.home |
| Signatur PIN | PIN.QES |

### 1.5.2 Verwendung von Schlüsselworten

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

Sie werden im Dokument wie folgt dargestellt:

**<AFO-ID> - <Titel der Afo>**
Text / Beschreibung
**[<=]**

Dabei umfasst die Anforderung sämtliche innerhalb der Afo-ID und der Textmarke angeführten Inhalte.

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

### 1.5.3 Komponentenspezifische Anforderungen

Da es sich beim vorliegenden Dokument um die Spezifikation einer Schnittstelle zwischen mehreren Komponenten handelt, ist es möglich, die Anforderungen aus der Sichtweise jeder Komponente zu betrachten. Die normativen Abschnitte tragen deshalb eine Kennzeichnung, aus wessen Sichtweise die Anforderung primär betrachtet wird.

**Tabelle 2: Tab_eGK_ObjSys_002: Liste der Komponenten, an welche dieses Dokument Anforderungen stellt**

| Komponente | Beschreibung |
|---|---|
| K_Initialisierung | Instanz, welche eine Chipkarte im Rahmen der Initialisierung befüllt |
| K_Personalisierung | Instanz, welche eine Chipkarte im Rahmen der Produktion individualisiert |
| K_COS | Betriebssystem einer Smartcard |

# 2 Optionen

In den Kapiteln 5.3.12 und 5.3.13 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen CMS/VSD und einer Karte beschrieben die bei der Ausgabe der Karte angelegt werden müssen.

**Card-G2-A_2973 - K_Personalisierung: Auswahl der Absicherung der Kartenadministration**
Da die eGK Online administriert wird, MUSS ein Kartenherausgeber bei der Personalisierung Schlüssel für mindestens eines der beiden Verfahren

1. asymmetrische Authentifizierung für CMS/VSD
2. symmetrische Authentifizierung für CMS/VSD

in die Karte einbringen und sicherstellen, dass das dazugehörende CMS bzw. der dazugehörende VSD über die entsprechenden Schlüssel verfügt.

**[<=]**

**Card-G2-A_3228 - K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten**
Die eGK KANN als Testkarte ausgestaltet werden. Soweit in dieser Spezifikation Anforderungen an Testkarten von den Anforderungen an Produktivkarten abweichen, wird dies an der entsprechenden Stelle aufgeführt.
**[<=]**

# 3 Lebenszyklus von Karte und Applikation

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

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

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

# 4 Anwendungsübergreifende Festlegungen

**Card-G2-A_2975 - K_eGK: Kontaktlose Schnittstelle**
Für das Objektsystem MUSS ein COS verwendet werden, das die Option_kontaktlose_Schnittstelle implementiert hat.
**[<=]**

## 4.1 Unterstützung optionaler Funktionspakete

### 4.1.1 USB-Schnittstelle (optional)

**Card-G2-A_2861 - K_eGK: USB-Schnittstelle**
Falls eine eGK die Option_USB_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_USB_Schnittstelle implementiert hat.
**[<=]**

**Card-G2-A_2974 - K_eGK: Vorhandensein einer USB-Schnittstelle**
Falls eine eGK die Option_USB_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_USB_Schnittstelle implementiert hat.
b) das die Option_USB_Schnittstelle nicht implementiert hat.

**[<=]**

### 4.1.2 Logische Kanäle (optional)

**Card-G2-A_2981 - K_eGK: logische_Kanäle**
Falls eine eGK die Option_logische_Kanäle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_logische_Kanäle implementiert hat.

**[<=]**

**Card-G2-A_2982 - K_Initialisierung: Anzeige von logischen Kanälen**
Falls das COS die Option_logische_Kanäle

a. nicht unterstützt, dann MUSS das dritte Oktett in den Card Capabilities den Wert ‘E0’ besitzen.
b. unterstützt, dann MUSS das Low Nibble im dritten Oktett der Card Capabilities die maximal angebotene Anzahl logischer Kanäle gemäß [ISO7816-4] anzeigen. (siehe 5.3.1).

**[<=]**

### 4.1.3 Kryptobox (optional)

Falls eine eGK die Option_Kryptobox nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_Kryptobox implementiert hat.

**Card-G2-A_2984 - K_eGK: Vorhandensein Kryptobox**
Für eine eGK KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_Kryptobox implementiert hat.
b) das die Option_Kryptobox nicht implementiert hat.
**[<=]**

### 4.1.4 RSA CV-Zertifikate (optional)

Falls eine eGK RSA CV-Zertifikate nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_RSA_CVC implementiert hat.

**Card-G2-A_3784 - K_eGK: Unterstützung RSA CV-Zertifikate**
Für eine eGK KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_RSA_CVC implementiert hat.
b) das die Option_RSA_CVC nicht implementiert hat.

**[<=]**

### 4.1.5 Symmetrischer Kryptographiealgorithmus DES (optional)

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

**Card-G2-A_3785 - K_eGK: Unterstützung symmetrischer Kryptographiealgorithmus DES**
Für eine eGK KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_DES implementiert hat.
b) das die Option_DES nicht implementiert hat.

**[<=]**

### 4.1.6 Onboard-RSA-Schlüsselgenerierung (optional)

**Card-G2-A_3846 - K_eGK: Onboard-RSA-Schlüsselgenerierung**
Falls eine eGK die Option_RSA_KeyGeneration nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_RSA_KeyGeneration implementiert hat.**[<=]**

**Card-G2-A_3847 - K_eGK: Vorhandensein Onboard-RSA-Schlüsselgenerierung**
Falls eine eGK die Option_RSA_KeyGeneration nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,

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

**[<=]**

## 4.2 Reservierung Speicherplatz

**Card-G2-A_3237 - K_Initialisierung: Speicherplatzreservierung für zukünftige Anwendungen**
Zusätzlich zu den Anforderungen zu AMTS MUSS für weitere zukünftige Anwendungen ein Speicherbereich > 0 Byte vorhanden sein. Die Größe dieses zusätzlichen freien Speicherbereichs MUSS im Zulassungsantrag für das Objektsystem angegeben werden.
**[<=]**

**Card-G2-A_3701 - K_Initialisierung: Angabe der Speicherplatzreserve**
Die Größe des zusätzlichen freien Speicherbereichs MUSS im Zulassungsantrag für das Objektsystem angegeben werden. Ist kein zusätzlicher freier Speicherbereich vorgesehen, so ist dessen Größe mit 0 Byte anzugeben.
**[<=]**

## 4.3 Attributstabellen

**Card-G2-A_2333 - K_Initialisierung: Änderung von Zugriffsregeln**
Die in diesem Dokument definierten Zugriffsregeln DÜRFEN nach Abschluss der Initialisierungsphase NICHT veränderbar sein.

**[<=]**

**Card-G2-A_2334 - K_Initialisierung: Eigenschaften aller Objekte in SE#1**
Alle Objekte MÜSSEN sich in SE#1 wie angegeben verwenden lassen.

**[<=]**

**Card-G2-A_2857 - K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs**
Jedes Objekt KANN in SE verwendbar sein, die verschieden sind von SE#1.

**[<=]**

**Card-G2-A_2858 - K_Initialisierung: Eigenschaften der Objekte in anderen SEs**
Falls ein Objekt in einem von SE#1 verschiedenen SE verwendbar ist, dann MUSS es dort dieselben Eigenschaften wie in SE#1 besitzen.

**[<=]**

**Card-G2-A_2335-01 - K_Initialisierung: Ordnerattribute**
Enthält eine Tabelle mit Ordnerattributen einen oder mehrere applicationIdentifier (AID), dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
**[<=]**

**Card-G2-A_3594 - K_Initialisierung: Herstellerspezifischer ApplicationIdentifier**
Enthält eine Tabelle mit Ordnerattributen keinen applicationIdentifier (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.

**[<=]**

**Card-G2-A_3595 - K_Initialisierung: Fehlender FileIdentifier**
Enthält eine Tabelle mit Ordnerattributen keinen fileIdentifier (FID), so DARF dieser Ordner NICHT mittels eines fileIdentifier aus dem Intervall gemäß [gemSpec_COS#8.1.1] selektierbar sein, es sei denn, es handelt sich um den Ordner root, dessen optionaler fileIdentifier den Wert '3F00' besitzen MUSS.

**[<=]**

**Card-G2-A_3596 - K_Initialisierung: Herstellerspezifischer FileIdentifier**
Enthält eine Tabelle mit Ordnerattributen keinen fileIdentifier (FID), so KANN diesem Ordner ein beliebiger fileIdentifier außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden.

**[<=]**

### 4.3.1 Attribute einer Datei (EF)

**Card-G2-A_2336 - 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_2667 - K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile"**
Für transparente EFs MUSS der Wert von „positionLogicalEndOfFile", soweit nicht anders spezifiziert, auf die Anzahl der tatsächlich belegten Bytes gesetzt werden.

**[<=]**

## 4.4 Zugriffsregeln für besondere Kommandos

**A_17570 - K_Initialisierung: Zugriffsregeln für besondere Kommandos**
Die Zugriffsbedingung für die Kommandos Get Challenge, List Public Key, Manage Security Environment, Get Security Status Key und Select MUSS für alle Schnittstellen stets ALWAYS sein.**[<=]**

## 4.5 Attributswerte und Personalisierung

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

Beispielsweise ist es denkbar, dass für die Datei EF.GDO das Attribut lifeCycleStatus nach der Initialisierung auf dem in [gemSpec_COS] nicht normativ geforderten Wert

„Initialize“ steht und für diesen Wert die Zugriffsregeln etwa ein Update Binary Kommando erlauben. In diesem Fall wiche nicht nur der Wert des Attributes lifeCycleStatus, sondern auch der des Attributes interfaceDependentAccessRules von den Vorgaben dieses Dokumentes ab. Nach Abschluss der Personalisierung wäre dann der Wert des Attributs 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_3242 - K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung**
Zur Unterstützung herstellerspezifischer Personalisierungsprozessen KÖNNEN die Werte von Attributen eines Kartenproduktes von den Festlegungen dieses Dokumentes abweichen. Hierbei MÜSSEN Abweichungen auf solche beschränkt sein, die hinsichtlich ihrer Wirkung in der personalisierten Karte sowohl fachlich wie sicherheitstechnisch der in der Spezifikation vorgegebenen Werten entsprechen.
**[**<=**]**

# 5 Spezifikation grundlegender Applikationen

Zu den grundlegenden Applikationen der elektronischen Gesundheitskarte (eGK) zählen:

- Das Wurzelverzeichnis der eGK, auch root oder Master File (MF) genannt,
- die Gesundheitsanwendung DF.HCA (Health Care Application) und
- die Krypto-Anwendung DF.ESIGN

Die QES-Anwendung gehört nicht zu den verpflichtenden Anwendungen einer eGK und wird deshalb in einem eigenen Kapitel 6 behandelt.

## 5.1 Attribute des Objektsystems

Das Objektsystem gemäß [gemSpec_COS#9.1] enthält folgende Attribute:

**Card-G2-A_2341 - K_Initialisierung: Wert des Attributes root**
Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_eGK_ObjSys_006 sein.

**[<=]**

**Card-G2-A_2342-01 - K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset**
Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A_2345, Card-G2-A_3597, Card-G2-A_2346-01, Card-G2-A_2347 und Card-G2-A_2985 entsprechen.

**[<=]**

**Card-G2-A_2343 - K_Personalisierung: Wert des Attributes iccsn8**
Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein.

**[<=]**

**Card-G2-A_2344 - K_Initialisierung: Inhalt persistentPublicKeyList**
Das Attribut *persistentPublicKeyList* MUSS den Schlüssel PuK.RCA.CS.E256 enthalten.

**[<=]**

**Card-G2-A_3180 - 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_3265-01 - 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_3391 - K_Personalisierung: personalisierter Wert von pointInTime**
Das Attribut *pointInTime* MUSS im Rahmen der Personalisierung auf den Wert von CED eines Endnutzerzertifikates gesetzt werden. Falls es mehrere Endnutzerzertifikate gibt, so ist das CED mit dem größten Wert zu verwenden.
**[<=]**

### 5.1.1 Answer To Reset

**Card-G2-A_2345 - K_Personalisierung und K_Initialisierung: ATR-Codierung**
Die ATR-Kodierung MUSS die in Tab_eGK_ObjSys_004 dargestellten Werte besitzen.

**Tabelle 3: Tab_eGK_ObjSys_004 ATR-Codierung**

| 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_3597 - K_Personalisierung und K_Initialisierung: TC1 Byte im ATR**
Der ATR SOLL ein TC1 Byte mit dem Wert 'FF' enthalten.

**[<=]**

**Card-G2-A_2346-01 - K_Personalisierung und K_Initialisierung: Wert des TC1 Bytes im ATR**
Wenn der ATR ein TC1 Byte mit dem Wert ‘FF’ enthält, dann MUSS T0 auf den Wert ‘Dx’ gesetzt werden.

**[<=]**

**Card-G2-A_2985 - K_Personalisierung und K_Initialisierung: Historical Bytes im ATR**
Das Attribut answerToReset SOLL KEINE Historical Bytes enthalten.

**[<=]**

**Card-G2-A_2347 - K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes**
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.

**[<=]**

## 5.2 Allgemeine Struktur

Abb_eGK_ObjSys_001 zeigt die allgemeine Struktur der eGK.

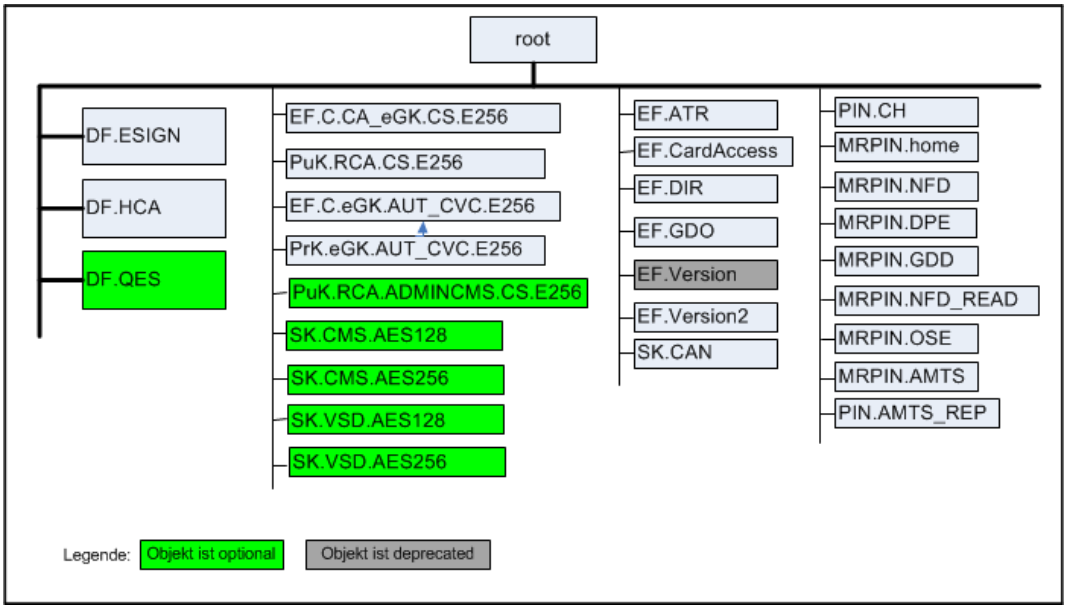



**Abbildung 1: Abb_eGK_ObjSys_001 Objektstruktur einer eGK auf oberster Ebene**

## 5.3 Root, die Wurzelapplikation (MF)

Das MF der eGK ist ein Ordner (siehe [gemSpec_COS#8.3.1]) mit den in Tab_eGK_ObjSys_006 gezeigten Eigenschaften.

**Card-G2-A_2351 - K_Initialisierung: Initialisierte Attribute von MF**
MF MUSS die in Tab_eGK_ObjSys_006 dargestellten initialisierten Attribute besitzen.

**Tabelle 4: Tab_eGK_ObjSys_006 Initialisierte Attribute von MF**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | 'D276 0001 4480 00' | |
| *fileIdentifier* | '3F 00' | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Fingerprint | Wildcard | |
| Load Application | AUT_CMS | |
| Get Random | 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Load Application | AUT_CMS | |

| | | |
|---|---|---|
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 2: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

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

### 5.3.1 MF / EF.ATR

Die transparente Datei EF.ATR enthält Informationen zur maximalen Größe der APDU. Ferner dient sie zur Versionierung unveränderlicher Elemente einer Karte.

**Card-G2-A_2352-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.ATR**
EF.ATR MUSS die in Tab_eGK_ObjSys_007 dargestellten initialisierten Attribute besitzen.

**Tabelle 5: Tab_eGK_ObjSys_007 Initialisierte Attribute von MF / EF.ATR**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | '2F 01' | siehe Hinweis 5: |
| *shortFileIdentifier* | '1D'= 29 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | herstellerspezifisch | |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |

| | | |
|---|---|---|
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Read Binary<br>Write 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Binary<br>Write Binary | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 4: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

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

**Card-G2-A_3205 - K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR**

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

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

**[<=]**

### 5.3.2 MF / EF.CardAccess

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

**Card-G2-A_3200 - K_Initialisierung: Initialisierte Attribute von MF / EF.CardAccess**
EF.CardAccess MUSS die in Tab_eGK_ObjSys_106 dargestellten initialisierten Attribute besitzen.

**Tabelle 6: Tab_eGK_ObjSys_106 Initialisierte Attribute von MF / EF.CardAccess**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘01 1C’ | siehe Hinweis 5: |
| *shortFileIdentifier* | ‘1C’= 28 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | passend zum Inhalt | |
| *positionLogicalEndOfFile* | passend zum Inhalt | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Binary | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.3.3 MF / EF.C.CA_eGK.CS.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_PKI, welches den öffentlichen Schlüssel PuK.CA_eGK.CS.E256 einer CA enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels PuK.RCA.CS.E256 (siehe Tab_eGK_ObjSys_023) prüfen.

**Card-G2-A_2359 - K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_eGK.CS.E256**
EF.C.CA_eGK.CS.E256 MUSS die in Tab_eGK_ObjSys_009 dargestellten initialisierten Attribute besitzen.

**Tabelle 7: Tab_eGK_ObjSys_009 Initialisierte Attribute von MF / EF.C.CA_eGK.CS.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | '2F 07' | |

| | | |
|---|---|---|
| | | |
| *shortFileIdentifier* | ‘07’= 7 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | ‘00DC’ Oktett = 220 Oktett | |
| *positionLogicalEndOfFile* | ‘0’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Update Binary | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Update Binary | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 6: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

**Card-G2-A_3207 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_eGK.CS.E256**

Bei der Personalisierung von EF.C.CA_eGK.CS.E256 MÜSSEN die in Tab_eGK_ObjSys_110 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 8: Tab_eGK_ObjSys_110 Personalisierte Attribute von MF / EF.C.CA_eGK.CS.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | '00DC' Oktett = 220 Oktett | |
| *body* | C.CA_eGK.CS.E256 gemäß [gemSpec_PKI#6.7.1] | |
| *body* Option_Erstellung _von_Testkarten | C.CA_eGK.CS.E256 gemäß [gemSpec_PKI#6.7.1] aus Test-CVC-CA | Details siehe [gemSpec_TK#3.1.2] |

**[<=]**

### 5.3.4 MF / EF.C.eGK.AUT_CVC.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptografie mit elliptischen Kurven gemäß [gemSpec_COS, welches den öffentlichen Schlüssel PuK.eGK.AUT_CVC.E256 zu PrK.eGK.AUT_CVC.E256 (siehe Tab_eGK_ObjSys_020) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_eGK.CS.E256 (siehe Tab_eGK_ObjSys_009) prüfen.

**Card-G2-A_2363 - K_Personalisierung: CHR in MF / EF.C.eGK.AUT_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_2370.**[<=]**

**Card-G2-A_2364-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.C.eGK.AUT_CVC.E256**
EF.C.eGK.AUT_CVC.E256 MUSS die in Tab_eGK_ObjSys_012 dargestellten initialisierten Attribute besitzen.

**Tabelle 9: Tab_eGK_ObjSys_012 Initialisierte Attribute von MF/EF.C.eGK.AUT_CVC.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | '2F 06' | |
| *shortFileIdentifier* | '06'= 6 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | '00DE' Oktett = 222 Oktett | |

| | | |
|---|---|---|
| | | |
| *positionLogicalEndOfFile* | '0' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Update Binary | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Update Binary | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3208 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.eGK.AUT_CVC.E256**
Bei der Personalisierung von EF.C.eGK.AUT_CVC.E256 MÜSSEN die in Tab_eGK_ObjSys_112 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 10: Tab_eGK_ObjSys_112 Personalisierte Attribute von MF / EF.C.eGK.AUT_CVC.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | '00DE' Oktett = 222 Oktett | |
| *body* | C.eGK.AUT_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.eGK.AUT_CVC.E256 | |

**[<=]**

### 5.3.5 MF / EF.DIR

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

**Card-G2-A_3598 - K_Initialisierung: Inhalt der Records von EF.DIR**
Für jede im Objektsystem vorhandene Anwendung MUSS die Datei einen eigenen Record besitzen, der den ApplicationIdentifier (AID) dieser Anwendung im Format ´61-$L_{61}$-{4F-$L_{4F}$-AID}´ enthält, wobei $L_{61}$ und $L_{4F}$ die Anzahl der nachfolgenden Bytes in dem mit Tag 61 bzw. Tag 4F adressierten Datenobjekt bezeichnen.
Zu jedem Record der Datei MUSS es auf der Karte eine Anwendung geben, deren AID durch diesen Record beschrieben ist.
Record 1 des EF.DIR MUSS den AID des MF enthalten.
**[<=]**

**Card-G2-A_2367-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.DIR**
EF.DIR MUSS die in Tab_eGK_ObjSys_014 dargestellten initialisierten Attribute besitzen.

**Tabelle 11: Tab_eGK_ObjSys_014 Initialisierte Attribute von MF / EF.DIR**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear variables Elementary File | |
| *fileIdentifier* | '2F 00' | |
| *shortFileIdentifier* | '1E'= 30 | |
| *lifeCycleStatus* | „Operational state (activated)" | |

| | | |
|---|---|---|
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *maxNumRecords* | 20 Records | |
| *maxRecordLength* | 32 Oktett | |
| *flagRecordLCS* | False | |
| *numberOfOctet* | '00C8' Oktett = 200 Oktett | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| recordList<br><br>Record 1<br>Record 2 und folgende | <br><br>'61- 09- (4F 07 D2760001448000)'<br>´61-$L_{61}$-{4F-$L_{4F}$-AID}´<br>für alle Applikationen im Objektsystem | <br><br>MF, Kap. 5.3 |
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Append Record<br>Delete Record<br>Update Record | AUT_CMS | |
| Read Record<br>Search Record | 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** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Append Record<br>Delete Record | AUT_CMS | |

| | | |
|---|---|---|
| Update Record | | |
| Read Record<br>Search Record | AUT_PACE<br>OR AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 7: Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind: Activate, Activate Record, Append Record, Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record, Write Record.*

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

### 5.3.6 MF / EF.GDO

In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte enthält. Die Kennnummer basiert auf [Resolution190].

**Card-G2-A_2369-01 - K_Initialisierung Attribute von MF / EF.GDO**
EF.GDO MUSS die in Tab_eGK_ObjSys_015 dargestellten Attribute besitzen.

**Tabelle 12: Tab_eGK_ObjSys_015 Initialisierte Attribute von MF / EF.GDO**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | '2F 02' | |
| *shortFileIdentifier* | '02'= 2 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | '00 0C' Oktett = 12 Oktett | |
| *positionLogicalEndOfFile* | Wildcard | |

| | | |
|---|---|---|
| | | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | Wildcard | wird personalisiert |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Binary | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 9: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

**Card-G2-A_2370-01 - K_Personalisierung: Personalisiertes Attribut von EF.GDO**
Bei der Personalisierung von EF.GDO MÜSSEN die in Tab_eGK_ObjSys_182 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 13: Tab_eGK_ObjSys_182 Personalisiertes Attribut von MF / EF.GDO**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | '000C' Oktett = 12 Oktett | |
| *body* | Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] | |

**[<=]**

### 5.3.7 MF / EF.Version @deprecated

*Wichtiger Hinweis:*

*Das Objekt EF.Version wird durch die vorliegende Spezifikation normativ gefordert, jedoch in zukünftigen Generationen des eGK-Objektsystems nicht mehr unterstützt. Es wird mit dieser Markierung „@deprecated" gekennzeichnet. Es ist dann ausschließlich EF.Version2 zu verwenden (siehe auch entsprechende Erläuterung in [gemSpec_Karten_Fach_TIP_G2.1#2.2].*

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

- Betriebssystem: Die "Schnittstelle" des Betriebssystems wird in [gemSpec_COS] spezifiziert. Dabei werden der grundsätzliche Funktionsumfang und der Aufbau der Nachrichten von und zur eGK festgelegt.
- Objektsystem: Die Konfiguration des Objektsystems wird in diesem Dokument spezifiziert. Damit wird für die fachliche Ebene festgelegt, wo Daten abgelegt sind und welche Zugriffsrechte die eGK durchsetzt.
- Fachliche Anwendung: Diese "Schnittstelle" beschreibt im Wesentlichen den Inhalt von Dateien, die im Rahmen fachlicher Anwendungen verwendet werden.

**Card-G2-A_2371-01 - K_Initialisierung: Attribute von MF / EF.Version @deprecated**
Wenn die Datei EF.Version auf der Karte vorhanden ist, MUSS sie die in Tab_eGK_ObjSys_016 dargestellten Attribute besitzen.

**Tabelle 14: Tab_eGK_ObjSys_016 Initialisierte Attribute von MF / EF.Version @deprecated**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear fixes Elementary File | |
| *fileIdentifier* | '2F 10' | |
| *shortFileIdentifier* | '10'= 16 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |

| | | |
|---|---|---|
| | | |
| *flagChecksum* | True | |
| *maxNumRecords* | 4 Records | |
| *maxRecordLength* | 5 Oktett | |
| *flagRecordLCS* | False | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| recordList<br>Record 1<br>Record 2<br>Record 3<br>Record 4 | <br>'XX…YY'<br>'XX…YY'<br>'XX…YY'<br>'XX…YY | Recordinhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] |
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Read Record<br>Search Record | ALWAYS | |
| Update Record | AUT_CMS | |
| 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** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Record<br>Search Record | ALWAYS | |
| Update Record | AUT_CMS | |
| andere | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 10: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate*

### 5.3.8 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_3231-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.Version2**
EF.Version2 MUSS die in Tab_eGK_ObjSys_183 dargestellten initialisierten Attribute besitzen.

**Tabelle 15: Tab_eGK_ObjSys_183 Initialisierte Attribute von MF / EF.Version2**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | '2F 11' | |
| *shortFileIdentifier* | '11'= 17 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '00 3C' Oktett = 60 Oktett | |

| | | |
|---|---|---|
| *positionLogicalEndOfFile* | passend zum Inhalt | gemäß [gemSpec_Karten_Fach_TIP_G2.1] |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1] | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Read Binary | ALWAYS | |
| Update Binary<br>Set Logical EOF | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Binary | ALWAYS | |
| Update Binary<br>Set Logical EOF | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 11: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

## 5.3.9 Passwortobjekte und Multireferenz-Passwortobjekte

### 5.3.9.1 MF / PIN.CH

Dieses reguläre Passwortobjekt wird zur Freischaltung von Schlüsseln und Inhalten der eGK verwendet. Dieses Passwortobjekt wird nur innerhalb der TI verwendet.

**Card-G2-A_2372-01 - K_Initialisierung: Initialisierte Attribute von MF / PIN.CH**
PIN.CH MUSS die in Tab_eGK_ObjSys_017 dargestellten initialisierten Attribute besitzen.

**Tabelle 16: Tab_eGK_ObjSys_017 Initialisierte Attribute von MF / PIN.CH**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Reguläres Passwortobjekt | |
| *pwdIdentifier* | '01' = 1 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 6 | |
| *maximumLength* | 8 | |
| *startRetryCounter* | 3 | |
| *retryCounter* | 3 | |
| *transportStatus* | regularPassword | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |
| *PUK* | undefiniert | wird personalisiert |
| *pukUsage* | 10 | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 12: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.*

*Hinweis 13: Die PIN.CH und alle Multireferenz-PINs können ohne Einschränkungen geändert werden.*

**Card-G2-A_3210 - K_Personalisierung: Personalisierte Attribute von MF / PIN.CH**
Bei der Personalisierung von PIN.CH MÜSSEN die in Tab_eGK_ObjSys_117 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 17: Tab_eGK_ObjSys_117 Personalisierte Attribute von MF / PIN.CH**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *secret* | PIN-Wert gemäß [gemSpec_PINPUK_TI] | regularPassword |
| *secretLength* | Anzahl Ziffern aus dem Intervall *[minimumLength*, *maximumLength*] | |
| *PUK* | PUK-Wert gemäß [gemSpec_PINPUK_TI] | |
| *PUKLength* | 8 Ziffern | |

**[<=]**

### 5.3.9.2 MF / MRPIN.home

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Schlüsseln und Inhalten der eGK verwendet. Dieses Passwortobjekt wird nur außerhalb der TI verwendet.

**Card-G2-A_2375-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.home**
MRPIN.home MUSS die in Tab_eGK_ObjSys_018 dargestellten initialisierten Attribute besitzen.

**Tabelle 18: Tab_eGK_ObjSys_018 Initialisierte Attribute von MF / MRPIN.home**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | ‘02’ = 2 | |
| *pwdReference* | PIN.CH (‘01’ = 1) | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |
| Zugriffsregeln für die Kontaktschnittstelle | | |

| Zugriffsart | Zugriffsbedingung | Bemerkung |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Change Reference Data, P1=0<br>Get Pin Status<br>Reset RC. P1 aus der Menge {0, 1}<br>Verify | 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Change Reference Data, P1=0<br>Get Pin Status<br>Reset RC. P1 aus der Menge {0, 1}<br>Verify | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 14: 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.*

#### 5.3.9.3 MF / MRPIN.NFD

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung Notfalldatensatz verwendet.

**Card-G2-A_2408-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.NFD**
MRPIN.NFD MUSS die in Tab_eGK_ObjSys_047 dargestellten initialisierten Attribute besitzen.

**Tabelle 19: Tab_eGK_ObjSys_047 Initialisierte Attribute von MF / MRPIN.NFD**

| **Attribute** | **Wert** | **Bemerkung** |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | '03' = 3 | |
| *pwdReference* | PIN.CH ('01' = 1) | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagEnabled* | False | |
| *startSsec* | unendlich | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Disable Verification Requirement (P1='0')<br>Enable Verification Requirement (P1='0') | ALWAYS | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Disable Verification Requirement (P1='0')<br>Enable Verification Requirement (P1='0') | AUT_PACE | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 15: 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.*

#### 5.3.9.4 MF / MRPIN.DPE

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung Datensatz Persönliche Erklärungen verwendet.

**Card-G2-A_2413-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.DPE**
MRPIN.DPE MUSS die in Tab_eGK_ObjSys_052 dargestellten initialisierten Attribute besitzen.

**Tabelle 20: Tab_eGK_ObjSys_052 Initialisierte Attribute von MF / MRPIN.DPE**

| **Attribute** | **Wert** | **Bemerkung** |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | ‘04’ = 4 | |
| *pwdReference* | PIN.CH (‘01’ = 1) | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagEnabled* | False | |
| *startSsec* | unendlich | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Disable Verification Requirement (P1=’0’)<br>Enable Verification Requirement (P1=’0’) | ALWAYS | |
| Change RD, P1=0 | ALWAYS | |
| Get Pin Status | ALWAYS | |
| Reset RC. P1 aus der Menge {0, 1}<br>Verify | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)<br>Enable Verification Requirement | AUT_PACE | |

| | | |
|---|---|---|
| (P1='0') | | |
| Change RD, P1=0 | AUT_PACE | |
| Get Pin Status | AUT_PACE | |
| Reset RC. P1 aus der Menge {0, 1} Verify | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 16: 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.*

#### 5.3.9.5 MF / MRPIN.GDD

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung Gesundheitsdatendienst verwendet.

**Card-G2-A_2417-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.GDD**
MRPIN.GDD MUSS die in Tab_eGK_ObjSys_056 dargestellten initialisierten Attribute besitzen.

**Tabelle 21: Tab_eGK_ObjSys_056 Initialisierte Attribute von MF / MRPIN.GDD**

| Initialisierte Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | '05' = 5 | |
| *pwdReference* | PIN.CH ('01' = 1) | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |

| Zugriffsregeln für die Kontaktschnittstelle | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Disable Verification Requirement (P1='0')<br>Enable Verification Requirement (P1='0') | ALWAYS | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Disable Verification Requirement (P1='0')<br>Enable Verification Requirement (P1='0') | AUT_PACE | |
| 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 | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 17: 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.*

### 5.3.9.6 MF / MRPIN.NFD_READ

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung Notfalldatensatz verwendet. Dieses Multireferenz-Passwortobjekt kann im Gegensatz zu MRPIN.NFD nicht deaktiviert werden.

**Card-G2-A_2864-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.NFD_READ**
MRPIN.NFD_READ MUSS die in Tab_eGK_ObjSys_092 dargestellten initialisierten Attribute besitzen.

**Tabelle 22: Tab_eGK_ObjSys_092 Initialisierte Attribute von MF / MRPIN.NFD_READ**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | ‘07’ = 7 | |
| *pwdReference* | PIN.CH (‘01’ = 1) | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Change Reference Data, 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Change Reference Data, 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 18: 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.*

#### 5.3.9.7 MF / MRPIN.OSE

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung Organspendeerklärung verwendet. Dieses Multireferenz-Passwortobjekt kann nicht deaktiviert werden.

**Card-G2-A_3236-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.OSE**
MRPIN.OSE MUSS die in Tab_eGK_ObjSys_187 dargestellten initialisierten Attribute besitzen.

**Tabelle 23: Tab_eGK_ObjSys_187 Initialisierte Attribute von MF / MRPIN.OSE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | '09' = 9 | |
| *pwdReference* | PIN.CH ('01' = 1) | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |

| | | |
|---|---|---|
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 19: 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.*

#### 5.3.9.8 MF / MRPIN.AMTS

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung AMTS Datenmanagement verwendet.

**Card-G2-A_3247-01 - K_Initialisierung: Initialisierte Attribute von MF / MRPIN.AMTS**

MRPIN.AMTS MUSS die in Tab_eGK_ObjSys_194 dargestellten initialisierten Attribute besitzen.

**Tabelle 24: Tab_eGK_ObjSys_194 Initialisierte Attribute von MF / MRPIN.AMTS**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Multireferenz Passwortobjekt | |
| *pwdIdentifier* | ´0C´ = 12 | |
| *pwdReference* | PIN.CH (´01´ = 1) | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |

| | | |
|---|---|---|
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Disable Verification Requirement (P1='0')<br>Enable Verification Requirement (P1='0') | ALWAYS | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Disable Verification Requirement (P1='0')<br>Enable Verification Requirement (P1='0') | AUT_PACE | |
| 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 | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

#### 5.3.9.9 MF / PIN.AMTS_REP

Dieses Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung AMTS Datenmanagement durch einen Vertreter des Versicherten verwendet. Dieses Passwortobjekt kann nicht abgeschaltet werden.

**Card-G2-A_3248-01 - K_Initialisierung: Initialisierte Attribute von MF / PIN.AMTS_REP**
PIN.AMTS_REP MUSS die in Tab_eGK_ObjSys_195 dargestellten initialisierten Attribute besitzen.

**Tabelle 25: Tab_eGK_ObjSys_195 Initialisierte Attribute von MF / PIN.AMTS_REP**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Passwortobjekt | |
| *pwdIdentifier* | ´0D´ = 13 | |
| *secret* | undefined | wird personalisiert |
| *minimum Length* | 6 | |
| *maximum Length* | 8 | |
| *startRetryCounter* | 3 | |
| *retryCounter* | 3 | |
| *transportStatus* | regularPassword | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagEnabled* | True | |
| *startSsec* | unendlich | |

| | | |
|---|---|---|
| *PUK* | Wildcard | |
| *pukUsage* | 0 | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Change RD, P1=´01´ | PWD (PIN.CH) | |
| Get Pin Status | ALWAYS | |
| Reset RC. P1=´02´ | PWD (PIN.CH) | |
| Verify | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Change RD, P1=´01´ | AUT_PACE<br>AND PWD(PIN.CH) | |
| Get Pin Status | AUT_PACE | |
| Reset RC. P1=´02´ | AUT_PACE<br>AND PWD (PIN.CH) | |
| Verify | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |

| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
|---|---|---|
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3249-01 - K_Personalisierung: Personalisierte Attribute von MF / PIN.AMTS_REP**
Bei der Personalisierung von PIN.AMTS_REP MÜSSEN die in Tab_eGK_ObjSys_196 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 26: Tab_eGK_ObjSys_196 Personalisierte Attribute von MF / PIN.AMTS_REP**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *secret* | PIN-Wert gemäß [gemSpec_PINPUK_TI] | wird personalisiert |

**[<=]**

**Card-G2-A_3335-01 - K_Personalisierung: Option des PIN-Brief-Versands für MF / PIN.AMTS_REP**
Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, KANN den PIN-Wert der PIN.AMTS_REP dem Karteninhaber per PIN-Brief übermitteln.
**[<=]**

### 5.3.10 MF / PrK.eGK.AUT_CVC.E256

Dieser Schlüssel wird im Rahmen von asymmetrischen Authentisierungsprotokollen mit elliptischer Kryptographie verwendet. Der zugehörige öffentliche Schlüssel PuK.eGK.AUT_CVC.E256 ist in EF.C.eGK.AUT_CVC.E256 enthalten.

**Card-G2-A_2377-01 - K_Initialisierung: Initialisierte Attribute von MF / PrK.eGK.AUT_CVC.E256**
PrK.eGK.AUT_CVC.E256 MUSS die in Tab_eGK_ObjSys_020 dargestellten initialisierten Attribute besitzen.

**Tabelle 27: Tab_eGK_ObjSys_020 Initialisierte Attribute von MF / PrK.eGK.AUT_CVC.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, ELC 256 | |
| *keyIdentifier* | ‘09’ = 9 | |
| | | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *privateElcKey* | *domainparameter = brainpoolP256r1* | wird personalisiert |
| *privateElcKey* | *keyData = AttributNotSet* | |

| | | |
|---|---|---|
| *keyAvailable* | WildCard | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, [gemSpec_COS] [elcRoleAuthentication, elcSessionkey4SM, elcAsynchronAdmin} | |
| *numberScenario* | '0' | |
| *accessRuleSessionkeys* | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| General Authenticate<br>Internal Authenticate | ALWAYS | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktbehaftet | | |
| andere | NEVER | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| General Authenticate | ALWAYS | |
| Internal Authenticate | AUT_PACE | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| Delete | AUT_CMS | |

| | | |
|---|---|---|
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktlos | | |
| andere | NEVER | |

**[<=]**

*Hinweis 20: 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 Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.*

**Card-G2-A_3211 - K_Personalisierung: Personalisierte Attribute von MF / PrK.eGK.AUT_CVC.E256**
Bei der Personalisierung von PrK.eGK.AUT_CVC.E256 MÜSSEN die in Tab_eGK_ObjSys_118 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 28: Tab_eGK_ObjSys_118 Personalisierte Attribute von MF / PrK.eGK.AUT_CVC.E256**

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

**[<=]**

## 5.3.11 Sicherheitsanker zum Import von CV-Zertifikaten

In diesem Kapitel wird das öffentliche Signaturprüfobjekt behandelt, das an der Wurzel eines PKI Baumes für CV-Zertifikate steht. Dieses wird auch Sicherheitsanker genannt und dient dem Import von CV-Zertifikaten der zweiten Ebene. Derzeit ist ein Sicherheitsanker vorhanden.

### 5.3.11.1 MF / PuK.RCA.CS.E256

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie steht. Er wird zur Prüfung von CV-Zertifikaten der zweiten Ebene unter Nutzung elliptischer Kryptographie benötigt.

**Card-G2-A_2380-01 - K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**
PuK.RCA.CS.E256 MUSS die in Tab_eGK_ObjSys_023 dargestellten initialisierten Attribute besitzen.

**Tabelle 29: Tab_eGK_ObjSys_023 Initialisierte Attribute von MF / PuK.RCA.CS.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | öffentliches Signaturprüfobjekt, ELC 256 | |
| Für Echtkarten MÜSSEN die vier folgenden Attribute mit den unten angegebenen Werten initialisiert werden.<br>Für Option_Erstellung_von_Testkarten MÜSSEN die vier folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| *keyIdentifier* | ELC 256 Root-CA-Kennung (5 Bytes) \|\| Erweiterung (3 Bytes) | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *publicKey* | Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP[gemSpec_CVC_TSP#4.5] | |
| *expirationDate* | Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß [gemSpec_CVC_Root#5.4.2] | |
| Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden.<br>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<br>‘2A8648CE3D040302’ =<br>{1.2.840.10045.4.3.2} | |
| CHAT | • $OIDf_{lags}$ = oid_cvc_fl_ti<br>• flagList = ‘FF FFFF FFFF FFC3’ | siehe Hinweis 22: |
| *accessRulesPublicSignatureVerificationObject* | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt:<br>Delete --> AUT_CMS<br>PSO Verify Certificate --> ALWAYS | |
| *accessRulesPublicAuthenticationObject* | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt:<br>Delete --> ALWAYS<br>External Authenticate --> ALWAYS | siehe Hinweis 23: |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| PSO Verify Certificate | ALWAYS | |

| | | |
|---|---|---|
| Delete | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| PSO Verify Certificate | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

*Hinweis 21: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate.*

*Hinweis 22: Während gemäß den Tabellen in [gemSpec_PKI#6.7.5] 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.*

*Hinweis 23: 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_3243 - 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_eGK_ObjSys_188 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_eGK_ObjSys_023 personalisiert werden.

**Tabelle 30: Tab_eGK_ObjSys_188 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *publicKey* | Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-CVC-CA | personalisieren gemäß [gemSpec_TK#3.1.2] |
| *keyIdentifier* | E 256 Root-CA-Kennung (5 Bytes) \|\| Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels | |
| CHAT | • $OID_{flags}$ = oid_cvc_fl_t<br>• flagList = 'FF FFFF FFFF FFC3' | |
| *expirationDate* | Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels | |

**[<=]**

## 5.3.12 Asymmetrische Kartenadministration

Die hier beschriebene optionale Variante der Administration der eGK umfasst sowohl das Kartenmanagementsystem (CMS), als auch die Pflege der Versichertenstammdaten (VSD).

Die Administration einer eGK 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 5.3.13 beschrieben.

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

Während die Schlüsselpaare auf Smartcards typischerweise kartenindividuell sind, so ist es denkbar, dass mit einem Schlüsselpaar eines administrierenden Systems genau eine,

oder mehrere oder alle Smartcards administriert werden. Das Sicherheitskonzept des administrierenden Systems erscheint die geeignete Stelle zu sein um eine Variante auszuwählen.

#### 5.3.12.1 MF / PuK.RCA.ADMINCMS.CS.E256

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie für die asymmetrische VSD/CMS-Authentisierung steht. Es wird dabei vorausgesetzt, dass bezüglich der organisationsspezifischen CV-Zertifikate für CMS und VSD eine einzige organisationsspezifische CVC-Root genutzt wird. PuK.RCA.ADMINCMS.CS.E256 wird für den Import weiterer Schlüssel für die elliptische Kryptographie benötigt.

**Card-G2-A_2986-01 - K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**
PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab_eGK_ObjSys_126 dargestellten initialisierten Attribute besitzen.

**Tabelle 31: Tab_eGK_ObjSys_126 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.<br>Für Option_Erstellung_von_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| CHAT | $OID_{flags}$ = oid_cvc_fl_cms<br>flagList = 'FF DFFF FFFF FFFF' | siehe Hinweis 25: |
| *expirationDate* | Identisch zu „expirationDate" von PuK.RCA.CS.E256 | |
| Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden.<br>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 Interfaces und alle relevanten Werte von lifeCycleStatus gilt:<br>Delete --> AUT_CMS<br>PSO Verify Certificate --> ALWAYS | |
| *accessRulesPublicAuthenticationObject* | Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt:<br>Delete --> ALWAYS | siehe Hinweis 23: |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| PSO Verify Certificate | ALWAYS | |
| Delete | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| PSO Verify Certificate | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

*Hinweis 24: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate.*

*Hinweis 25: Während gemäß den Tabellen in [gemSpec_PKI#6.7.5] 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_3212-01 - K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**
Bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 MÜSSEN die in Tab_eGK_ObjSys_121 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_eGK_ObjSys_126 personalisiert werden.

**Tabelle 32: Tab_eGK_ObjSys_121 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *publicKey* | Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Admin-CVC-Root | |
| *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<br>flagList = 'FF DFFF FFFF FFFF' | |
| *expirationDate Option_Erstellung _von_Testkarten* | Identisch zu „expirationDate" des personalisierten PuK.RCA.CS.E256 | |

**[<=]**

## 5.3.13 Symmetrische Kartenadministration

Die hier beschriebene Variante der Administration der eGK umfasst sowohl das Kartenmanagementsystem (CMS), als auch die Pflege der Versichertenstammdaten (VSD).

Die Administration einer eGK 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 5.3.12 beschrieben.

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

Während die Schlüssel auf Smartcards typischerweise kartenindividuell sind, ist es denkbar, dass mit einem Schlüssel eines administrierenden Systems genau eine, oder mehrere oder alle Smartcards administriert werden. Das Sicherheitskonzept des

administrierenden Systems erscheint die geeignete Stelle zu sein um eine Variante auszuwählen.

Es sind getrennte Schlüssel für das CMS und den VSD definiert. Bei der Personalisierung sind nur die Schlüssel personalisieren, die tatsächlich benötigt werden.

#### 5.3.13.1 MF / SK.CMS.AES128

Dieser AES-Schlüssel mit 128 bit Schlüssellänge wird benötigt, um administrative Aufgaben am Objektsystem (z. B. das Anlegen von neuen Anwendungen) auszuführen.

**Card-G2-A_2388 - K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128**
SK.CMS.AES128 MUSS die in Tab_eGK_ObjSys_027 dargestellten initialisierten Attribute besitzen.

**Tabelle 33: Tab_eGK_ObjSys_027 Initialisierte Attribute von MF / SK.CMS.AES128**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Symmetrisches Authentisierungsobjekt | |
| *keyType* | AES-128 | |
| *keyIdentifier* | '13' = 19 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 128 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 128 Bit | wird personalisiert |
| *numberScenario* | 0 | |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec_COS] | |
| *accessRuleSessionkeys* | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |

| | | |
|---|---|---|
| Delete | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS<br>NEVER | siehe Hinweis 27: |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

*Hinweis 26:Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind: Activate, Deactivate, Delete, External Authenticate, General Authenticate, Get Security Status Key, Internal Authenticate, Mutual Authenticate, Terminate.*

*Hinweis 27: Falls ein Kartenherausgeber Karten asynchron unter Nutzung symmetrischer Schlüssel administrieren will, so ist die Variante „ALWAYS" umzusetzen. Andernfalls liegt es im Belieben des Kartenherstellers ob die Variante „ALWAYS" oder die Variante „NEVER" umgesetzt wird.*

**Card-G2-A_3213 - K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128**

Bei der Personalisierung von SK.CMS.AES128 MÜSSEN die in Tab_eGK_ObjSys_122 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 34: Tab_eGK_ObjSys_122 Personalisierte Attribute von MF / SK.CMS.AES128**

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

**[<=]**

### 5.3.13.2 MF / SK.CMS.AES256

Dieser AES-Schlüssel mit 256 bit Schlüssellänge wird benötigt, um administrative Aufgaben am Objektsystem (z. B. das Anlegen von neuen Anwendungen) auszuführen.

**Card-G2-A_2389-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256**
SK.CMS.AES256 MUSS die in Tab_eGK_ObjSys_028 dargestellten initialisierten Attribute besitzen.

**Tabelle 35: Tab_eGK_ObjSys_028 Initialisierte Attribute von MF / SK.CMS.AES256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Symmetrisches Authentisierungsobjekt | |
| *keyType* | AES-256 | |
| *keyIdentifier* | ’18’ = 24 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 256 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 256 Bit | wird personalisiert |
| *numberScenario* | 0 | |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec_COS] | |
| *accessRuleSessionkeys* | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |

| | | |
|---|---|---|
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |
| Delete | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

**Card-G2-A_3214 - K_Personalisierung: Personalisierte Attribute von von MF / SK.CMS.AES256**
Bei der Personalisierung von SK.CMS.AES256 MÜSSEN die in Tab_eGK_ObjSys_123 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 36: Tab_eGK_ObjSys_123 Personalisierte Attribute von MF / SK.CMS.AES256**

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

**[<=]**

### 5.3.13.3 MF / SK.VSD.AES128

Dieser AES-Schlüssel mit 128 bit Schlüssellänge wird benötigt, um administrative Aufgaben bezüglich der Dateien mit Versichertendaten (z. B. das Aktualisieren der Daten) auszuführen.

**Card-G2-A_2390-01 - K_Initialisierung: Initialisierte Attribute von MF /SK.VSD.AES128**
SK.VSD.AES128 MUSS die in Tab_eGK_ObjSys_029 dargestellten initialisierten Attribute besitzen.

**Tabelle 37: Tab_eGK_ObjSys_029 Initialisierte Attribute von MF / SK.VSD.AES128**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Symmetrisches Authentisierungsobjekt | |
| *keyType* | AES-128 | |
| *keyIdentifier* | ’12’ = 18 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 128 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 128 Bit t | wird personalisiert |
| *numberScenario* | 0 | |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec_COS] | |
| *accessRuleSessionkeys* | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |
| Delete | AUT_CMS | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

**Card-G2-A_3215 - K_Personalisierung: Personalisierte Attribute von MF / SK.VSD.AES128**
Bei der Personalisierung von SK.VSD.AES128 MÜSSEN die in Tab_eGK_ObjSys_124 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 38: Tab_eGK_ObjSys_124 Personalisierte Attribute von MF / SK.VSD.AES128**

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

**[<=]**

### 5.3.13.4 MF/ SK.VSD.AES256

Dieser AES-Schlüssel mit 256 bit Schlüssellänge wird benötigt, um administrative Aufgaben bezüglich der Dateien mit Versichertendaten (z. B. das Aktualisieren der Daten) auszuführen.

**Card-G2-A_2391-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.VSD.AES256**
SK.VSD.AES256 MUSS die in Tab_eGK_ObjSys_030 dargestellten initialisierten Attribute besitzen.

**Tabelle 39: Tab_eGK_ObjSys_030 Initialisierte Attribute von MF / SK.VSD.AES256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Symmetrisches Authentisierungsobjekt | |
| *keyType* | AES-256 | |
| *keyIdentifier* | '19' = 25 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 256 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES mit 256 Bit | wird personalisiert |
| *numberScenario* | 0 | |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec_COS] | |
| *accessRuleSessionkeys* | irrelevant | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |
| Delete | AUT_CMS | |

| | | |
|---|---|---|
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Mutual Authenticate | ALWAYS | |
| General Authenticate | ALWAYS | siehe Hinweis 27: |
| | NEVER | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

**Card-G2-A_3216 - K_Personalisierung: Personalisierte Attribute von MF / SK.VSD.AES256**
Bei der Personalisierung von SK.VSD.AES256 MÜSSEN die in Tab_eGK_ObjSys_125 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 40: Tab_eGK_ObjSys_125 Personalisierte Attribute von MF / SK.VSD.AES256**

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

**[<=]**

### 5.3.14 MF / SK.CAN

Das Schlüsselobjekt CAN (Card Access Number) dient dazu eine kontaktlose Kommunikationsschnittstelle zur eGK kryptographisch abzusichern.

**Card-G2-A_2862 - K_Initialisierung: Initialisierte Attribute von MF / SK.CAN**
SK.CAN MUSS die in Tab_eGK_ObjSys_093 dargestellten initialisierten Attribute besitzen.

**Tabelle 41: Tab_eGK_ObjSys_093 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 | wird personalisiert |
| *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 | |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| General Authenticate | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | NEVER | |

**[<=]**

*Hinweis 28: Kommandos, die gemäß [gemSpec_COS] mit symmetrischen Kartenverbindungsobjekten arbeiten, sind: Activate; Deactivate; Delete, General Authenticate, Terminate.*

**Card-G2-A_3229 - K_Personalisierung: Personalisierte Attribute von MF / SK.CAN**
Bei der Personalisierung von SK.CAN MÜSSEN die in Tab_eGK_ObjSys_181 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 42: Tab_eGK_ObjSys_181 Personalisierte Attribute von MF / SK.CAN**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *can* | SK.CAN gemäß [gemSpec_CAN_TI] | siehe Card-G2-A_2863] |

**[<=]**

**Card-G2-A_2863 - K_Personalisierung: Anzahl Stellen einer CAN**
Das Attribut *can* von SK.CAN MUSS eine sechsstellige Ziffernfolge gemäß [gemSpec_CAN_TI] enthalten.**[<=]**

## 5.4 Gesundheitsanwendung, Health Care Application (DF.HCA)

**Card-G2-A_2394 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA**
DF.HCA MUSS die in Tab_eGK_ObjSys_033 dargestellten initialisierten Attribute besitzen.

**Tabelle 43: Tab_eGK_ObjSys_033 Initialisierte Attribute von MF / DF.HCA**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | 'D276000001 02' | |
| *fileIdentifier* | – | |
| *lifeCycleStatus* | „Operational state (activated)" | |

| | | |
|---|---|---|
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | AUT_CMS | |
| Deactivate | AUT_CMS | |
| Load Application | AUT_CMS | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Activate | AUT_CMS | |
| Deactivate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | AUT_CMS | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |

| | | |
|---|---|---|
| | AUT_CMS | |
| Deactivate | AUT_CMS | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Activate | AUT_CMS | |
| Deactivate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 29: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 30: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4 relevant.*

*Hinweis 31: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.*

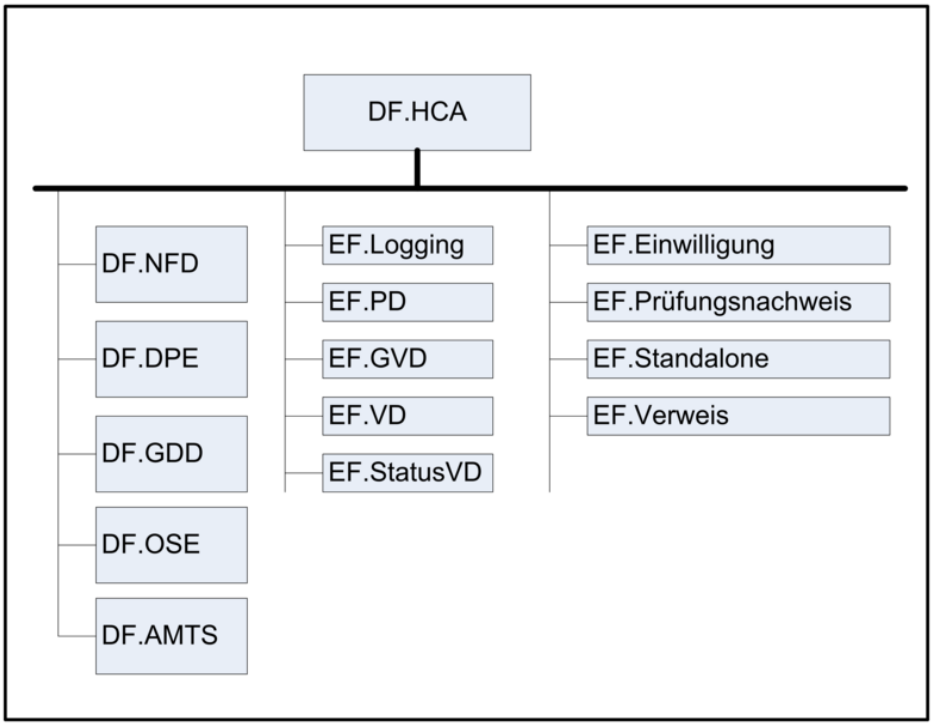



**Abbildung 2: Abb_eGK_ObjSys_002 Dateistruktur der Gesundheitsanwendung**

### 5.4.1 MF / DF.HCA / EF.Einwilligung

Diese Datei enthält die Information über die Einwilligungen zu freiwilligen Anwendungen.

**Card-G2-A_2395-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Einwilligung**
EF.Einwilligung MUSS die in Tab_eGK_ObjSys_034 dargestellten initialisierten Attribute besitzen.

**Tabelle 44: Tab_eGK_ObjSys_034 Initialisierte Attribute von MF / DF.HCA / EF.Einwilligung**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear fixes Elementary File | |
| *fileIdentifier* | ‘D0 05’ | |
| *shortFileIdentifier* | ‘05’= 5 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |

| | | |
|---|---|---|
| *flagChecksum* | True | |
| *maxNumRecords* | 10 Records | |
| *maxRecordLength* | 69 Oktett | |
| *flagRecordLCS* | True | |
| *recordList*<br>*alle Records* | *Records aktiviert, Inhalt der Records ‘00…00’* | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Activate Record<br>Deactivate Record | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.24]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10)])* | |
| Read Record<br>Search Record | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.25]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10)])* | |
| Update Record | PWD(PIN.CH) AND flagTI.27<br>*(informativ: OR [PWD(PIN.CH) AND (C.2.3.4)]* | Siehe Hinweis 33: |
| Erase Record<br>Delete Record | PWD(PIN.CH) AND flagTI.25<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate Record<br>Deactivate Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.24] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10)])* | |
| Read Record<br>Search Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.25] } | |

| | | |
|---|---|---|
| | *(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10)])* | |
| Update Record | AUT_PACE<br>AND [PWD(PIN.CH) AND flagTI.27]<br>*(informativ: OR [PWD(PIN.CH) AND (C.2.3.4)])* | Siehe Hinweis 33: |
| Erase Record<br>Delete Record | AUT_PACE<br>AND [PWD(PIN.CH) AND flagTI.25]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 32: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate*

*Hinweis 33: Eine Einwilligung wird anwendungsspezifisch eingetragen. Da die Einwilligung nur im Beisein eines Leistungserbringers eingetragen werden kann, wird für die Freischaltung des Schreibrechts die Eingabe der PIN.CH verlangt.*

### 5.4.2 MF / DF.HCA / EF.GVD

Diese Datei enthält die geschützten Versichertendaten. Die Details sind in Tab_eGK_ObjSys_035 beschrieben.

**Card-G2-A_2396-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.GVD**
EF.GVD MUSS die in Tab_eGK_ObjSys_035 dargestellten initialisierten Attribute besitzen.

**Tabelle 45: Tab_eGK_ObjSys_035 Initialisierte Attribute von MF / DF.HCA / EF.GVD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'D0 03' | |
| *shortFileIdentifier* | '03'= 3 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | False | |

| | | |
|---|---|---|
| | | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘0258’ Oktett = 600 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.29]<br>OR flagTI.30<br>OR {AUT_VSD}<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.7.10) OR C2.3.4.5.8.9)])* | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | ( AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.29]<br>OR flagTI.30 })<br>OR AUT_VSD | |

| | | |
|---|---|---|
| | *(informativ: OR [PWD(PIN.CH) AND (C.1.7.10) OR C2.3.4.5.8.9)])* | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 34: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

### 5.4.3 MF / DF.HCA / EF.Logging

Diese Datei enthält Protokollierungsinformationen über Zugriffe auf die eGK.

**Card-G2-A_2397-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Logging**
EF.Logging MUSS die in Tab_eGK_ObjSys_036 dargestellten initialisierten Attribute besitzen.

**Tabelle 46: Tab_eGK_ObjSys_036 Initialisierte Attribute von MF / DF.HCA / EF.Logging**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | zyklisches Elementary File | |
| *fileIdentifier* | 'D0 06' | |
| *shortFileIdentifier* | '06'= 6 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *maxNumRecords* | 50 Records | |

| | | |
|---|---|---|
| | | |
| *maxRecordLength* | 46 Oktett | |
| *flagRecordLCS* | False | |
| *recordList*<br>*alle Records* | *Records aktiviert, Inhalt der Records ‘00…00’* | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Append Record | flagTI.32<br>*(informativ: C1.2.3.4.5.7.8.9.10)* | |
| Read Record<br>Search Record | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10))* | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Append Record | AUT_PACE<br>AND flagTI.32<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)*<br>*OR C1.2.3.4.5.7.8.9.10)* | |
| Read Record<br>Search Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [ PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER | |

| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
|---|---|---|
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 35: 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.*

### 5.4.4 MF / DF.HCA / EF.PD

Diese Datei enthält die persönlichen Daten des Karteninhabers.

**Card-G2-A_2398-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.PD**
EF.PD MUSS die in Tab_eGK_ObjSys_037 dargestellten initialisierten Attribute besitzen.

**Tabelle 47: Tab_eGK_ObjSys_037 Initialisierte Attribute von MF / DF.HCA / EF.PD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘D0 01’ | |
| *shortFileIdentifier* | ‘01’= 1 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘0352’ Oktett = 850 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |

| | | |
|---|---|---|
| Read Binary | ALWAYS | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_VSD | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 36: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

### 5.4.5 MF / DF.HCA / EF.Prüfungsnachweis

Diese Datei speichert einen Nachweis, der im Rahmen einer Online-Prüfung erstellt wurde.

**Card-G2-A_2399-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Prüfungsnachweis**
EF.Prüfungsnachweis MUSS die in Tab_eGK_ObjSys_038 dargestellten initialisierten Attribute besitzen.

**Tabelle 48: Tab_eGK_ObjSys_038 Initialisierte Attribute von MF / DF.HCA / EF.Prüfungsnachweis**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘D0 1C’ | |
| *shortFileIdentifier* | ‘1C’= 28 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘012C’ Oktett = 300 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | ALWAYS | |

| | | |
|---|---|---|
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 37: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

### 5.4.6 MF / DF.HCA / EF.Standalone

Diese Datei enthält die Informationen aus EF.GVD und EF.DPE in verschlüsselter Form.

**Card-G2-A_2400-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Standalone**
EF.Standalone MUSS die in Tab_eGK_ObjSys_039 dargestellten initialisierten Attribute besitzen.

**Tabelle 49: Tab_eGK_ObjSys_039 Initialisierte Attribute von MF / DF.HCA / EF.Standalone**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |

| | | |
|---|---|---|
| *fileIdentifier* | 'DA 0A' | |
| *shortFileIdentifier* | '0A'= 10 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '384' Oktett = 900 Oktett | |
| *positionLogicalEndOfFile* | '0' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| **Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos** | | |
| Delete | AUT_CMS | |

| | | |
|---|---|---|
| Read Binary<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 38: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

### 5.4.7 MF / DF.HCA / EF.StatusVD

Diese Datei enthält die Information über den Status der Daten in EF.PD, EF.VD und EF.GVD.

**Card-G2-A_2401-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.StatusVD**
EF.StatusVD MUSS die in Tab_eGK_ObjSys_040 dargestellten initialisierten Attribute besitzen.

**Tabelle 50: Tab_eGK_ObjSys_040 Initialisierte Attribute von MF / DF.HCA / EF.StatusVD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'D0 0C' | |
| *shortFileIdentifier* | '0C'= 12 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '0019' Oktett = 25 Oktett | |

| | | |
|---|---|---|
| | | |
| *positionLogicalEndOfFile* | ’0’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | ALWAYS | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_VSD | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.4.8 MF / DF.HCA / EF.VD

Diese Datei enthält die Versichertendaten.

**Card-G2-A_2403-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.VD**
EF.VD MUSS die in Tab_eGK_ObjSys_042 dargestellten initialisierten Attribute besitzen.

**Tabelle 51: Tab_eGK_ObjSys_042 Initialisierte Attribute von MF / DF.HCA / EF.VD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘D0 02’ | |
| *shortFileIdentifier* | ‘02’= 2 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘04 E2’ Oktett = 1.250 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | ALWAYS | |

| | | |
|---|---|---|
| | | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_VSD | |
| Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_VSD | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.4.9 MF / DF.HCA / EF.Verweis

Diese Datei enthält die Informationen über die Speicherorte der Daten der freiwilligen Anwendungen, die nicht auf der eGK gespeichert werden.

**Card-G2-A_2404-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Verweis**
EF.Verweis MUSS die in Tab_eGK_ObjSys_043 dargestellten initialisierten Attribute besitzen.

**Tabelle 52: Tab_eGK_ObjSys_043 Initialisierte Attribute von MF / DF.HCA / EF.Verweis**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear fixes Elementary File | |
| *fileIdentifier* | 'D0 09' | |
| *shortFileIdentifier* | '09'= 9 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *maxNumRecords* | 10 Records | |
| *maxRecordLength* | 20 Oktett | |
| *flagRecordLCS* | True | |
| *recordList*<br>*alle Records* | *Record aktiviert, Inhalt des Records '00…00'* | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate Record<br>Deactivate Record | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.24]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10))* | |
| Read Record<br>Search Record<br>Update Record | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.28]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.9.10))* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate Record<br>Deactivate Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [ PWD(PIN.CH) AND flagTI.24 ] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.10))* | |
| Read Record<br>Search Record<br>Update Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [ PWD(PIN.CH) AND flagTI.28 ] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.9.10))* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 39: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate*

### 5.4.10 Anwendung Notfalldatensatz (DF.NFD)

Diese Anwendung enthält einen Notfalldatensatz.

**Card-G2-A_2405-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD**
DF.NFD MUSS die in Tab_eGK_ObjSys_044 dargestellten initialisierten Attribute besitzen.

**Tabelle 53: Tab_eGK_ObjSys_044 Initialisierte Attribute von MF / DF.HCA / DF.NFD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | 'D276 0001 4407' | |
| *fileIdentifier* | - | herstellerspezifisch |
| *lifeCycleStatus* | „Operational state (activated)" | |

| | | |
|---|---|---|
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | |
| Deactivate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | |
| Load Application | AUT_CMS | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Activate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden |
| | AUT_PACE | |

| | | |
|---|---|---|
| | AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]}<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | Varianten erlaubt |
| Deactivate | AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]}<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Activate | AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]}<br>*((informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER<br>AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.NFD) AND flagTI.14]<br>OR [PWD(PIN.CH) AND flagTI.33]}<br>*(informativ: [PWD(MRPIN.NFD) AND (C.1.10)]*<br>*OR [PWD( PIN.CH) AND (C.1.10)])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 40: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 41: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.10 relevant.*

*Hinweis 42: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.*

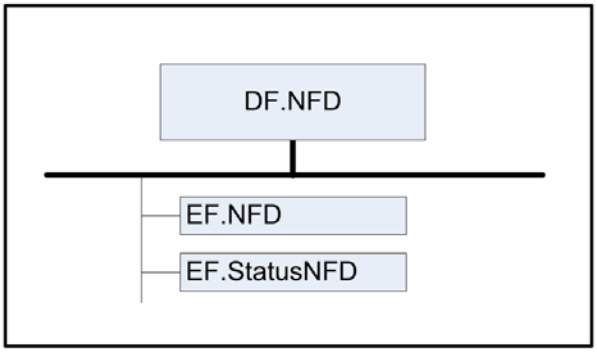



**Abbildung 3: Abb_eGK_ObjSys_003 Dateistruktur der Anwendung Notfalldatensatz**

### 5.4.10.1 MF / DF.HCA / DF.NFD / EF.NFD

Diese Datei enthält einen Notfalldatensatz.

**Card-G2-A_2406-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.NFD**

EF.NFD MUSS die in Tab_eGK_ObjSys_045 dargestellten initialisierten Attribute besitzen.

**Tabelle 54: Tab_eGK_ObjSys_045 Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.NFD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘D0 10’ | |
| *shortFileIdentifier* | ‘10’= 16 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | False | |
| *numberOfOctet* | ‘2F 2B’ Oktett = 12.075 Oktett | |
| *positionLogicalEndOfFile* | ‘2F 2B’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | ‘00…00’ | |

| Zugriffsregeln für die Kontaktschnittstelle | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | flagTI.18<br>OR [PWD(MRPIN.NFD_READ) AND flagTI.17]<br>OR [PWD(PIN.CH) AND flagTI.17 AND flagTI.33]<br>*(informativ: C2.7 OR [PWD(MRPIN.NFD_READ) AND (C.3.4.10)] OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 44: |
| Erase Binary<br>Set Logical EOF (P1P2 = '90 00')<br>Update Binary<br>Write Binary | [PWD(MRPIN.NFD) AND flagTI.15]<br>OR [PWD(PIN.CH) AND flagTI.15 AND flagTI.33]<br>*(informativ: [PWD(MRPIN.NFD) AND (C.2.10)] OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 45: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { flagTI.18<br>OR [PWD(MRPIN.NFD_READ) AND flagTI.17]<br>OR [PWD(PIN.CH) AND flagTI.17 AND flagTI.33]}<br>*(informativ: C2.7 OR [PWD(MRPIN.NFD_READ) AND (C.3.4.10)] OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 44: |
| Erase Binary<br>Set Logical EOF (P1P2 = '90 00')<br>Update Binary<br>Write Binary | AUT_PACE<br>AND {PWD(MRPIN.NFD) AND flagTI.15]<br>OR [PWD(PIN.CH) AND flagTI.15 AND flagTI.33]}<br>*(informativ: [PWD(MRPIN.NFD) AND (C.2.10)] OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 45: |
| andere | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 43: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

*Hinweis 44: Profil.10 kennzeichnet die Rolle zu „Anwendungen des Versicherten" (LE-AdV) im Kontrollbereich eines Leistungserbringers, die zum Zugriff auf die Notfalldaten berechtigt ist. Dies ist der Unterschied zum Profil Profil.1 (KTR-AdV) für „Anwendungen des Versicherten" im Kontrollbereich eines Kostenträgers.*

*Hinweis 45: Das Lösch- und Schreibrecht mit Profil.10 ist beschränkt auf das Löschen der Daten sowie das Wiederherstellen der Daten aus einem Backup. Diese Beschränkung ist außerhalb der eGK durchzusetzen.*

### 5.4.10.2 MF / DF.HCA / DF.NFD / EF.StatusNFD

Diese Datei enthält die Information über den Status des Notfalldatensatzes.

**Card-G2-A_2407-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.StatusNFD**

EF.StatusNFD MUSS die in Tab_eGK_ObjSys_046 dargestellten initialisierten Attribute besitzen.

**Tabelle 55: Tab_eGK_ObjSys_046 Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.StatusNFD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'D0 0E' | |
| *shortFileIdentifier* | '0E'= 14 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '0019' Oktett = 25 Oktett | |

| | | |
|---|---|---|
| *positionLogicalEndOfFile* | '0019' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | '00…00' | |

| Zugriffsregeln für die Kontaktschnittstelle | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | flagTI.18<br>OR [PWD(MRPIN.NFD_READ) AND flagTI.17]<br>OR [PWD(PIN.CH) AND flagTI.17 AND flagTI.33]<br>*(informativ: C.2.7*<br>*OR [PWD(MRPIN.NFD_READ) AND (C.3.4.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 44: |
| Erase Binary<br>Set Logical EOF (P1P2 = '8E 00')<br>Update Binary<br>Write Binary | [PWD(MRPIN.NFD) AND flagTI.15]<br>OR [PWD(PIN.CH) AND flagTI.15 AND flagTI.33]<br>*(informativ: [PWD(MRPIN.NFD) AND (C.2.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 45: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { flagTI.18<br>OR [PWD(MRPIN.NFD_READ) AND flagTI.17]<br>OR [PWD(PIN.CH) AND flagTI.17<br>AND flagTI.33]}<br>*(informativ: OR C2.7*<br>*OR [PWD(MRPIN.NFD_READ) AND (C.3.4.10)]* | siehe Hinweis 44: |

| | | |
|---|---|---|
| | *OR [PWD(PIN.CH) AND (C.10)])* | |
| Erase Binary<br>Set Logical EOF (P1P2 = '8E 00')<br>Update Binary<br>Write Binary | AUT_PACE<br>AND { [PWD(MRPIN.NFD) AND flagTI.15]<br>OR [PWD(PIN.CH) AND flagTI.15<br>AND flagTI.33]}<br><br>*(informativ: [PWD(MRPIN.NFD) AND (C.2.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | siehe Hinweis 45: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.4.11 Anwendung Datensatz Persönliche Erklärungen (DF.DPE)

Diese Anwendung enthält den Datensatz mit den persönlichen Erklärungen des Versicherten.

**Card-G2-A_2410-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.DPE**
DF.DPE MUSS die in Tab_eGK_ObjSys_049 dargestellten initialisierten Attribute besitzen.

**Tabelle 56: Tab_eGK_ObjSys_049 Initialisierte Attribute von MF / DF.HCA / DF.DPE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | 'D276 0001 4408' | |
| *fileIdentifier* | - | herstellerspezifisch |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate | ALWAYS | herstellerspezifisch |

| | | |
|---|---|---|
| | PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10]*<br>*OR [PWD(PIN.CH) AND C.1.10]))* | ist eine der beiden Varianten erlaubt |
| Deactivate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10]*<br>*OR [PWD(PIN.CH) AND C.1.10]))* | |
| Load Application | AUT_CMS | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Activate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10]*<br>*OR [PWD(PIN.CH) AND C.1.10]))* | |
| Deactivate | NEVER<br>PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10]*<br>*OR [PWD(PIN.CH) AND C.1.10]))* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Activate | ALWAYS<br>AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10]*<br>*OR [PWD(PIN.CH) AND C.1.10]))* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Deactivate | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33] } | |

| | | |
|---|---|---|
| | *(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10] OR [PWD(PIN.CH) AND C.1.10]))* | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Activate | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10] OR [PWD(PIN.CH) AND C.1.10]))* | |
| Deactivate | NEVER<br>AUT_PACE<br>AND PWD(MRPIN.home)<br>OR [PWD(MRPIN.DPE) AND flagTI.19]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.DPE ) AND C.1.10] OR [PWD(PIN.CH) AND C.1.10]))* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 46: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 47: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekten in 5.4.11 relevant.*

*Hinweis 48: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.*

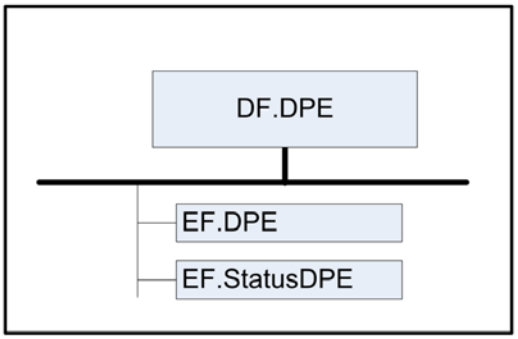



**Abbildung 4: Abb_eGK_ObjSys_004 Dateistruktur der Anwendung Datensatz Persönliche Erklärungen**

#### 5.4.11.1 MF / DF.HCA / DF.DPE / EF.DPE

Diese Datei enthält den Datensatz mit den persönlichen Erklärungen des Versicherten.

**Card-G2-A_2411-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.DPE**

EF.DPE MUSS die in Tab_eGK_ObjSys_050 dargestellten initialisierten Attribute besitzen.

**Tabelle 57: Tab_eGK_ObjSys_050 Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.DPE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘D0 1B’ | |
| *shortFileIdentifier* | ‘1B’= 27 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘06BD’ Oktett = 1.725 Oktett | |
| *positionLogicalEndOfFile* | ‘06BD’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | ‘00…00’ | |

| | | |
|---|---|---|
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | [PWD(PIN.CH) AND flagTI.33]<br>OR flagTI.23<br>OR PWD(MRPIN.home)<br>*(informativ: [PWD(PIN.CH) AND (C.1.10)]*<br>*OR C.2*<br>*OR PWD(MRPIN.home)* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '9B 00')<br>Update Binary<br>Write Binary | [PWD(MRPIN.DPE) AND flagTI.20]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.DPE) AND (C.1.2.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { [PWD(PIN.CH) AND flagTI.33]<br>OR flagTI.23<br>OR PWD(MRPIN.home) }<br>*(informativ:[PWD(PIN.CH) AND (C.1.10)]*<br>*OR C.2*<br>*OR PWD(MRPIN.home)* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '9B 00')<br>Update Binary<br>Write Binary | AUT_PACE<br>AND { [PWD(MRPIN.DPE) AND flagTI.20]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.DPE) AND (C.1.2.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |

| | | |
|---|---|---|
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 49: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

#### 5.4.11.2 MF / DF.HCA / DF.DPE / EF.StatusDPE

Diese Datei enthält die Information über den Status des Datensatzes mit den persönlichen Erklärungen.

**Card-G2-A_2412-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.StatusDPE**
EF.StatusDPE MUSS die in Tab_eGK_ObjSys_051 dargestellten initialisierten Attribute besitzen.

**Tabelle 58: Tab_eGK_ObjSys_051 Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.StatusDPE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘D0 18’ | |
| *shortFileIdentifier* | ‘18’= 24 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘0019’ Oktett = 25 Oktett | |
| *positionLogicalEndOfFile* | ‘0019’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | ‘00…00’ | |

| Zugriffsregeln für die Kontaktschnittstelle | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | [PWD(PIN.CH) AND flagTI.33]<br>OR flagTI.23<br>OR PWD(MRPIN.home)<br>*(informativ: [PWD(PIN.CH) AND (C.1.10)]*<br>*OR C.2*<br>*OR PWD(MRPIN.home)* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '98 00')<br>Update Binary<br>Write Binary | [PWD(MRPIN.DPE) AND flagTI.20]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.DPE) AND (C.1.2.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { [PWD(PIN.CH) AND flagTI.33]<br>OR flagTI.23<br>OR PWD(MRPIN.home) }<br>*(informativ:[PWD(PIN.CH) AND (C.1.10)]*<br>*OR C.2*<br>*OR PWD(MRPIN.home)* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '98 00')<br>Update Binary<br>Write Binary | AUT_PACE<br>AND { [PWD(MRPIN.DPE) AND flagTI.20]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.DPE) AND (C.1.2.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.4.12 Anwendung Gesundheitsdatendienst (GDD)

Diese Anwendung enthält Daten zum Gesundheitsdatendienst des Versicherten.

**Card-G2-A_2415-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.GDD**
DF.GDD MUSS die in Tab_eGK_ObjSys_054 dargestellten initialisierten Attribute besitzen.

**Tabelle 59: Tab_eGK_ObjSys_054 Initialisierte Attribute von MF / DF.HCA / DF.GDD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | ‘D276 0001 440A’ | |
| *fileIdentifier* | - | herstellerspezifisch |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10))])* | |
| Deactivate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10))])* | |
| Load Application | AUT_CMS | |
| Get Random | ALWAYS | |

| | | |
|---|---|---|
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Activate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10))])* | |
| Deactivate | NEVER<br>PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10))])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Activate | ALWAYS<br>AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10))])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Deactivate | AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10))])* | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Activate | AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33] } | |

| | | |
|---|---|---|
| | *(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | AUT_PACE<br>AND {PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.39]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.GDD ) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 50: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 51: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.12 relevant.*

*Hinweis 52: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.*

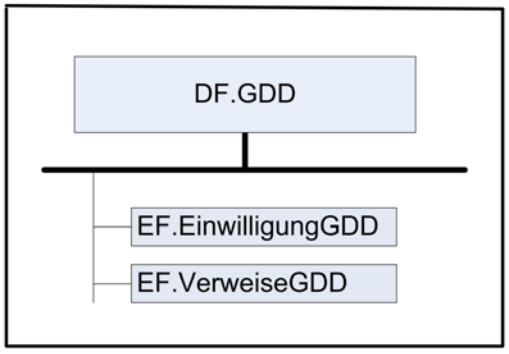



**Abbildung 5: Abb_eGK_ObjSys_005 Dateistruktur der Anwendung Gesundheitsdatendienst**

#### 5.4.12.1 MF / DF.HCA / DF.GDD / EF.EinwilligungGDD

Diese Datei enthält die Information über die Einwilligungen zu freiwilligen Anwendungen Gesundheitsdatendienste.

**Card-G2-A_2416-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.EinwilligungGDD**

EF.EinwilligungGDD MUSS die in Tab_eGK_ObjSys_055 dargestellten initialisierten Attribute besitzen.

**Tabelle 60: Tab_eGK_ObjSys_055 Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.EinwilligungGDD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear variables Elementary File | |
| *fileIdentifier* | 'D0 13' | |
| *shortFileIdentifier* | '13'= 19 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '0258' Oktett = 600 Oktett | |
| *maxNumRecords* | 20 Records | |
| *maxRecordLength* | 60 Oktett | |
| *flagRecordLCS* | True | |
| *recordList* | 17 Records aktiviert, Inhalt der Records '000000e164f0467ffe5d379d0b8bb7cb23230263ada3508540508399db7c06aa873a3d' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Append Record<br>Erase Record<br>Delete Record<br>Read Record<br>Search Record<br>Update Record | PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.40]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.GDD) AND (C.1.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND C.1.10])* | siehe Hinweis 54: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |

| | | |
|---|---|---|
| | | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Append Record<br>Erase Record<br>Delete Record<br>Read Record<br>Search Record<br>Update Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.40]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.GDD) AND (C.1.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND C.1.10])* | siehe Hinweis 54: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 53: Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind: Activate, Activate Record, Append Record, Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record, Write Record.*

*Hinweis 54: Eine Einwilligung wird anwendungsspezifisch eingetragen. Der Zugriff auf die Einwilligung im Beisein eines Leistungserbringers erfolgt nach Freischaltung durch Eingabe der MRPIN.GDD. Der Zugriff auf die Einwilligung in einer AdV-Umgebung erfogt nach Freischaltung durch Eingabe der PIN.CH.*

### 5.4.12.2 MF / DF.HCA / DF.GDD / EF.VerweiseGDD

Diese Datei enthält die Informationen über die Speicherorte der Daten der freiwilligen Anwendungen Gesundheitsdatendienste, die nicht auf der eGK gespeichert werden.

**Card-G2-A_2418-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.VerweiseGDD**

EF.VerweiseGDD MUSS die in Tab_eGK_ObjSys_057 dargestellten initialisierten Attribute besitzen.

**Tabelle 61: Tab_eGK_ObjSys_057 Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.VerweiseGDD**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear variables Elementary File | |

| | | |
|---|---|---|
| *fileIdentifier* | 'D0 1A' | |
| *shortFileIdentifier* | '1A'= 26 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '04B0' Oktett = 1200 Oktett | |
| *maxNumRecords* | 20 Records | |
| *maxRecordLength* | 60 Oktett | |
| *flagRecordLCS* | True | |
| *recordList* | 17 Records aktiviert, Inhalt der Records '000000e164f0467ffe5d379d0b8bb7cb232302ecd446eee98852d785614ef5f0acdb23' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |

| Zugriffsregeln für die Kontaktschnittstelle | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Append Record<br>Erase Record<br>Delete Record<br>Read Record<br>Search Record<br>Update Record | PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.40]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.GDD) AND (C.1.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND C.1.10])* | siehe Hinweis 54: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |

| Zugriffsregeln für die kontaktlose Schnittstelle | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Append Record<br>Erase Record<br>Delete Record<br>Read Record<br>Search Record<br>Update Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(MRPIN.GDD) AND flagTI.40]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(MRPIN.GDD) AND (C.1.2.3.4.10)] OR [PWD(PIN.CH) AND C.1.10])* | siehe Hinweis 54: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.4.13 Anwendung Organspendeerklärung (DF.OSE)

Diese Anwendung enthält die Daten zur Organspendeerklärung.

**Card-G2-A_3233-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.OSE**
DF.OSE MUSS die in Tab_eGK_ObjSys_184 dargestellten initialisierten Attribute besitzen.

**Tabelle 62: Tab_eGK_ObjSys_184 Initialisierte Attribute von MF / DF.HCA / DF.OSE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | 'D276 0001 440B' | |
| *fileIdentifier* | - | herstellerspezifisch |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate | ALWAYS | herstellerspezifisch |

| | | |
|---|---|---|
| | PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.OSE) AND (C.1.2.10)])*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | ist eine der beiden Varianten erlaubt |
| Deactivate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.OSE) AND (C.1.2.10)])*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Load Application | AUT_CMS | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Activate | PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.OSE) AND (C.1.2.10)])*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER<br>PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: OR [PWD(MRPIN.OSE) AND (C.1.2.10)])*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | Herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Activate | ALWAYS<br>AUT_PACE<br>AND { [PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*((informativ: OR [PWD(MRPIN.OSE) AND (C.1.2.10)])*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Deactivate | AUT_PACE<br>AND { [PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33] } | |

| | | |
|---|---|---|
| | *(informativ: OR [PWD(MRPIN.OSE) AND (C.1.2.10)])*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Activate | AUT_PACE<br>AND { [PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER<br>---<br>AUT_PACE<br>AND { [PWD(MRPIN.home)<br>OR [PWD(MRPIN.OSE) AND flagTI.44]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 55: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 56: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.13 relevant.*

*Hinweis 57: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.*

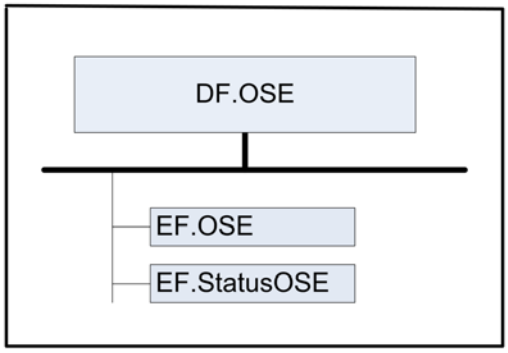



**Abbildung 6: Abb_eGK_ObjSys_010 Dateistruktur der Anwendung Organspendeerklärung**

### 5.4.13.1 MF / DF.HCA / DF.OSE / EF.OSE

Diese Datei enthält einen Datensatz zur Organspendeerklärung.

**Card-G2-A_3234-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.OSE**

EF.OSE MUSS die in Tab_eGK_ObjSys_185 dargestellten initialisierten Attribute besitzen.

**Tabelle 63: Tab_eGK_ObjSys_185 Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.OSE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘E0 01’ | |
| *shortFileIdentifier* | ‘01’= 01 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | ‘1B 58’ Oktett = 7000 Oktett | |
| *positionLogicalEndOfFile* | ‘1B 58’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | ‘00…00’ | |

| | | |
|---|---|---|
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | flagTI.42<br>OR [PWD(MRPIN.OSE) AND flagTI.41]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)]<br>*(informativ: C.2*<br>*OR [PWD(MRPIN.OSE) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)]*<br>*OR PWD(MRPIN.home))* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '81 00')<br>Update Binary<br>Write Binary | [PWD(MRPIN.OSE) AND flagTI.43]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ: [PWD(MRPIN.OSE) AND C.1.2.10]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| Alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { flagTI. 42<br>OR [PWD(MRPIN.OSE) AND flagTI.41]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home] }<br>*(informativ: C.2*<br>*OR [PWD(MRPIN.OSE) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)]*<br>*OR PWD(MRPIN.home))* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '81 00')<br>Update Binary<br>Write Binary | AUT_PACE<br>AND { [PWD(MRPIN.OSE) AND flagTI. 43]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ: [PWD(MRPIN.OSE) AND C.1.2.10]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |

| | | |
|---|---|---|
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 58: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

### 5.4.13.2 MF / DF.HCA / DF.OSE / EF.StatusOSE

Diese Datei enthält die Information über den Status der Organspendeerklärung.

**Card-G2-A_3235-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.StatusOSE**

EF.StatusOSE MUSS die in Tab_eGK_ObjSys_186 dargestellten initialisierten Attribute besitzen.

**Tabelle 64: Tab_eGK_ObjSys_186 Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.StatusOSE**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'E0 02' | |
| *shortFileIdentifier* | '02'= 02 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | '0019' Oktett = 25 Oktett | |
| *positionLogicalEndOfFile* | '0019' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |

| | | |
|---|---|---|
| *body* | '00…00' | |
| **Zugriffsregeln für die Kontaktschnittstelle** | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | flagTI.42<br>OR [PWD((MRPIN.OSE) AND flagTI.41]<br>OR [PWD((PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)<br>*(informativ: C.2*<br>*OR [PWD(MRPIN.OSE) AND (C.1.10)]*<br>*OR [PWD(PIN.CH) AND (C.1.10)]*<br>*OR PWD(MRPIN.home))* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '82 00')<br>Update Binary<br>Write Binary | [PWD(MRPIN.OSE) AND flagTI.43]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>*(informativ:*<br>*[PWD(MRPIN.OSE) AND C.1.2.10]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { flagTI. 42<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)]}<br>*(informativ: C.2*<br>*OR [PWD(PIN.CH) AND (C.1.10)]*<br>*OR PWD(MRPIN.home))* | |
| Erase Binary<br>Set Logical EOF<br>(P1P2 = '82 00')<br>Update Binary<br>Write Binary | AUT_PACE<br>AND { [PWD(MRPIN.OSE) AND flagTI. 43]<br>OR [PWD(PIN.CH) AND flagTI.33] }<br>*(informativ:*<br>*[PWD(MRPIN.OSE) AND C.1.2.10]*<br>*OR [PWD(PIN.CH) AND (C.1.10)])* | |

| | | |
|---|---|---|
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |

**[<=]**

### 5.4.14 Anwendung AMTS Datenmanagement (DF.AMTS)

Diese Anwendung enthält die Daten zum AMTS-Datenmanagement.und ist mit den im Folgenden beschriebenen Objekten angelegt.

**Card-G2-A_3240-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS**
DF.AMTS MUSS die in Tab_eGK_ObjSys_189 dargestellten initialisierten Attribute besitzen.

**Tabelle 65: Tab_eGK_ObjSys_189 Initialisierte Attribute von MF / DF.HCA / DF.AMTS**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | ´D276 0001 440C´ | |
| *fileIdentifier* | - | herstellerspezifisch |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | [PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Deactivate | [PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Load Application | AUT_CMS | |

| | | |
|---|---|---|
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Activate | [PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER<br>---<br>[PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home)<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | Herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Activate | ALWAYS<br>---<br>AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home) }<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| Deactivate | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home) }<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Activate | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.45] | |

| | | |
|---|---|---|
| | OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home) }<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.45]<br>OR [PWD(PIN.CH) AND flagTI.33]<br>OR PWD(MRPIN.home) }<br>*(informativ: OR [PWD(MRPIN.AMTS) AND (C.1.10)] OR [PWD(PIN.CH) AND (C.1.10)])* | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

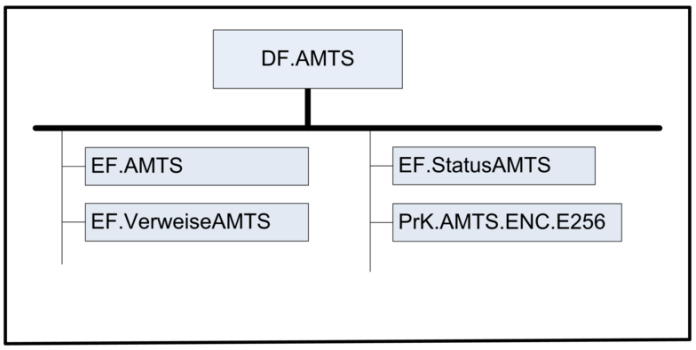



**Abbildung 7: Abb_eGK_ObjSys_011 Dateistruktur der Anwendung AMTS-Datenmanagement**

#### 5.4.14.1 MF / DF.HCA / DF.AMTS / EF.AMTS

Diese Datei enthält einen Datensatz zum AMTS Datenmanagement.

**Card-G2-A_3244-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.AMTS**

EF.AMTS MUSS die in Tab_eGK_ObjSys_191 dargestellten initialisierten Attribute besitzen.

**Tabelle 66: Tab_eGK_ObjSys_191 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.AMTS**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |

| | | |
|---|---|---|
| *fileIdentifier* | ´E0 05´ | |
| *shortFileIdentifier* | ´05´ = 05 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | False | |
| *flagChecksum* | True | |
| *numberOfOctet* | ´35 C7´ Oktett = 13767 Oktett | |
| *positionLogicalEndOfFile* | ´35 C7´ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | ’00…00’ | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | [PWD(MRPIN.AMTS AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP**)** AND flagTI.46]<br>OR [PWD(PIN.CH**)** AND (flagTI.46<br>AND flagTI.33)]<br>*informativ: [PWD(MRPIN.AMTS) AND C.2.3.4.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | Siehe Hinweis 59: |
| Erase Binary<br>Update Binary<br>Set Logical EOF (P1P2 = ’85 00’)<br>Write Binary | [PWD(MRPIN.AMTS) AND flagTI.47]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.47]<br>OR [PWD(PIN.CH**)** AND (flagTI.47<br>AND flagTI.33)]<br>*informativ: [PWD(MRPIN.AMTS) AND C.2.3.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | Siehe Hinweis 59:<br>Siehe Hinweis 60: |
| Andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Alle | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { [PWD(MRPIN.AMTS**)** AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP**)** AND flagTI.46]<br>OR [PWD(PIN.CH**)** AND (flagTI.46<br>AND flagTI.33)] }<br>*informativ: [PWD(MRPIN.AMTS) AND C.2.3.4.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | Siehe Hinweis 59: |
| Erase Binary<br>Update Binary<br>Set Logical EOF<br>(P1P2 = ’85 00’)<br>Write Binary | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.47]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.47]<br>OR [PWD(PIN.CH**)** AND (flagTI.47<br>AND flagTI.33)] }<br>*informativ: [PWD(MRPIN.AMTS) AND C.2.3.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | Siehe Hinweis 59:<br>Siehe Hinweis 60: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 59: Profil.10 kennzeichnet die Rolle zu „Anwendungen des Versicherten“ (LE-AdV) im Kontrollbereich eines Leistungserbringers, die zum Zugriff auf die AMTS-Daten berechtigt ist.*

*Hinweis 60: Das Lösch- und Schreibrecht mit Profil.10 ist beschränkt auf das Löschen der Daten sowie das Wiederherstellen der Daten aus einem Backup. Diese Beschränkung ist außerhalb der eGK durchzusetzen.*

### 5.4.14.2 MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS

Diese Datei enthält die Informationen über die Speicherorte der Daten der freiwilligen Anwendung AMTS Datenmanagement, die nicht auf der eGK gespeichert werden.

**Card-G2-A_3245-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS**
EF.VerweiseAMTS MUSS die in Tab_eGK_ObjSys_192 dargestellten initialisierten Attribute besitzen.

**Tabelle 67: Tab_eGK_ObjSys_192 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | linear variables Elementary File | |
| *fileIdentifier* | ´E0 06´ | |
| *shortFileIdentifier* | ´06´ = 06 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | ´0258´ Oktett = 600 Oktett | |
| *maxNumRecords* | 5 Record | |
| *maxRecordLength* | 120 Oktett | |
| *flagRecordLCS* | False | |
| *recordList* | alle Records aktiviert, fünf Records vorhanden, Inhalt jedes Records: ‘00’ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Read Record<br>Search Record | PWD(MRPIN.home)<br>OR [PWD(MRPIN.AMTS) AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.46]<br>OR [PWD(PIN.CH) AND (flagTI.46 AND flagTI.33)]<br>*(informativ: PWD(MRPIN.home OR [PWD(MRPIN.AMTS) AND C.2.3.4.10]* | |

| | | |
|---|---|---|
| | *OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Append Record<br>Erase Record<br>Delete Record<br>Update Record | [PWD(MRPIN.AMTS) AND flagTI.47]<br>OR [PWD(PIN.CH) AND (flagTI.47 AND flagTI.33)]<br>*(informativ: [PWD(MRPIN.AMTS) AND C.2.3.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Record<br>Search Record | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(MRPIN.AMTS) AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.46]<br>OR [PWD(PIN.CH) AND (flagTI.46 AND flagTI.33)] }<br>*(informativ: PWD(MRPIN.home*<br>*OR [PWD(MRPIN.AMTS) AND C.2.3.4.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Append Record<br>Erase Record<br>Delete Record<br>Update Record | AUT_PACE<br>AND {<br>[PWD(MRPIN.AMTS) AND flagTI.47]<br>OR [PWD(PIN.CH) AND (flagTI.47 AND flagTI.33)] }<br>(informativ: *[PWD(MRPIN.AMTS) AND C.2.3.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

### 5.4.14.3 MF / DF.HCA / DF.AMTS / EF.StatusAMTS

Diese Datei enthält die Information über den Status der Anwendung AMTS Datenmanagement.

**Card-G2-A_3246-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.StatusAMTS**
EF.StatusAMTS MUSS die in Tab_eGK_ObjSys_193 dargestellten initialisierten Attribute besitzen.

**Tabelle 68: Tab_eGK_ObjSys_193 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.StatusAMTS**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ´E0 07´ | |
| *shortFileIdentifier* | ´07´ = 07 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | True | |
| *numberOfOctet* | ´0019´ Oktett = 25 Oktett | |
| *positionLogicalEndOfFile* | ´0019´ | Auf diese Weise soll ausgeschlossen werden, dass der eGK bereits vor der PIN Eingabe anzusehen ist, ob AMTS genutzt wird |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | ’00…00’ | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete | AUT_CMS | |
| Read Binary | [PWD(MRPIN.AMTS) AND flagTI.46] | |

| | | |
|---|---|---|
| | OR [PWD(PIN.AMTS_REP) AND flagTI.46]<br>OR [PWD(PIN.CH) AND (flagTI.46 AND flagTI.33)]<br>*informativ: PWD(MRPIN.home*<br>*OR [PWD(MRPIN.AMTS) AND C.2.3.4.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Update Binary | [PWD(MRPIN.AMTS) AND flagTI.47]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.47]<br>OR [PWD(PIN.CH) AND (flagTI.47 AND flagTI.33)]<br>*informativ: PWD(MRPIN.home*<br>*OR [PWD(MRPIN.AMTS) AND C.2.3.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | Herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete | AUT_CMS | |
| Read Binary | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.46]<br>OR [PWD(PIN.CH) AND (flagTI.46 AND flagTI.33)] }<br>*informativ: PWD(MRPIN.home*<br>*OR [PWD(MRPIN.AMTS) AND C.2.3.4.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Update Binary | AUT_PACE<br>AND<br>{ [PWD(MRPIN.AMTS) AND flagTI.47]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.47]<br>OR [PWD(PIN.CH) AND (flagTI.47 AND flagTI.33)] }<br>*informativ: PWD(MRPIN.home*<br>*OR [PWD(MRPIN.AMTS) AND C.2.3.4.10]*<br>*OR [PWD(PIN.AMTS_REP) AND C.2.3.4.10]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| andere | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | NEVER | |

**[<=]**

### 5.4.14.4 MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256

PrK.AMTS.ENC.E256 ist der private Schlüssel des Versicherten auf Basis elliptischer Kurven in der Fachanwendung AMTS.

**Card-G2-A_3263-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256**

PrK.AMTS.ENC.E256 MUSS die in Tab_eGK_ObjSys_197 dargestellten Werte besitzen.

**Tabelle 69: Tab_eGK_ObjSys_197 Initialisierte Attribute von MF /DF.HCA / DF.AMTS PrK.AMTS.ENC.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates ELC Schlüsselobjekt, ELC256 | |
| *keyIdentifier* | ´08´ = 8 | |
| *privateElcKey* | domainparameter = brainpoolP256r1 | |
| *privateElcKey* | d = *wird personalisiert* | |
| *keyAvailable* | Wildcard | |
| *listAlgorithmIdentifier* | elcSharedSecretCalculation | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Decipher<br>PSO Transcipher | [PWD(MRPIN.AMTS) AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.46]<br>OR [PWD(PIN.CH**)** AND (flagTI.46 AND flagTI.33)]<br>*informativ: [PWD(MRPIN.AMTS) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.AMTS_REP) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Generate Asymmetric Key Pair mit P1 = ´81´ | [PWD(MRPIN.AMTS) AND (flagTI.46 OR flagTI.47)]<br>OR [PWD(PIN.AMTS_REP) AND (flagTI.46<br>OR flagTI.47)]<br>OR [PWD(PIN.CH**)** AND (flagTI.46 OR flagTI.47) | |

| | | |
|---|---|---|
| | AND flagTI.33]<br>*informativ: [PWD(MRPIN.AMTS) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.AMTS_REP) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Generate Asymmetric Key Pair mit P1 = ´C0´ | PWD(MRPIN.AMTS) AND flagTI.47<br>OR [PWD(PIN.CH**)** AND flagTI.47 AND flagTI.33]<br>*informativ: [PWD(MRPIN.AMTS) AND (C.2.3.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| 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 | NEVER | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Decipher<br>PSO Transcipher | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND flagTI.46]<br>OR [PWD(PIN.AMTS_REP) AND flagTI.46]<br>OR [PWD(PIN.CH**)** AND (flagTI.46 AND flagTI.33)] }<br>*informativ: [PWD(MRPIN.AMTS) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.AMTS_REP) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Generate Asymmetric Key Pair mit P1 = ´81´ | AUT_PACE<br>AND { [PWD(MRPIN.AMTS) AND (flagTI.46 OR flagTI.47)]<br>OR [PWD(PIN.AMTS_REP) AND (flagTI.46 OR flagTI.47)]<br>OR [PWD(PIN.CH**)** AND (flagTI.46 OR flagTI.47) AND flagTI.33] }<br>*informativ: [PWD(MRPIN.AMTS) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.AMTS_REP) AND (C.2.3.4.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)])* | |
| Generate Asymmetric Key Pair mit P1 = ´C0´ | AUT_PACE<br>AND { PWD(MRPIN.AMTS) AND flagTI.47<br>OR [PWD(PIN.CH**)** AND (flagTI.47 AND flagTI.33)] }<br>*informativ: [PWD(MRPIN.AMTS) AND (C.2.3.10)]*<br>*OR [PWD(PIN.CH) AND (C.10)]* | |
| 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 | NEVER | |

**[<=]**

**Card-G2-A_3264-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256**
Bei der Personalisierung von PrK.AMTS.ENC.E256 MÜSSEN die in Tab_eGK_ObjSys_198 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 70: Tab_eGK_ObjSys_198 Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *privateKey.d* | wird personalisiert | wird bei der ersten Nutzung von AMTS mit Generate Asymmetric Key Pair überschrieben |
| *keyAvailable* | true | |

**[<=]**

## 5.5 DF.ESIGN (Krypto-Anwendung ESIGN)

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

- die Client/Server-Authentisierung,
- die pseudonymisierte Client/Server-Authentisierung und Nachrichtensignatur,
- die Schlüssel-Chiffrierungsfunktion für die kryptographische Sicherung von Daten und
- die Schlüssel-Chiffrierungsfunktion im Kontext elektronischer Verordnungen.

**Card-G2-A_2420 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN**
DF.ESIGN MUSS die in Tab_eGK_ObjSys_059 dargestellten initialisierten Attribute besitzen.

**Tabelle 71: Tab_eGK_ObjSys_059 Initialisierte Attribute von MF / DF.ESIGN**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | 'A000000167 455349474E' | siehe Hinweis 61: |
| *fileIdentifier* | – | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Load Application | AUT_CMS | |
| Get Random | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Load Application | AUT_CMS | |
| Get Random | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 61: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 62: Der Wert des Attributes applicationIdentifier ist in [EN14890–1] festgelegt.*

*Hinweis 63: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren oder terminieren lassen, sind diese Zustände für Objekte in 5.5 im Allgemeinen irrelevant.*

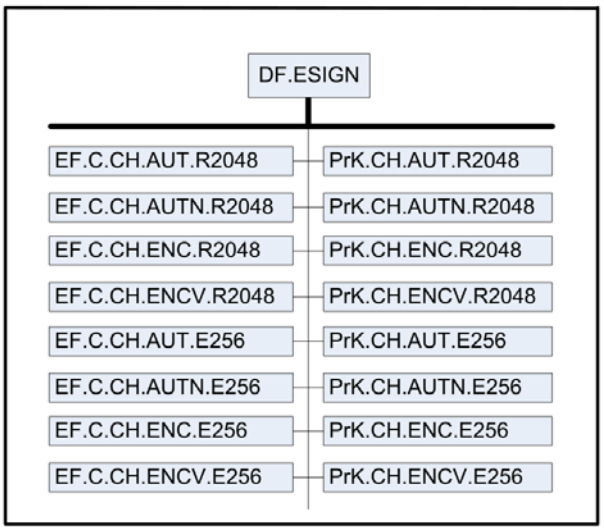



**Abbildung 8: Abb_eGK_ObjSys_006 Objektstruktur der Anwendung DF.ESIGN**

### 5.5.1 MF / DF.ESIGN / EF.C.CH.AUT.R2048

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.AUT.R2048 zu PrK.CH.AUT.R2048 (siehe 5.5.5).

**Card-G2-A_2421-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048**
EF.C.CH.AUT.R2048 MUSS die in Tab_eGK_ObjSys_060 dargestellten initialisierten Attribute besitzen.

**Tabelle 72: Tab_eGK_ObjSys_060 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘C5 00’ | |
| *shortFileIdentifier* | ‘01’= 1 | |

| | | |
|---|---|---|
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_CMS | |
| andere | NEVER | |

| | | |
|---|---|---|
| | | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 64: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

**Card-G2-A_3217-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048**
Bei der Personalisierung von EF.C.CH.AUT.R2048 MÜSSEN die in Tab_eGK_ObjSys_146 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 73: Tab_eGK_ObjSys_146 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *body* | C.CH.AUT.R2048 gemäß [gemSpec_PKI#5.1.3.1] passend zu dem privaten Schlüssel in PrK.CH.AUT.R2048 | |

**[<=]**

### 5.5.2 MF / DF.ESIGN / EF.C.CH.AUTN.R2048

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.AUTN.R2048 zu PrK.CH.AUTN.R2048 (siehe 5.5.6).

**Card-G2-A_2424-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048**
EF.C.CH.AUTN.R2048 MUSS die in Tab_eGK_ObjSys_061 dargestellten initialisierten Attribute besitzen.

**Tabelle 74: Tab_eGK_ObjSys_061 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'C5 09' | |

| | | |
|---|---|---|
| *shortFileIdentifier* | '09'= 9 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | *'07* 6C' Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | '0' | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)] OR C.2.3.4.5.8.9)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete<br>Erase Binary<br>Set Logical EOF | AUT_CMS | |

| | | |
|---|---|---|
| Update Binary<br>Write Binary | | |
| Read Binary | ( AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9 })<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)] OR C.2.3.4.5.8.9)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 65: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

**Card-G2-A_3218 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048**
Bei der Personalisierung von EF.C.CH.AUTN.R2048 MÜSSEN die in Tab_eGK_ObjSys_148 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 75: Tab_eGK_ObjSys_148 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| | | |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *Body* | C.CH.AUTN.R2048 gemäß [gemSpec_PKI#5.1.3.4] passend zu dem privaten Schlüssel in PrK.CH.AUTN.R2048 | |

**[<=]**

### 5.5.3 MF / DF.ESIGN / EF.C.CH.ENC.R2048

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.ENC.R2048 zu PrK.CH.ENC.R2048 (siehe 5.5.7).

**Card-G2-A_2427-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048**
EF.C.CH.ENC.R2048 MUSS die in Tab_eGK_ObjSys_062 dargestellten initialisierten Attribute besitzen.

**Tabelle 76: Tab_eGK_ObjSys_062 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'C2 00' | |
| *shortFileIdentifier* | '02'= 2 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | '07 6C' Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | '0' | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| 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 „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Binary | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 66: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

**Card-G2-A_3219 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048**
Bei der Personalisierung von EF.C.CH.ENC.R2048 MÜSSEN die in Tab_eGK_ObjSys_150 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 77: Tab_eGK_ObjSys_150 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *body* | C.CH.ENC.R2048 gemäß [gemSpec_PKI#5.1.3.2] passend zu dem privaten Schlüssel in PrK.CH.ENC.R2048 | |

**[<=]**

### 5.5.4 MF / DF.ESIGN / EF.C.CH.ENCV.R2048

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.ENCV.R2048 zu PrK.CH.ENCV.R2048 (siehe 5.5.8).

**Card-G2-A_2434-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048**
EF.C.CH.ENCV.R2048 MUSS die in Tab_eGK_ObjSys_063 dargestellten initialisierten Attribute besitzen.

**Tabelle 78: Tab_eGK_ObjSys_063 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘C5 0A’ | |
| *shortFileIdentifier* | ‘0A’= 10 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | ( AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11 })<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 67: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

**Card-G2-A_3220 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048**

Bei der Personalisierung von EF.C.CH.ENCV.R2048 MÜSSEN die in Tab_eGK_ObjSys_154 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 79: Tab_eGK_ObjSys_154 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *Body* | C.CH.ENCV.R2048 gemäß [gemSpec_PKI#5.1.3.5] passend zu dem privaten Schlüssel in PrK.CH.ENCV.R2048 | |

**[<=]**

### 5.5.5 MF / DF.ESIGN / PrK.CH.AUT.R2048

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit RSA befindet sich in EF.C.CH.AUT.R2048, siehe 5.5.1.

**Card-G2-A_2437-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048**
PrK.CH.AUT.R2048 MUSS die in Tab_eGK_ObjSys_064 dargestellten initialisierten Attribute besitzen.

**Tabelle 80: Tab_eGK_ObjSys_064 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, RSA 2048 | |
| *keyIdentifier* | '02' = 2 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *privateKey* | herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, [gemSpec_COS] {rsaClientAuthentication, signPKCS1_V1_5, signPSS} | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Internal Authenticate<br>PSO Comp Digital Sig. | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.12]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.9.10)])* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Internal Authenticate<br>PSO Comp Digital Sig. | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.12] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.9.10)])* | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 68: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.*

**Card-G2-A_3221 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048**

Bei der Personalisierung von PrK.CH.AUT.R2048 MÜSSEN die in Tab_eGK_ObjSys_156 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 81: Tab_eGK_ObjSys_156 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *privateKey* | Schlüssel mit Moduluslänge 2048 Bit | |
| *keyAvailable* | True | |

**[<=]**

### 5.5.6 MF / DF.ESIGN / PrK.CH.AUTN.R2048

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit RSA befindet sich in EF.C.CH.AUTN.R2048, siehe 5.5.2.

**Card-G2-A_2440-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048**
PrK.CH.AUTN.R2048 MUSS die in Tab_eGK_ObjSys_067 dargestellten initialisierten Attribute besitzen.

**Tabelle 82: Tab_eGK_ObjSys_067 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, RSA 2048 | |
| *keyIdentifier* | '06' = 6 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *privateKey* | herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, [gemSpec_COS] {rsaClientAuthentication, signPSS} | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Internal Authenticate<br>PSO Comp Digital Sig. | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)] OR C.2.3.4.5.8.9)* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Internal Authenticate<br>PSO Comp Digital Sig. | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9 }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)]<br>OR C.2.3.4.5.8.9)* | |
| Generate Asymmetric Key Pair<br>P1=‘81’ | AUT_PACE | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 69: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.*

**Card-G2-A_3222 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048**

Bei der Personalisierung von PrK.CH.AUTN.R2048 MÜSSEN die in Tab_eGK_ObjSys_159 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 83: Tab_eGK_ObjSys_159 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048**

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

**[<=]**

### 5.5.7 MF / DF.ESIGN / PrK.CH.ENC.R2048

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit RSA befindet sich in EF.C.CH.ENC.R2048, siehe 5.5.3.

**Card-G2-A_2443-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048**
PrK.CH.ENC.R2048 MUSS die in Tab_eGK_ObjSys_070 dargestellten initialisierten Attribute besitzen.

**Tabelle 84: Tab_eGK_ObjSys_070 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, RSA 2048 | |
| *keyIdentifier* | '03' = 3 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *privateKey* | herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, [gemSpec_COS] {rsaDecipherOaep} | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| PSO Decipher<br>PSO Transcipher | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.13]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.10)])* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| | | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Decipher<br>PSO Transcipher | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.13] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.10)])* | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 70: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.*

**Card-G2-A_3223 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048**

Bei der Personalisierung von PrK.CH.ENC.R2048 MÜSSEN die in Tab_eGK_ObjSys_162 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 85: Tab_eGK_ObjSys_162 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048**

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

**[<=]**

### 5.5.8 MF / DF.ESIGN / PrK.CH.ENCV.R2048

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptografie mit RSA befindet sich in EF.C.CH.ENCV.R2048, siehe 5.5.4.

**Card-G2-A_2449-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048**
PrK.CH.ENCV.R2048 MUSS die in Tab_eGK_ObjSys_076 dargestellten initialisierten Attribute besitzen.

**Tabelle 86: Tab_eGK_ObjSys_076 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, RSA 2048 | |
| *keyIdentifier* | '07' = 7 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *privateKey* | herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, [gemSpec_COS] {rsaDecipherOaep} | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| PSO Decipher<br>PSO Transcipher | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| PSO Decipher<br>PSO Transcipher | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11 }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| Generate Asymmetric Key Pair<br>P1=‘81’ | AUT_PACE | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 71: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.*

### Card-G2-A_3224 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048

Bei der Personalisierung von PrK.CH.ENCV.R2048 MÜSSEN die in Tab_eGK_ObjSys_168 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 87: Tab_eGK_ObjSys_168 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048**

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

**[<=]**

### 5.5.9 MF / DF.ESIGN / EF.C.CH.AUT.E256

Diese Datei enthält ein X.509-Authentisierungs-Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.CH.AUT.E256 zu PrK.CH.AUT.E256 (siehe 5.5.13).

**Card-G2-A_3603 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.E256**
EF.C.CH.AUT.E256 MUSS die in Tab_eGK_ObjSys_200 dargestellten initialisierten Attribute besitzen.

**Tabelle 88: Tab_eGK_ObjSys_200 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘C5 04’ | |
| *shortFileIdentifier* | ‘04’= 4 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | ALWAYS | |
| andere | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | AUT_PACE<br>OR AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3604 - K_Personalisierung: Personalisierte Attribute von von MF / DF.ESIGN / EF.C.CH.AUT.E256**
Bei der Personalisierung von EF.C.CH.AUT.E256 MÜSSEN die in Tab_eGK_ObjSys_201 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 89: Tab_eGK_ObjSys_201 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.E256**

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

**[<=]**

### 5.5.10 MF / DF.ESIGN / EF.C.CH.AUTN.E256

Diese Datei enthält ein pseudonymes X.509-Authentisierungs-Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.CH.AUTN.E256 zu PrK.CH.AUTN.256 (siehe 5.5.14).

**Card-G2-A_3605 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.E256**
EF.C.CH.AUTN.E256 MUSS die in Tab_eGK_ObjSys_202 dargestellten initialisierten Attribute besitzen.

**Tabelle 90: Tab_eGK_ObjSys_202 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'C5 0B' | |
| *shortFileIdentifier* | '0B'= 11 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | '07 6C' Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | '0' | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)]* | |

| | | |
|---|---|---|
| | *OR C.2.3.4.5.8.9)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | ( AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9 })<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)] OR C.2.3.4.5.8.9)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3606 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.E256**

Bei der Personalisierung von EF.C.CH.AUTN.E256 MÜSSEN die in Tab_eGK_ObjSys_203 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 91: Tab_eGK_ObjSys_203 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |

| | | |
|---|---|---|
| *body* | C.CH.AUTN.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.CH.AUTN. E256 | |

**[<=]**

### 5.5.11 MF / DF.ESIGN / EF.C.CH.ENC.E256

Diese Datei enthält ein Verschlüsselungs-Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.CH.ENC.E256 zu PrK.CH.ENC.E256 (siehe 5.5.15).

**Card-G2-A_3607 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.E256**
EF.C.CH.ENC.E256 MUSS die in Tab_eGK_ObjSys_204 dargestellten initialisierten Attribute besitzen.

**Tabelle 92: Tab_eGK_ObjSys_204 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘C2 05’ | |
| *shortFileIdentifier* | ‘05’= 5 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| 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 „Termination state" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Read Binary | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3608 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.E256**
Bei der Personalisierung von EF.C.CH.ENC.E256 MÜSSEN die in Tab_eGK_ObjSys_205 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 93: Tab_eGK_ObjSys_205 Personalisierte Attribute von MF / DF.ESIGN/ EF.C.CH.ENC.E256**

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

**[<=]**

## 5.5.12 MF / DF.ESIGN / EF.C.CH.ENCV.E256

Diese Datei enthält ein Verschlüsselungs-Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.CH.ENCV.E256 zu PrK.CH.ENCV.E256 (siehe 5.5.16).

**Card-G2-A_3609 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.E256**
EF.C.CH.ENCV.E256 MUSS die in Tab_eGK_ObjSys_206 dargestellten initialisierten Attribute besitzen.

**Tabelle 94: Tab_eGK_ObjSys_206 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | 'C5 0C' | |
| *shortFileIdentifier* | '0C'= 12 | |
| *lifeCycleStatus* | „Operational state (activated)" | |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *numberOfOctet* | '07 6C' Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | '0' | wird personalisiert |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| *body* | kein Inhalt | wird personalisiert |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete<br>Erase Binary<br>Set Logical EOF<br>Update Binary<br>Write Binary | AUT_CMS | |
| Read Binary | ( AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11 })<br>OR AUT_CMS<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3610 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.E256**
Bei der Personalisierung von EF.C.CH.ENCV.E256 MÜSSEN die in Tab_eGK_ObjSys_207 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 95: Tab_eGK_ObjSys_207 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *body* | C.CH.ENCV.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.CH.ENCV.E256 | |

**[<=]**

### 5.5.13 MF / DF.ESIGN / PrK.CH.AUT.E256

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit elliptischen Kurven befindet sich in EF.C.CH.AUT.E256, siehe 5.5.9.

**Card-G2-A_3611-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.E256**
PrK.CH.AUT.E256 MUSS die in Tab_eGK_ObjSys_208 dargestellten initialisierten Attribute besitzen.

**Tabelle 96: Tab_eGK_ObjSys_208 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, ELC 256 | |
| *keyIdentifier* | '04' = 4 | |
| *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 | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| PSO Comp Digital Sig. | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.12]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.9.10)])* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| PSO Comp Digital Sig. | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.12] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.9.10)])* | |
| Generate Asymmetric Key Pair<br>P1=‘81’ | AUT_PACE | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3612 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.E256**

Bei der Personalisierung von PrK.CH.AUT.E256 MÜSSEN die in Tab_eGK_ObjSys_209 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 97: Tab_eGK_ObjSys_209 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.E256**

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

**[<=]**

## 5.5.14 MF / DF.ESIGN / PrK.CH.AUTN. E256

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit elliptischen Kurven befindet sich in EF.C.CH.AUTN.E256, siehe 5.5.10.

**Card-G2-A_3613-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN. E256**
PrK.CH.AUTN. E256 MUSS die in Tab_eGK_ObjSys_210 dargestellten initialisierten Attribute besitzen.

**Tabelle 98: Tab_eGK_ObjSys_210 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN. E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, ELC 256 | |
| *keyIdentifier* | '0B' = 11 | |
| *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 | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| PSO Comp Digital Sig. | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)] OR C.2.3.4.5.8.9)* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| PSO Comp Digital Sig. | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.8]<br>OR flagTI.9 }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.10)] OR C.2.3.4.5.8.9)* | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3614 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN. E256**
Bei der Personalisierung von PrK.CH.AUTN. E256 MÜSSEN die in Tab_eGK_ObjSys_211 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 99: Tab_eGK_ObjSys_211 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN. E256**

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

**[<=]**

### 5.5.15 MF / DF.ESIGN / PrK.CH.ENC.E256

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit elliptischen Kurven befindet sich in EF.C.CH.ENC.E256, siehe 5.5.11.

**Card-G2-A_3615-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.E256**
PrK.CH.ENC.E256 MUSS die in Tab_eGK_ObjSys_212 dargestellten initialisierten Attribute besitzen.

**Tabelle 100: Tab_eGK_ObjSys_212 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.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 | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| PSO Decipher<br>PSO Transcipher | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.13]<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.10)])* | |
| Generate Asymmetric Key Pair<br>P1=‘81’ | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | |
| PSO Decipher<br>PSO Transcipher | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.13] }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.10)])* | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3616 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.E256**
Bei der Personalisierung von PrK.CH.ENC.E256 MÜSSEN die in Tab_eGK_ObjSys_213 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 101: Tab_eGK_ObjSys_213 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.E256**

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

**[<=]**

## 5.5.16 MF / DF.ESIGN / PrK.CH.ENCV.E256

Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit elliptischen Kurven befindet sich in EF.C.CH.ENCV.E256, siehe 5.5.12.

**Card-G2-A_3617-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.E256**
PrK.CH.ENCV.E256 MUSS die in Tab_eGK_ObjSys_214 dargestellten initialisierten Attribute besitzen.

**Tabelle 102: Tab_eGK_ObjSys_214 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates Schlüsselobjekt, ELC 256 | |
| *keyIdentifier* | '0C' = 12 | |
| *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 | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| PSO Decipher<br>PSO Transcipher | PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |

| | | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| PSO Decipher<br>PSO Transcipher | AUT_PACE<br>AND { PWD(MRPIN.home)<br>OR [PWD(PIN.CH) AND flagTI.10]<br>OR flagTI.11 }<br>*(informativ: OR [PWD(PIN.CH) AND (C.1.9.10)] OR C.2.3.5)* | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3618 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.E256**
Bei der Personalisierung von PrK.CH.ENCV.E256 MÜSSEN die in Tab_eGK_ObjSys_215 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 103: Tab_eGK_ObjSys_215 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.E256**

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

**[<=]**

# 6 Qualifizierte elektronische Signatur

Im Hinblick auf den Zustand der QES-Anwendung bei eGK-Ausgabe sind zwei Varianten zu unterscheiden:

- Es gibt kein DF.QES. Damit ist dieses Kapitel nicht relevant. Es ist möglich, eine entsprechende Anwendung mittels LOAD APPLICATION (siehe [gemSpec_COS]) nachzuladen. Entsprechende Rechte sind derzeit in der Anwendung *root* (siehe Tab_eGK_ObjSys_006 Initialisierte Attribute von MF) vorhanden. Bei diesem Nachladen ist es vom technischen Standpunkt aus möglich, jeden der im Folgenden genannten Punkte zu erreichen. Ob dies aus sicherheitstechnischen Aspekten möglich ist, ist nicht Gegenstand dieses Dokumentes.
- Die QES-Anwendung ist komplett angelegt und sofort nutzbar. Dieser Zustand wird in 6.1 beschrieben. PrK.CH.QES (siehe Tab_eGK_ObjSys _087) ist nutzbar und EF.C.CH.QES (siehe Tab_eGK_ObjSys _085) enthält ein Zertifikat.

**Card-G2-A_3202 - K_Initialisierung: Option QES**
Falls die Option QES für die eGK umgesetzt wird, MÜSSEN alle Anforderungen aus Kapitel 6.1erfüllt werden.
**[<=]**

## 6.1 DF.QES (QES-Anwendung komplett angelegt und nutzbar)

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

**Card-G2-A_2459 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES**
DF.QES MUSS die in Tab_eGK_ObjSys_086 dargestellten initialisierten Attribute besitzen.

**Tabelle 104: Tab_eGK_ObjSys_086 Initialisierte Attribute von MF / DF.QES**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Ordner | |
| *applicationIdentifier* | ‘D276000066 01’ | siehe Hinweis 78: |
| *fileIdentifier* | – | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *shareable* | True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch | |
| Zugriffsregeln für die Kontaktschnittstelle | | |

| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Load Application | herstellerspezifisch | sieheHinweis 79: |
| 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** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Load Application | herstellerspezifisch | sieheHinweis 79: |
| Get Random | AUT_PACE | |
| 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 | |

**[<=]**

*Hinweis 72: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.*

*Hinweis 73: Der Wert des Attributes applicationIdentifier ist in [DIN66291-4] festgelegt.*

*Hinweis 74: 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.*

*Hinweis 75: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im 6.1 nicht berücksichtigt werden.*

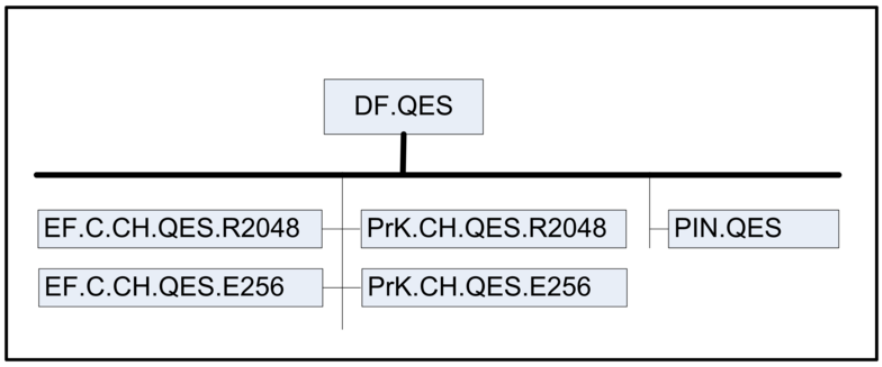



**Abbildung 9: Abb_eGK_ObjSys_009 Objektstruktur der vollständigen Signaturanwendung DF.QES**

### 6.1.1 MF / DF.QES / EF.C.CH.QES.R2048

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.QES.R2048 zu PrK.CH.QES.R2048 (siehe 6.1.3).

**Card-G2-A_2460-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048**
EF.C.CH.QES.R2048 MUSS die in Tab_eGK_ObjSys_087 dargestellten initialisierten Attribute besitzen.

**Tabelle 105: Tab_eGK_ObjSys_087 Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘C0 00’ | siehe Hinweis 78: |
| *shortFileIdentifier* | ‘10’= 16 | |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *lifeCycleStatus* | „Operational state (activated)“ | |

| | | |
|---|---|---|
| *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 | herstellerspezifisch | sieheHinweis 76: |
| Read Binary | ALWAYS | |
| Update Binary | herstellerspezifisch | sieheHinweis 76: |
| 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 | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | herstellerspezifisch | sieheHinweis 76: |
| Read Binary | AUT_PACE | |
| Update Binary | herstellerspezifisch | sieheHinweis 76: |
| 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 | |

**[<=]**

*Hinweis 76: 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.*

*Hinweis 77: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.*

*Hinweis 78: Der Wert des Attributes fileIdentifier ist in [DIN66291-4] festgelegt.*

**Card-G2-A_3225 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048**
Bei der Personalisierung von EF.C.CH.QES.R2048 MÜSSEN die in Tab_eGK_ObjSys_175 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 106: Tab_eGK_ObjSys_175 Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogical EndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *body* | C.CH.QES.R2048 gemäß [gemSpec_PKI#5.1.3.3] passend zu dem privaten Schlüssel in PrK.CH.QES | |

**[<=]**

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

Dieses Benutzergeheimnis wird zur Freischaltung der Signaturfunktionalität mit dem Schlüssel PrK.CH.QES (siehe Kapitel 6.1.3) benötigt.

**Card-G2-A_2463-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PIN.QES**
PIN.QES MUSS die in Tab_eGK_ObjSys_088 dargestellten initialisierten Attribute besitzen.

**Tabelle 107: Tab_eGK_ObjSys_088 Initialisierte Attribute von MF / DF.QES / PIN.QES**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | Reguläres Passwortobjekt | |
| *pwdIdentifier* | ‘01’ = 1 | |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 6 | |

| | | |
|---|---|---|
| *maximumLength* | 8 | |
| *startRetryCounter* | 3 | |
| *retryCounter* | 3 | |
| *transportStatus* | Transport-PIN | wird personalisiert |
| *flagEnabled* | True | |
| *startSsec* | 1 | |
| *PUK* | … | wird personalisiert |
| *pukUsage* | 10 | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | ALWAYS | |
| Get Pin Status | ALWAYS | |
| Reset RC. P1 = 1 | ALWAYS | |
| Verify | ALWAYS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |

| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet | | |
|---|---|---|
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | AUT_PACE | |
| Get Pin Status | AUT_PACE | |
| Reset RC. P1 = 1 | AUT_PACE | |
| Verify | AUT_PACE | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |

**[<=]**

*Hinweis 79: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.*

Hinweis 80: 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_3226 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PIN.QES**

Bei der Personalisierung von PIN.QES MÜSSEN die in Tab_eGK_ObjSys_177 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 108: Tab_eGK_ObjSys_177 Personalisierte Attribute von MF / DF.QES / PIN.QES**

| Attribute | Wert | Bemerkung |
|---|---|---|
| **secret** | PIN-Wert gemäß [gemSpec_PINPUK_TI] | Transport-PIN |
| *secretLength* | 5 Ziffern (*minimumLength* - 1) | Länge der Transport-PIN |

| | | |
|---|---|---|
| *PUK* | PUK-Wert gemäß [gemSpec_PINPUK_TI] | |
| *PUKLength* | 8 Ziffern | |

**[<=]**

### 6.1.3 MF / DF.QES / PrK.CH.QES.R2048

Dieser private Schlüssel für die Kryptographie mit RSA erstellt qualifizierte Signaturen. Der zugehörige öffentliche Teil findet sich in EF.C.CH.QES.R2048, siehe 6.1.1.

**Card-G2-A_2464-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048**
PrK.CH.QES.R2048 MUSS die in Tab_eGK_ObjSys_089 dargestellten initialisierten Attribute besitzen.

**Tabelle 109: Tab_eGK_ObjSys_089 Initialisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | privates RSA Signierobjekt | |
| *keyIdentifier* | ‘04’ = 4 | siehe Hinweis 82: |
| *privateKey* | hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | True | |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec_COS] {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 | |
| PSO Comp Dig Sig. | PWD(PIN.QES) | |
| Delete | AUT_CMS | |
| andere | NEVER | |

| | | |
|---|---|---|
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER | |
| **Zugriffsregeln für die kontaktlose Schnittstelle** | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair P1='81' | AUT_PACE | |
| PSO Comp Dig Sig. | AUT_PACE<br>AND PWD(PIN.QES) | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER | |

**[<=]**

*Hinweis 81: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.*

*Hinweis 82: Der Wert des Attributes keyIdentifier ist in [DIN66291-4] festgelegt.*

**Card-G2-A_3227 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048**
Bei der Personalisierung von PrK.CH.QES.R2048 MÜSSEN die in Tab_eGK_ObjSys_178 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 110: Tab_eGK_ObjSys_178 Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *privateKey* | Moduluslänge 2048 Bit | |

**[<=]**

## 6.1.4 MF / DF.QES / EF.C.CH.QES.E256

Diese Datei enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.CH.QES.E256 zu PrK.CH.QES.E256 (siehe 6.1.5).

**Card-G2-A_3619 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.E256**
EF.C.CH.QES.E256 MUSS die in Tab_eGK_ObjSys_216 dargestellten initialisierten Attribute besitzen.

**Tabelle 111: Tab_eGK_ObjSys_216 Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| Objekttyp | transparentes Elementary File | |
| *fileIdentifier* | ‘C0 06’ | siehe Hinweis 83: |
| *shortFileIdentifier* | ‘06’= 6 | |
| *numberOfOctet* | ‘07 6C’ Oktett = 1900 Oktett | |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *flagTransactionMode* | True | |
| *flagChecksum* | False | |
| *lifeCycleStatus* | „Operational state (activated)“ | |
| *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 | herstellerspezifisch | sieheHinweis 76: |
| Read Binary | ALWAYS | |
| Update Binary | herstellerspezifisch | sieheHinweis 76: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | |
| alle | herstellerspezifisch | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | |
| Delete | herstellerspezifisch | sieheHinweis 76: |
| Read Binary | AUT_PACE | |
| Update Binary | herstellerspezifisch | sieheHinweis 76: |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | |
| alle | herstellerspezifisch | |

**[<=]**

**Card-G2-A_3620 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.E256**
Bei der Personalisierung von EF.C.CH.QES.E256 MÜSSEN die in Tab_eGK_ObjSys_217 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 112: Tab_eGK_ObjSys_217 Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.E256**

| Attribute | Wert | Bemerkung |
|---|---|---|
| *positionLogical EndOfFile* | Zahl der tatsächlich belegten Oktette | |
| *body* | C.CH.QES.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.CH.QES.E256 | |

**[<=]**

## 6.1.5 MF / DF.QES / PrK.CH.QES.E256

Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven erstellt qualifizierte Signaturen. Der öffentliche Teil zu diesem privaten Schlüssel für die Kryptographie mit elliptischen Kurven befindet sich in EF.C.CH.QES.E256, siehe 6.1.4.

**Card-G2-A_3621 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.CH.QES.E256**
PrK.CH.QES.E256 MUSS die in Tab_eGK_ObjSys_218 dargestellten initialisierten Attribute besitzen.

**Tabelle 113: Tab_eGK_ObjSys_218 Initialisierte Attribute von MF / DF.QES / PrK.CH.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 | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair<br>P1='81' | ALWAYS | |
| PSO Comp Dig Sig | PWD(PIN.QES) | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | |
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet<br>Zugriffsart Zugriffsbedingung | | |
| alle | NEVER | |
| Zugriffsregeln für die kontaktlose Schnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)" kontaktlos<br>Zugriffsart Zugriffsbedingung | | |
| Generate Asymmetric Key Pair<br>P1='81' | AUT_PACE | |
| PSO Comp Dig Sig | AUT_PACE<br>AND PWD(PIN.QES) | |
| Delete | AUT_CMS | |
| andere | NEVER | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos | | |

| Zugriffsart | Zugriffsbedingung | |
|---|---|---|
| alle | herstellerspezifisch | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos<br>Zugriffsart Zugriffsbedingung | | |
| alle | NEVER | |

**[<=]**

**Card-G2-A_3622 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.E256**
Bei der Personalisierung von PrK.CH.QES.E256 MÜSSEN die in Tab_eGK_ObjSys_219 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

**Tabelle 114: Tab_eGK_ObjSys_219 Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.E256**

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

**[<=]**

## 6.2 Optionen für unvollständige QES-Anwendung

*Das Verfahren zum Nachladen einer QES ist noch nicht ausreichend definiert und muss mit allen Beteiligten abgestimmt werden. Gemäß dieser Spezifikation sind Karten mit von Anfang an installierter QES oder Karten ohne QES zuzulassen. Falls ein bestätigungsfähiger Prozess zum Nachladen der QES mit den beteiligten Parteien abgestimmt ist, kann der kartenbezogene Teil dieses Prozesses später in die Spezifikation aufgenommen werden.*

# 7 Anhang A – Verzeichnisse

## 7.1 Abkürzungen

| Kürzel | Erläuterung |
|---|---|
| AID | Application Identifier |
| AdV | Anwendungen des Versicherten |
| LE-AdV | Anwendungen des Versicherten in der Umgebung eines Leistungserbringers |
| KTR-AdV | Anwendungen des Versicherten in der Umgebung eines Kostenträgers |
| BCD | Binary Coded Decimal |
| BER | Basic Encoding Rules |
| CAN | Card Access Number |
| CMS | Card Management System,<br>System zur Administration von Karten und Applikationen |
| CHAT | Certificate Holder Autorisation Template<br>Liste von Rechten, die ein Zertifikatsinhaber besitzt |
| CIA | Cryptographic Information Application, Anwendung mit Informationen zu kryptographischen Diensten |
| CIO | Cryptographic Information Object, Objekt mit Informationen zu einem kryptographischen Dienst |
| CVC | Card Verifiable Certificate, kartenverifizierbares Zertifikat |
| DER | Distinguished Encoding Rules |
| DF | Dedicated File, Ordner |
| DF.ESIGN | Electronic Signature (Application) |
| DF.HCA | Health Care Application |
| DO | Datenobjekt bestehend aus Tag, Länge und Wert |

| | |
|---|---|
| EF | Elementary File, Datei |
| eIDAS | Verordnung über elektronische Identifizierung und Vertrauensdienste |
| ELC | Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven |
| FID | File Identifier |
| LCS | Life Cycle Status |
| MF | Master File, Wurzelverzeichnis |
| PuK | Public Key, öffentlicher Teil eines Schlüsselpaares |
| PrK | Private Key, privater Teil eines asymmetrischen Schlüsselpaares |
| SE#1 | Security Environment Number 1,<br>Sicherheitsumgebung mit der Nummer 1 |
| SFI | Short File Identifier |
| SK | Secret Key, geheimer, symmetrischer Schlüssel |
| tbd | to be defined (noch festzulegen) |
| TLV | Tag-Length-Value-Kodierung, siehe auch DO |
| VSD | Versichertenstammdatendienst |
| ZDA | Zertifizierungsdiensteanbieter |

## 7.2 Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

## 7.3 Abbildungsverzeichnis

Abbildung 1: Abb_eGK_ObjSys_001 Objektstruktur einer eGK auf oberster Ebene .....21
Abbildung 2: Abb_eGK_ObjSys_002 Dateistruktur der Gesundheitsanwendung .....76
Abbildung 3: Abb_eGK_ObjSys_003 Dateistruktur der Anwendung Notfalldatensatz .....95
Abbildung 4: Abb_eGK_ObjSys_004 Dateistruktur der Anwendung Datensatz Persönliche Erklärungen .....102

Abbildung 5: Abb_eGK_ObjSys_005 Dateistruktur der Anwendung Gesundheitsdatendienst ....108
Abbildung 6: Abb_eGK_ObjSys_010 Dateistruktur der Anwendung Organspendeerklärung ....115
Abbildung 7: Abb_eGK_ObjSys_011 Dateistruktur der Anwendung AMTS-Datenmanagement ....121
Abbildung 8: Abb_eGK_ObjSys_006 Objektstruktur der Anwendung DF.ESIGN ....132
Abbildung 9: Abb_eGK_ObjSys_009 Objektstruktur der vollständigen Signaturanwendung DF.QES ....167

## 7.4 Tabellenverzeichnis

Tabelle 1: Tab_eGK_ObjSys_001: Zuordnung der Bezeichnungen für PINs ....10
Tabelle 2: Tab_eGK_ObjSys_002: Liste der Komponenten, an welche dieses Dokument Anforderungen stellt....11
Tabelle 3: Tab_eGK_ObjSys_004 ATR-Codierung ....20
Tabelle 4: Tab_eGK_ObjSys_006 Initialisierte Attribute von MF ....22
Tabelle 5: Tab_eGK_ObjSys_007 Initialisierte Attribute von MF / EF.ATR....23
Tabelle 6: Tab_eGK_ObjSys_106 Initialisierte Attribute von MF / EF.CardAccess....25
Tabelle 7: Tab_eGK_ObjSys_009 Initialisierte Attribute von MF / EF.C.CA_eGK.CS.E256 ....26
Tabelle 8: Tab_eGK_ObjSys_110 Personalisierte Attribute von MF / EF.C.CA_eGK.CS.E256 ....29
Tabelle 9: Tab_eGK_ObjSys_012 Initialisierte Attribute von MF/EF.C.eGK.AUT_CVC.E256 ....29
Tabelle 10: Tab_eGK_ObjSys_112 Personalisierte Attribute von MF / EF.C.eGK.AUT_CVC.E256 ....31
Tabelle 11: Tab_eGK_ObjSys_014 Initialisierte Attribute von MF / EF.DIR....31
Tabelle 12: Tab_eGK_ObjSys_015 Initialisierte Attribute von MF / EF.GDO....33
Tabelle 13: Tab_eGK_ObjSys_182 Personalisiertes Attribut von MF / EF.GDO ....35
Tabelle 14: Tab_eGK_ObjSys_016 Initialisierte Attribute von MF / EF.Version @deprecated ....35
Tabelle 15: Tab_eGK_ObjSys_183 Initialisierte Attribute von MF / EF.Version2....37
Tabelle 16: Tab_eGK_ObjSys_017 Initialisierte Attribute von MF / PIN.CH ....39
Tabelle 17: Tab_eGK_ObjSys_117 Personalisierte Attribute von MF / PIN.CH....41
Tabelle 18: Tab_eGK_ObjSys_018 Initialisierte Attribute von MF / MRPIN.home ....41
Tabelle 19: Tab_eGK_ObjSys_047 Initialisierte Attribute von MF / MRPIN.NFD....43

Tabelle 20: Tab_eGK_ObjSys_052 Initialisierte Attribute von MF / MRPIN.DPE.....45
Tabelle 21: Tab_eGK_ObjSys_056 Initialisierte Attribute von MF / MRPIN.GDD.....46
Tabelle 22: Tab_eGK_ObjSys_092 Initialisierte Attribute von MF / MRPIN.NFD_READ.48
Tabelle 23: Tab_eGK_ObjSys_187 Initialisierte Attribute von MF / MRPIN.OSE .....50
Tabelle 24: Tab_eGK_ObjSys_194 Initialisierte Attribute von MF / MRPIN.AMTS.....51
Tabelle 25: Tab_eGK_ObjSys_195 Initialisierte Attribute von MF / PIN.AMTS_REP .....53
Tabelle 26: Tab_eGK_ObjSys_196 Personalisierte Attribute von MF / PIN.AMTS_REP.55
Tabelle 27: Tab_eGK_ObjSys_020 Initialisierte Attribute von MF / PrK.eGK.AUT_CVC.E256.....55
Tabelle 28: Tab_eGK_ObjSys_118 Personalisierte Attribute von MF / PrK.eGK.AUT_CVC.E256.....57
Tabelle 29: Tab_eGK_ObjSys_023 Initialisierte Attribute von MF / PuK.RCA.CS.E256..58
Tabelle 30: Tab_eGK_ObjSys_188 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten .....60
Tabelle 31: Tab_eGK_ObjSys_126 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256.....61
Tabelle 32: Tab_eGK_ObjSys_121 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256.....63
Tabelle 33: Tab_eGK_ObjSys_027 Initialisierte Attribute von MF / SK.CMS.AES128.....64
Tabelle 34: Tab_eGK_ObjSys_122 Personalisierte Attribute von MF / SK.CMS.AES128 .....66
Tabelle 35: Tab_eGK_ObjSys_028 Initialisierte Attribute von MF / SK.CMS.AES256.....66
Tabelle 36: Tab_eGK_ObjSys_123 Personalisierte Attribute von MF / SK.CMS.AES256 .....68
Tabelle 37: Tab_eGK_ObjSys_029 Initialisierte Attribute von MF / SK.VSD.AES128 .....68
Tabelle 38: Tab_eGK_ObjSys_124 Personalisierte Attribute von MF / SK.VSD.AES128 70
Tabelle 39: Tab_eGK_ObjSys_030 Initialisierte Attribute von MF / SK.VSD.AES256 .....70
Tabelle 40: Tab_eGK_ObjSys_125 Personalisierte Attribute von MF / SK.VSD.AES256 71
Tabelle 41: Tab_eGK_ObjSys_093 Initialisierte Attribute von MF / SK.CAN .....72
Tabelle 42: Tab_eGK_ObjSys_181 Personalisierte Attribute von MF / SK.CAN .....73
Tabelle 43: Tab_eGK_ObjSys_033 Initialisierte Attribute von MF / DF.HCA .....73
Tabelle 44: Tab_eGK_ObjSys_034 Initialisierte Attribute von MF / DF.HCA / EF.Einwilligung .....76
Tabelle 45: Tab_eGK_ObjSys_035 Initialisierte Attribute von MF / DF.HCA / EF.GVD ...78
Tabelle 46: Tab_eGK_ObjSys_036 Initialisierte Attribute von MF / DF.HCA / EF.Logging .....80
Tabelle 47: Tab_eGK_ObjSys_037 Initialisierte Attribute von MF / DF.HCA / EF.PD.....82

Tabelle 48: Tab_eGK_ObjSys_038 Initialisierte Attribute von MF / DF.HCA / EF.Prüfungsnachweis ....84
Tabelle 49: Tab_eGK_ObjSys_039 Initialisierte Attribute von MF / DF.HCA / EF.Standalone ....85
Tabelle 50: Tab_eGK_ObjSys_040 Initialisierte Attribute von MF / DF.HCA / EF.StatusVD ....87
Tabelle 51: Tab_eGK_ObjSys_042 Initialisierte Attribute von MF / DF.HCA / EF.VD ....89
Tabelle 52: Tab_eGK_ObjSys_043 Initialisierte Attribute von MF / DF.HCA / EF.Verweis ....91
Tabelle 53: Tab_eGK_ObjSys_044 Initialisierte Attribute von MF / DF.HCA / DF.NFD ....92
Tabelle 54: Tab_eGK_ObjSys_045 Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.NFD ....95
Tabelle 55: Tab_eGK_ObjSys_046 Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.StatusNFD ....97
Tabelle 56: Tab_eGK_ObjSys_049 Initialisierte Attribute von MF / DF.HCA / DF.DPE ....99
Tabelle 57: Tab_eGK_ObjSys_050 Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.DPE ....102
Tabelle 58: Tab_eGK_ObjSys_051 Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.StatusDPE ....104
Tabelle 59: Tab_eGK_ObjSys_054 Initialisierte Attribute von MF / DF.HCA / DF.GDD ....106
Tabelle 60: Tab_eGK_ObjSys_055 Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.EinwilligungGDD ....109
Tabelle 61: Tab_eGK_ObjSys_057 Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.VerweiseGDD ....110
Tabelle 62: Tab_eGK_ObjSys_184 Initialisierte Attribute von MF / DF.HCA / DF.OSE ....112
Tabelle 63: Tab_eGK_ObjSys_185 Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.OSE ....115
Tabelle 64: Tab_eGK_ObjSys_186 Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.StatusOSE ....117
Tabelle 65: Tab_eGK_ObjSys_189 Initialisierte Attribute von MF / DF.HCA / DF.AMTS ....119
Tabelle 66: Tab_eGK_ObjSys_191 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.AMTS ....121
Tabelle 67: Tab_eGK_ObjSys_192 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS ....124
Tabelle 68: Tab_eGK_ObjSys_193 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.StatusAMTS ....126
Tabelle 69: Tab_eGK_ObjSys_197 Initialisierte Attribute von MF /DF.HCA / DF.AMTS PrK.AMTS.ENC.E256 ....128

Tabelle 70: Tab_eGK_ObjSys_198 Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256....130
Tabelle 71: Tab_eGK_ObjSys_059 Initialisierte Attribute von MF / DF.ESIGN ....131
Tabelle 72: Tab_eGK_ObjSys_060 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048....132
Tabelle 73: Tab_eGK_ObjSys_146 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048....134
Tabelle 74: Tab_eGK_ObjSys_061 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048....134
Tabelle 75: Tab_eGK_ObjSys_148 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048....136
Tabelle 76: Tab_eGK_ObjSys_062 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048....137
Tabelle 77: Tab_eGK_ObjSys_150 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048....138
Tabelle 78: Tab_eGK_ObjSys_063 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048....139
Tabelle 79: Tab_eGK_ObjSys_154 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048....140
Tabelle 80: Tab_eGK_ObjSys_064 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048....141
Tabelle 81: Tab_eGK_ObjSys_156 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048....142
Tabelle 82: Tab_eGK_ObjSys_067 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048....143
Tabelle 83: Tab_eGK_ObjSys_159 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048....144
Tabelle 84: Tab_eGK_ObjSys_070 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048....145
Tabelle 85: Tab_eGK_ObjSys_162 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048....146
Tabelle 86: Tab_eGK_ObjSys_076 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048....147
Tabelle 87: Tab_eGK_ObjSys_168 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048....148
Tabelle 88: Tab_eGK_ObjSys_200 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.E256....149
Tabelle 89: Tab_eGK_ObjSys_201 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.E256....150
Tabelle 90: Tab_eGK_ObjSys_202 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.E256....151

Tabelle 91: Tab_eGK_ObjSys_203 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.E256 ....152
Tabelle 92: Tab_eGK_ObjSys_204 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.E256 ....153
Tabelle 93: Tab_eGK_ObjSys_205 Personalisierte Attribute von MF / DF.ESIGN/ EF.C.CH.ENC.E256 ....154
Tabelle 94: Tab_eGK_ObjSys_206 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.E256 ....155
Tabelle 95: Tab_eGK_ObjSys_207 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.E256 ....156
Tabelle 96: Tab_eGK_ObjSys_208 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.E256 ....157
Tabelle 97: Tab_eGK_ObjSys_209 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.E256 ....158
Tabelle 98: Tab_eGK_ObjSys_210 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN. E256 ....159
Tabelle 99: Tab_eGK_ObjSys_211 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN. E256 ....160
Tabelle 100: Tab_eGK_ObjSys_212 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.E256....161
Tabelle 101: Tab_eGK_ObjSys_213 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.E256....162
Tabelle 102: Tab_eGK_ObjSys_214 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.E256 ....163
Tabelle 103: Tab_eGK_ObjSys_215 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.E256 ....164
Tabelle 104: Tab_eGK_ObjSys_086 Initialisierte Attribute von MF / DF.QES ....165
Tabelle 105: Tab_eGK_ObjSys_087 Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048 ....167
Tabelle 106: Tab_eGK_ObjSys_175 Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048 ....169
Tabelle 107: Tab_eGK_ObjSys_088 Initialisierte Attribute von MF / DF.QES / PIN.QES ....169
Tabelle 108: Tab_eGK_ObjSys_177 Personalisierte Attribute von MF / DF.QES / PIN.QES....171
Tabelle 109: Tab_eGK_ObjSys_089 Initialisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048 ....172
Tabelle 110: Tab_eGK_ObjSys_178 Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048 ....174
Tabelle 111: Tab_eGK_ObjSys_216 Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.E256 ....174

Tabelle 112: Tab_eGK_ObjSys_217 Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.E256 .....176
Tabelle 113: Tab_eGK_ObjSys_218 Initialisierte Attribute von MF / DF.QES / PrK.CH.QES.E256.....176
Tabelle 114: Tab_eGK_ObjSys_219 Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.E256.....178

## 7.5 Referenzierte Dokumente

### 7.5.1 Dokumente der gematik

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

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
|---|---|
| [gemProdT_eGK] | gematik: Produkttypsteckbrief – Prüfvorschrift eGK |
| [gemSpec_COS] | gematik: Spezifikation des Card Operating System (COS) - Elektrische Schnittstelle für Karten (eGK, SMC und HBA) der Generation 2 |
| [gemSpec_eGK_OPT] | gematik: Spezifikation der elektronischen Gesundheitskarte Äußere Gestaltung für eGK der Generation 2 |
| [gemSpec_Karten_Fach_TIP_G2.1] | gematik: Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1 |
| [gemSpec_Krypt] | gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec_PINPUK_TI] | gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur |
| [gemSpec_CAN_TI] | gematik: Übergreifende Spezifikation CAN-Policy |
| [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 |

### 7.5.2 Weitere Dokumente

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
|---|---|
| [DIN_EN_1867] | EN 1867:1997<br>Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers<br>DIN EN 1867:1997<br>Maschinenlesbare Karten – Anwendungen im Gesundheitswesen – Benummerungssystem und Registrierungsverfahren für Kartenausgeberschlüssel |
| [DIN66291-4] | DIN V66291-4 (2002):<br>Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG/SigV<br>Teil 4: Grundlegende Sicherheitsdienste |
| [ISO3166-1] | ISO/IEC 3166-1:1997<br>Codes for the representations of names of countries – Part 1: Country codes |
| [ISO7816-15] | ISO/IEC 7816-15: 2004<br>Identification cards - Integrated circuit cards - Part 15: Cryptographic information application |
| [ISO7816-4] | ISO/IEC 7816-4: 2005 (2nd edition)<br>Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange |
| [ISO8825-1] | ISO/IEC 8825-1: 1995<br>Information technology – ASN.1 encoding rules:<br>Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)<br>http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf |

| | |
|---|---|
| [EN14890–1] | EN 14890-1: 2008<br>Application Interface for Smartcards used as secure signature creation devices, Part 1: Basic services |
| [Resolution190] | 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<br>Key words for use in RFCs to Indicate Requirement Levels<br>http://www.apps.ietf.org/rfc/rfc2119.html |
| [SD5] | ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19<br>Register of IC manufacturers<br>http://www.pkicc.de/cms/media/pdfs/IC_manufacturer_ISO_SD5_1962006.pdf |
| [TR-03110-2] | Technische Richtlinie TR-03116-2<br>Worked Example for Extended Access Control (EAC)<br>PACE, Chip Authentication and Terminal Authentication, Version 1.02 |