Einführung der Gesundheitskarte

Spezifikation der elektro­nischen Gesundheitskarte  
eGK-Objektsystem

|  |  |
| --- | --- |
| Version: | 3.11.0 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\18 |
| Stand: | 28.10.2016 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec\_eGK\_ObjSys] |

Dokumentinformationen

Änderungen zur Vorversion

Überarbeitung der Dokumente für den Online-Produktivbetrieb (Stufe 1), als Grundlage für Produktivzulassungen und den bundesweiten Rollout.

Dokumentenhistorie

| **Version** | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | **Bearbeitung** |
| --- | --- | --- | --- | --- |
| 2.3.2 | 05.08.09 |  | Die Version 2.2.0 der „Spezifikation des elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen“ für die Generation 1 einschließlich der dazu veröffentlichten SRQ ist Grundlage der vorliegenden Spezifikation. Die Dokumentenhistorie der Version 2.2.0 ist nicht in dieses Dokument übernommen worden; sie kann bei Bedarf dort eingesehen werden. | gematik |
| 3.0.0 | 19.09.12 |  | Einfügen Korrekturen nach Kommentaren | P71 |
| 3.0.1 | 01.10.12 |  | Einfügen von Korrekturen nach Kommentaren, Konsolidierung der Änderungen | P71 |
| 3.1.1 | 23.01.13 |  | Entfernung der Objekte für CVC R2048  Umwandlung der Zugriffsbedingungen für G1 von normativer Vorgabe in informative Erläuterung | PL P71 |
| 3.2.0 RC | 26.03.13 |  | Einfügen Änderung EF.DIR gemäß Abstimmung, Vorgaben Schlichterspruch zu PIN.CH eingefügt | P71 |
| 3.2.0 RC B | 22.08.13 |  | Fehlerkorrektur, Beschreibung Flaglist präzisiert  Einfügen einer Anforderung zu *persistentPublicKeyList* | gematik |
| 3.3.0 RC | 23.10.13 |  | Das Attribut *shareable* wurde für alle Ordner und Dateien hinzugefügt, Ändern der Flaglist-Darstellung, Fehlerkorrekturen, Einfügen von EF.CardAccess, Bearbeitung gemäß Kommentaren Industrie | P71 |
| 3.4.0 RC | 18.12.13 |  | Aufnahme des Kommandos List Public Key für MF, Zuordnung der AFOs zu Initialisierung und Personalisierung, Überarbeitung der Struktur, Entfernen der Option Lange Lebensdauer sowie EF.ZZ, Einfügen Änderungen zu EF.ATR, EF.DIR und EF.Version, Option „Testkarten“ wurde aufgenommen Präzisierung Referenzen für Zertifikate und Schlüssel, Modifizieren von EF.GDO | P71 |
| 3.5.0 | 21.02.14 |  | Einfügen einer Liste offener Punkte, Kommentare eingearbeitet, Expiration Date für Sicherheitsanker festgelegt, Iteration 2b, Streichen von EF.VerweisNFD und EF.VerweisDPE | P71 |
| 3.6.0 | 27.03.14 |  | Einarbeitung Fehlerkorrektur Iteration 2b | gematik |
| 3.7.0 | 06.06.14 |  | Einarbeitung Änderungen Iteration 3 | gematik |
| 3.8.0 | 26.08.14 |  | Einarbeitung Änderungen Iteration 3, Vorgaben zu AMTS, Änderungen Iteration 4 | gematik |
| 3.9.0 | 23.07.15 |  | Folgende Errata eingearbeitet:  R.1.4.1, R1.4.2, R1.4.3, R1.4.5, R1.4.7 | Technik / SPE |
| 3.10.0 | 24.08.16 |  | Anpassungen zum Online-Produktivbetrieb (Stufe 1) | gematik |
|  |  |  | Anpassungen gemäß Änderungsliste |  |
| 3.11.0 | 28.10.16 |  | freigegeben | gematik |

Inhaltsverzeichnis

[Dokumentinformationen 2](#_Toc503163351)

[Inhaltsverzeichnis 4](#_Toc503163352)

[1 Einordnung des Dokuments 8](#_Toc503163353)

[1.1 Zielsetzung 8](#_Toc503163354)

[1.2 Zielgruppe 8](#_Toc503163355)

[1.3 Geltungsbereich 8](#_Toc503163356)

[1.4 Abgrenzung des Dokuments 9](#_Toc503163357)

[1.5 Methodik 9](#_Toc503163358)

[1.5.1 Nomenklatur 9](#_Toc503163359)

[1.5.2 Verwendung von Schlüsselworten 11](#_Toc503163360)

[1.5.3 Komponentenspezifische Anforderungen 12](#_Toc503163361)

[2 Optionen 13](#_Toc503163362)

[3 Lebenszyklus von Karte und Applikation 14](#_Toc503163363)

[4 Anwendungsübergreifende Festlegungen 15](#_Toc503163364)

[4.1 Unterstützung optionaler Funktionspakete 15](#_Toc503163365)

[4.1.1 USB-Schnittstelle (optional) 15](#_Toc503163366)

[4.1.2 Kontaktlose Schnittstelle (optional) 15](#_Toc503163367)

[4.1.3 Logische Kanäle (optional) 16](#_Toc503163368)

[4.1.4 Kryptobox (optional) 17](#_Toc503163369)

[4.2 Reservierung Speicherplatz 17](#_Toc503163370)

[4.2.1 AMTS 17](#_Toc503163371)

[4.2.2 Speicherplatz für zukünftige Anwendungen 17](#_Toc503163372)

[4.2.3 Größe der Speicherplatzreservierung für zukünftige Anwendungen 18](#_Toc503163373)

[4.3 Attributstabellen 18](#_Toc503163374)

[4.3.1 Attribute einer Datei (EF) 19](#_Toc503163375)

[4.4 Zugriffsregeln für besondere Kommandos 19](#_Toc503163376)

[4.5 Attributswerte und Personalisierung 19](#_Toc503163377)

[5 Spezifikation grundlegender Applikationen 21](#_Toc503163378)

[5.1 Attribute des Objektsystems 21](#_Toc503163379)

[5.1.1 Answer To Reset 22](#_Toc503163380)

[5.2 Allgemeine Struktur 24](#_Toc503163381)

[5.3 Root, die Wurzelapplikation (MF) 24](#_Toc503163382)

[5.3.1 MF / EF.ATR 25](#_Toc503163383)

[5.3.2 MF / EF.CardAccess (Option kontaktlose Schnittstelle) 26](#_Toc503163384)

[5.3.3 MF / EF.C.CA\_eGK.CS.E256 27](#_Toc503163385)

[5.3.4 MF / EF.C.eGK.AUT\_CVC.E256 29](#_Toc503163386)

[5.3.5 MF / EF.DIR 30](#_Toc503163387)

[5.3.6 MF / EF.GDO 31](#_Toc503163388)

[5.3.7 MF / EF.Version 32](#_Toc503163389)

[5.3.8 MF / EF.Version2 34](#_Toc503163390)

[5.3.9 MF / PIN.CH 35](#_Toc503163391)

[5.3.10 MF / MRPIN.home 37](#_Toc503163392)

[5.3.11 MF / PrK.eGK.AUT\_CVC.E256 38](#_Toc503163393)

[5.3.12 Sicherheitsanker zum Import von CV-Zertifikaten 39](#_Toc503163394)

[5.3.12.1 MF / PuK.RCA.CS.E256 39](#_Toc503163395)

[5.3.13 Asymmetrische Kartenadministration 41](#_Toc503163396)

[5.3.13.1 MF / PuK.RCA.ADMINCMS.CS.E256 42](#_Toc503163397)

[5.3.14 Symmetrische Kartenadministration 44](#_Toc503163398)

[5.3.14.1 MF / SK.CMS.AES128 44](#_Toc503163399)

[5.3.14.2 MF / SK.CMS.AES256 46](#_Toc503163400)

[5.3.14.3 MF / SK.VSD.AES128 47](#_Toc503163401)

[5.3.14.4 MF/ SK.VSD.AES256 48](#_Toc503163402)

[5.3.15 MF / SK.CAN 49](#_Toc503163403)

[5.4 Gesundheitsanwendung, Health Care Application (DF.HCA) 50](#_Toc503163404)

[5.4.1 MF / DF.HCA / EF.Einwilligung 51](#_Toc503163405)

[5.4.2 MF / DF.HCA / EF.GVD 53](#_Toc503163406)

[5.4.3 MF / DF.HCA / EF.Logging 54](#_Toc503163407)

[5.4.4 MF / DF.HCA / EF.PD 55](#_Toc503163408)

[5.4.5 MF / DF.HCA / EF.Prüfungsnachweis 56](#_Toc503163409)

[5.4.6 MF / DF.HCA / EF.Standalone 58](#_Toc503163410)

[5.4.7 MF / DF.HCA / EF.StatusVD 59](#_Toc503163411)

[5.4.8 MF / DF.HCA / EF.TTN 59](#_Toc503163412)

[5.4.9 MF / DF.HCA / EF.VD 61](#_Toc503163413)

[5.4.10 MF / DF.HCA / EF.Verweis 61](#_Toc503163414)

[5.4.11 Anwendung Notfalldatensatz (DF.NFD) 62](#_Toc503163415)

[5.4.11.1 MF / DF.HCA / DF.NFD / EF.NFD 64](#_Toc503163416)

[5.4.11.2 MF / DF.HCA / DF.NFD / EF.StatusNFD 65](#_Toc503163417)

[5.4.11.3 MF / DF.HCA / DF.NFD / MRPIN.NFD 67](#_Toc503163418)

[5.4.11.4 MF / DF.HCA / DF.NFD / MRPIN.NFD\_READ 69](#_Toc503163419)

[5.4.12 Anwendung Datensatz Persönliche Erklärungen (DF.DPE) 70](#_Toc503163420)

[5.4.12.1 MF / DF.HCA / DF.DPE / EF.DPE 72](#_Toc503163421)

[5.4.12.2 MF / DF.HCA / DF.DPE / EF.StatusDPE 73](#_Toc503163422)

[5.4.12.3 MF / DF.HCA / DF.DPE / MRPIN.DPE 74](#_Toc503163423)

[5.4.12.4 MF / DF.HCA / DF.DPE / MRPIN.DPE\_READ 76](#_Toc503163424)

[5.4.13 Anwendung Gesundheitsdatendienst (GDD) 77](#_Toc503163425)

[5.4.13.1 MF / DF.HCA / DF.GDD / EF.EinwilligungGDD 79](#_Toc503163426)

[5.4.13.2 MF / DF.HCA / DF.GDD / EF.VerweiseGDD 80](#_Toc503163427)

[5.4.13.3 MF / DF.HCA / DF.GDD / MRPIN.GDD 81](#_Toc503163428)

[5.4.14 Anwendung Organspendeerklärung (DF.OSE) 83](#_Toc503163429)

[5.4.14.1 MF / DF.HCA / DF.OSE / EF.OSE 85](#_Toc503163430)

[5.4.14.2 MF / DF.HCA / DF.OSE / EF.StatusOSE 86](#_Toc503163431)

[5.4.14.3 MF / DF.HCA / DF.OSE / MRPIN.OSE 87](#_Toc503163432)

[5.4.15 Anwendung AMTS Datenmanagement (DF.AMTS), (AMTS\_angelegt) 89](#_Toc503163433)

[5.4.15.1 MF / DF.HCA / DF.AMTS / EF.EinwilligungAMTS (AMTS\_angelegt) 90](#_Toc503163434)

[5.4.15.2 MF / DF.HCA / DF.AMTS / EF.AMTS (AMTS\_angelegt) 92](#_Toc503163435)

[5.4.15.3 MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS (AMTS\_angelegt) 93](#_Toc503163436)

[5.4.15.4 MF / DF.HCA / DF.AMTS / EF.StatusAMTS (AMTS\_angelegt) 93](#_Toc503163437)

[5.4.15.5 MF / DF.HCA / DF.AMTS / MRPIN.AMTS (AMTS\_angelegt) 95](#_Toc503163438)

[5.4.15.6 MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP (AMTS\_angelegt) 96](#_Toc503163439)

[5.4.15.7 MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256 (AMTS\_angelegt) 98](#_Toc503163440)

[5.5 DF.ESIGN (Krypto-Anwendung ESIGN) 100](#_Toc503163441)

[5.5.1 MF / DF.ESIGN / EF.C.CH.AUT.R2048 101](#_Toc503163442)

[5.5.2 MF / DF.ESIGN / EF.C.CH.AUTN.R2048 103](#_Toc503163443)

[5.5.3 MF / DF.ESIGN / EF.C.CH.ENC.R2048 105](#_Toc503163444)

[5.5.4 MF / DF.ESIGN / EF.C.CH.ENCV.R2048 106](#_Toc503163445)

[5.5.5 MF / DF.ESIGN / PrK.CH.AUT.R2048 108](#_Toc503163446)

[5.5.6 MF / DF.ESIGN / PrK.CH.AUTN.R2048 109](#_Toc503163447)

[5.5.7 MF / DF.ESIGN / PrK.CH.ENC.R2048 111](#_Toc503163448)

[5.5.8 MF / DF.ESIGN / PrK.CH.ENCV.R2048 112](#_Toc503163449)

[5.6 Beschreibung kryptographischer Objekte, CIA\_ESIGN 114](#_Toc503163450)

[5.6.1 MF / DF.CIA\_ESIGN / EF.CIA\_Info 115](#_Toc503163451)

[6 Qualifizierte elektronische Signatur 118](#_Toc503163452)

[6.1 DF.QES (QES-Anwendung komplett angelegt und nutzbar) 118](#_Toc503163453)

[6.1.1 MF / DF.QES / EF.C.CH.QES.R2048 120](#_Toc503163454)

[6.1.2 MF / DF.QES / PIN.QES 121](#_Toc503163455)

[6.1.3 MF / DF.QES / PrK.CH.QES.R2048 123](#_Toc503163456)

[6.2 Optionen für unvollständige QES-Anwendung 125](#_Toc503163457)

[Anhang A – Verzeichnisse 126](#_Toc503163458)

# 

# Einordnung des Dokuments

## 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).

## 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.

## 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.*

## 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.

## Methodik

### Nomenklatur

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

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

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

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.

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

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)  OR SmMac(SK.CMS.AES256)  OR SmMac(flagCMS.08)}  AND SmCmdEnc  AND SmRspEnc |
| AUT\_VSD | {SmMac(SK.VSD.AES128)  OR SmMac(SK.VSD.AES256)  OR SmMac(flagCMS.09)}  AND SmCmdEnc  AND SmRspEnc |

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

1. Für Kommandonachrichten ohne Kommandodaten ist der Term SmCmdEnc sinnlos.
2. Für Antwortnachrichten ohne Antwortdaten ist der Term SmRspEnc sinnlos.
3. Die Spezifikation ist wie folgt zu interpretieren:
   1. Falls eine Kommandonachricht keine Kommandodaten enthält, ist es zulässig den Term SmCmdEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
   2. 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:
   1. Falls für eine Zugriffsart keine Kommandodaten existieren, ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmCmdEnc zu verwenden.
   2. Falls für eine Zugriffsart keine Antwortdaten existieren, ist es für den Prüfling zulässig in der zugehörige 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 |

### 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:

**⌦ Card-G2-A\_xxxx <Titel der Afo>**

Text / Beschreibung

**⌫**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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

### Komponentenspezifische Anforderungen

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

Tabelle 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 |

# 

# Optionen

In den Kapiteln 5.3.13 und 5.3.14 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**

1. Da die eGK Online administriert wird, MUSS ein Kartenherausgeber bei der Personalisierung Schlüssel für mindestens eines der beiden Verfahren
2. asymmetrische Authentifizierung für CMS/VSD
3. symmetrische Authentifizierung für CMS/VSD
4. in die Karte einbringen und sicherstellen, dass das dazugehörende CMS bzw. der dazugehörende VSD über die entsprechenden Schlüssel verfügt.
5. **⌫**

**⌦ 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.

**⌫**

# Lebenszyklus von Karte und Applikation

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

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

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

# 

# Anwendungsübergreifende Festlegungen

Zur Umsetzung dieses Kartentyps ist ein Betriebssystem hinreichend, welches keine der in [gemSpec\_COS] spezifizierten Optionen umsetzt.

## Unterstützung optionaler Funktionspakete

### 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**

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

### Kontaktlose Schnittstelle (optional)

**⌦ Card-G2-A\_2975 K\_eGK: Kontaktlose Schnittstelle**

Falls eine eGK die Option\_kontaktlose\_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option\_kontaktlose\_Schnittstelle implementiert hat.

**⌫**

**⌦ Card-G2-A\_2976 K\_eGK:** Vorhandensein einer Kontaktlosen Schnittstelle

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

**⌦ Card-G2-A\_2977 K\_eGK: Zusatzanforderungen für kontaktlose Schnittstelle**

1. Falls eine eGK die Option\_kontaktlose\_Schnittstelle nutzen will, dann MÜSSEN zusätzlich zu allen nicht gekennzeichneten Anforderungen auch alle Anforderungen erfüllt sein, die mit Option\_kontaktlose\_Schnittstelle gekennzeichnet sind.
2. **⌫**

**⌦ Card-G2-A\_2978 K\_Initialisierung: Kontaktlose Schnittstelle wird nicht genutzt**

1. Will der Kartenherausgeber einer eGK mit einem COS, das die Option\_kontaktlose\_Schnittstelle gemäß [gemSpec\_COS] implementiert hat, die Nutzung dieser Schnittstelle verhindern, dann MUSS das Attribut *interfaceDependentAccessRules* aller Objekte so gesetzt sein, dass im Rahmen einer kontaktlosen Kommunikation die Zugriffsregelauswertung AccessRuleEvaluation (siehe [gemSpec\_COS#10.4] stets den Wert „False“ liefert.
2. **⌫**

**⌦ Card-G2-A\_2979 K\_Initialisierung: Kontaktlose Schnittstelle im COS nicht vorhanden**

1. Falls das COS für eine eGK die Option\_kontaktlose\_Schnittstelle nicht implementiert hat, MUSS der Teil des Attributes *interfaceDependentAccessRules*, welcher sich auf die kontaktlose Kommunikation bezieht, für alle Objekte irrelevant für die Zulassung sein.
2. **⌫**

**⌦ Card-G2-A\_2980 K\_Personalisierung: Absicherung der kontaktlosen Schnittstelle**

1. Falls eine eGK die Option\_kontaktlose\_Schnittstelle nutzen will, MUSS die Kommunikation zwischen Karte und Kartenleser mit einer gegenseitigen Authentifizierung und Aufbau eines sicheren Kommunikationskanals abgesichert werden. Hierfür MUSS das PACE-Protokoll genutzt werden.
2. **⌫**

**⌦ Card-G2-A\_2339 K\_Personalisierung: Druck der CAN auf die eGK bei Verwendung der optionalen kontaktlosen Schnittstelle**

1. Falls eine eGK die Option\_kontaktlose\_Schnittstelle nutzen will, MUSS das Attribut *can* des Objektes SK.CAN mit der Nummer übereinstimmen, die gemäß [gemSpec\_eGK\_OPT#Card-G2-A\_2258] auf die eGK gedruckt ist.
2. **⌫**

**⌦ Card-G2-A\_3204 K\_Personalisierung und K\_Initialisierung: Konformität kontaktlose Schnittstelle**

1. Eine eGK mit kontaktloser Schnittstelle MUSS in ihrer endgültigen Konfiguration (einschließlich Kartenkörper und Antenne) bezüglich der elektrischen Eigenschaften dieser kontaktlosen Schnittstelle konform zu [ISO-IEC 14443] und [ISO/IEC FCD 10373-6] sein.
2. **⌫**

### Logische Kanäle (optional)

**⌦ Card-G2-A\_2981 K\_eGK: logische\_Kanäle**

1. Falls eine eGK die Option\_logische\_Kanäle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option\_logische\_Kanäle implementiert hat.
2. **⌫**

**⌦ Card-G2-A\_2982 K\_Initialisierung: Anzeige von logischen Kanälen**

1. Falls das COS die Option\_logische\_Kanäle
2. nicht unterstützt, dann MUSS das dritte Oktett in den Card Capabilities den Wert ‘E0’ besitzen.
3. 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. **⌫**

### 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**

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

## Reservierung Speicherplatz

### AMTS

**⌦ Card-G2-A\_3272 K\_Initialisierung: Vorgaben für AMTS**

Für die Anwendung AMTS MUSS eine der beiden folgenden Varianten umgesetzt werden:

* 1. AMTS\_vorbereitet
  2. AMTS\_angelegt
  3. **⌫**

**⌦ Card-G2-A\_3230 K\_Initialisierung: AMTS\_** **vorbereitet**

Falls die Variante AMTS\_vorbereitet umgesetzt wird, MUSS ein Speicherbereich in der Größe von 15.360 Byte für das nachträgliche Anlegen von DF.AMTS vorhanden sein.

**⌫**

**⌦ Card-G2-A\_3279 K\_Initialisierung: AMTS\_angelegt**

Falls die Variante AMTS\_angelegt umgesetzt wird, MÜSSEN alle Anforderungen erfüllt werden, die mit AMTS\_angelegt gekennzeichneten sind.

**⌫**

### Speicherplatz für zukünftige Anwendungen

**⌦ 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.

**⌫**

### Größe der Speicherplatzreservierung für zukünftige Anwendungen

**⌦ Card-G2-A\_3238 K\_Initialisierung: Größe der Speicherplatzreservierung für zukünftige Anwendungen**

Zusätzlich zu den Anforderungen zu AMTS SOLL für weitere zukünftige Anwendungen ein Speicherbereich in der Größe von 10.000 Byte vorhanden sein.

**⌫**

## Attributstabellen

**⌦ Card-G2-A\_2333 K\_Initialisierung: Änderung von Zugriffsregeln**

1. Die in diesem Dokument definierten Zugriffsregeln DÜRFEN nach Abschluss der Initialisierungsphase NICHT veränderbar sein.
2. **⌫**

**⌦ Card-G2-A\_2334 K\_Initialisierung: Eigenschaften aller Objekte in SE#1**

1. Alle Objekte MÜSSEN sich in SE#1 wie angegeben verwenden lassen.
2. **⌫**

**⌦ Card-G2-A\_2857 K\_Initialisierung: Verwendbarkeit der Objekte in anderen SEs**

1. Jedes Objekt KANN in SE verwendbar sein, die verschieden sind von SE#1.
2. **⌫**

**⌦ Card-G2-A\_2858 K\_Initialisierung: Eigenschaften der Objekte in anderen SEs**

1. Falls ein Objekt in einem von SE#1 verschiedenen SE verwendbar ist, dann MUSS es dort dieselben Eigenschaften wie in SE#1 besitzen.
2. **⌫**

**⌦ Card-G2-A\_2335 K\_Initialisierung: Ordnerattribute**

1. Enthält eine Tabelle mit Ordnerattributen
2. keinen applicationIdentifier (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.
3. einen oder mehrere AID, dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
4. keinen *fileIdentifier* (FID),
5. 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.
6. so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec\_COS#8.1.1] zugeordnet werden.
7. **⌫**

### Attribute einer Datei (EF)

**⌦ Card-G2-A\_2336 K\_Initialisierung: Dateiattribute**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_2667 K\_Personalisierung und K\_Initialisierung: Wert von „positionLogicalEndOfFile“**

1. Für transparente EFs MUSS der Wert von „positionLogicalEndOfFile“, soweit nicht anders spezifiziert, auf die Anzahl der tatsächlich belegten Bytes gesetzt werden.
2. **⌫**

## Zugriffsregeln für besondere Kommandos

**⌦ Card-G2-A\_2337 K\_Initialisierung: Zugriffsregeln für besondere Kommandos**

1. Für Kommandos, für die eine Zugriffsregelauswertung gemäß [gemSpec\_COS] optional ist, werden nicht in den Attributstabellen, sondern zentral in dieser Anforderung die Zugriffsbedingungen festgelegt:
2. Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kom­mandos Get Challenge, List Public Key, Manage Security Environment und Select stets ALWAYS sein.
3. Falls eGK die Option\_kontaktlose\_Schnittstelle unterstützt, dann MUSS die Zugriffsbedingung für die Kommandos Get Challenge, List Public Key, Manage Security Environment und Select für die kontaktlose Schnittstelle stets ALWAYS sein.
4. Falls ein Kartenherausgeber die Nutzung einer im COS vorhandenen kontaktlosen Schnittstelle unterbinden will, dann MUSS die Zugriffs­bedingung für die Kommandos Get Challenge, List Public Key, Manage Security Environment und Select für die kontaktlose Schnittstelle herstellerspezifisch stets entweder ALWAYS oder NEVER sein.
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.

**⌫**

# 

# 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),
* die Krypto-Anwendung DF.ESIGN und
* die Beschreibung kryptographischer Objekte DF.CIA\_ESIGN.

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

## Attribute des Objektsystems

Das Objektsystem gemäß [gemSpec\_COS#9.1] enthält folgende Attribute:

**⌦ Card-G2-A\_2341 K\_Initialisierung: Wert des Attributes *root***

1. Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab\_eGK\_ObjSys\_006 sein.
2. **⌫**

**⌦ Card-G2-A\_2342 K\_Personalisierung und K\_Initialisierung: Wert des Attributes answerToReset**

1. Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A\_2345, Card-G2-A\_2346, Card-G2-A\_2347 und Card-G2-A\_2985entsprechen.
2. **⌫**

**⌦ Card-G2-A\_2343 K\_Personalisierung: Wert des Attributes iccsn8**

1. Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein.
2. **⌫**

**⌦ Card-G2-A\_2344 K\_Initialisierung: Inhalt persistentPublicKeyList**

1. Das Attribut *persistentPublicKeyList* MUSS den Schlüssel PuK.RCA.CS.E256 enthalten.
2. **⌫**

**⌦ Card-G2-A\_3180 K\_Initialisierung: Größe persistentPublicKeyList**

1. Für das Attribut *persistentPublicKeyList* MUSS so viel Speicherplatz bereitgestellt werden, dass mindestens fünf weitere öffentliche Signaturprüfschlüssel einer Root-CA mittels Linkzertifikaten persistent importierbar sind
2. **⌫**

**⌦ Card-G2-A\_3265 K\_Initialisierung: Wert von *pointInTime***

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

**⌫**

**⌦ Card-G2-A\_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.

**⌫**

### Answer To Reset

**⌦ Card-G2-A\_2345 K\_Personalisierung und K\_Initialisierung: ATR-Codierung**

1. 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\_2346 K\_Personalisierung und K\_Initialisierung: TC1 Byte im ATR**

1. Der ATR SOLL ein TC1 Byte mit dem Wert ‘FF’ enthalten. In diesem Fall MUSS T0 auf den Wert ‘Dx’ gesetzt werden.
2. **⌫**

**⌦ Card-G2-A\_2985 K\_Personalisierung und K\_Initialisierung: Historical Bytes im ATR**

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

⌦ 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.
3. **⌫**

## Allgemeine Struktur

Abb\_eGK\_ObjSys\_001 zeigt die allgemeine Struktur der eGK.



Abbildung 1: Abb\_eGK\_ObjSys\_001 Objektstruktur einer eGK auf oberster Ebene

## 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**

1. 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’ | falls vorhanden |
| *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 |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren oder terminieren lassen, sind diese Zustände für Objekte im 5.3 im Allgemeinen irrelevant.

### 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 K\_Initialisierung: Initialisierte Attribute von MF / EF.ATR**

1. 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] |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Read Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Binary  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 |  |

**⌫**

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

**⌦ Card-G2-A\_3205 K\_Initialisierung: Initialisiertes Attribu*t numberOfOctet* von MF / EF.ATR**

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

* genau 23 Oktette für die Artefakte PT\_Pers und PI\_Personalisierung frei bleiben, falls PI\_Kartenkörper initialisiert wird, oder
* genau 41 Oktette für die Artefakte PI\_Kartenkörper, PT\_Pers und PI\_Personalisierung frei bleiben.

**⌫**

### MF / EF.CardAccess (Option kontaktlose Schnittstelle)

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

**⌦ Card-G2-A\_3200 K\_Initialisierung: Initialisierte Attribute von MF / EF.CardAccess**

1. Falls die kontaktlose Schnittstelle für die eGK genutzt wird, MUSS EF.CardAccess vorhanden sein und 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos | | |
| alle | herstellerspezifisch |  |

2. **⌫**

### MF / EF.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**

1. 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Update Binary | AUT\_CMS |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  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 |  |

**⌫**

1. 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] |

**⌫**

### 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**

1. 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.
2. **⌫**

**⌦ Card-G2-A\_2364 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.eGK.AUT\_CVC.E256**

1. 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** | | |
| *accessRules* | identisch zu EF.C.CA\_eGK.CS.E256 |  |

**⌫**

**⌦ 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 |  |

**⌫**

### 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\_2367 K\_Initialisierung: Initialisierte Attribute von MF / EF.DIR**

1. 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 Rekord |  |
| *maxRecordLength* | 32 Oktett |  |
| *flagRecordLCS* | False |  |
| *numberOfOctet* | ‘00C8’ Oktett = 200 Oktett |  |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch |  |
| recordList  Rekord 1  Rekord 2  Rekord 3  Rekord 4    Rekord 5  Rekord 6  Rekord 7    Rekord 8  Rekord 9    Rekord 8  Rekord 8 | ‘61- 09- (4F 07 D2760001448000)’  ‘61- 08- (4F 06 D27600000102)’  ‘61- 0C- (4F 0A A000000167455349474E)’  ‘61- 11- (4F 0F E828BD080FA000000167455349474E)’  ‘61- 08- (4F 06 D27600014407)’  ‘61- 08- (4F 06 D27600014408)’  ‘61- 08- (4F 06 D2760001440A)’  Fall 1: DF.QES vorhanden, AMTS\_angelegt  ´61- 08- (4F 06 D27600006601)’  ´61-08- (4F 06 D276 0001 440C)´  weitere Rekords nicht vorhanden  Fall 2: DF.QES vorhanden, AMTS\_vorbereitet  ‘61- 08- (4F 06 D27600006601)’  weitere Rekords nicht vorhanden  Fall 3: DF.QES fehlt, AMTS\_angelegt  ´61-08- (4F 06 D276 0001 440C)´  Fall 4: DF.QES fehlt, AMTS\_vorbereitet  weitere Rekords nicht vorhanden | MF, 5.3  DF.HCA, 5.4  DF.ESIGN, 5.5  DF.CIA\_ESIGN, 5.6  DF.NFD, 5.4.11 DF.DPE, 5.4.12  DF.GDD, 5.4.13  DF.QES, 6.1,  DF.AMTS, 5.4.14  DF.QES, 6.1,  DF.AMTS, 5.4.14 |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Append Record  Delete Record  Update Record | AUT\_CMS |  |
| Read Record  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Append Record  Delete Record  Update Record | AUT\_CMS |  |
| Read Record  Search Record | SmMac(SK.CAN)  AND SmRspEnc  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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem linear variablen EF arbeiten, sind: Activate, Activate Record, Append Record, Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record, Write Record.
2. Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.

### 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 K\_Initialisierung Attribute von MF / EF.GDO**

1. 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. 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 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] |  |

**⌫**

### MF / EF.Version

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

* Betriebssystem: Die "Schnittstelle" des Betriebssystems wird in [gemSpec\_COS] spezifiziert. Dabei werden der grundsätzliche Funktionsumfang und der Aufbau der Nachrichten von und 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 K\_Initialisierung: Attribute von MF / EF.Version**

1. EF.Version MUSS die in Tab\_eGK\_ObjSys\_016 dargestellten Attribute besitzen.

Tabelle 14: Tab\_eGK\_ObjSys\_016 Initialisierte Attribute von MF / EF.Version

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | linear fixes Elementary File |  |
| *fileIdentifier* | ‘2F 10’ |  |
| *shortFileIdentifier* | ‘10’= 16 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *maxNumRecords* | 4 Rekord |  |
| *maxRecordLength* | 5 Oktett |  |
| *flagRecordLCS* | False |  |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch |  |
| recordList  Rekord 1  Rekord 2  Rekord 3  Rekord 4 | ‘XX…YY’  ‘XX…YY’  ‘XX…YY’  ‘XX…YY | Rekordinhalt gemäß [gemSpec\_Karten\_Fach\_TIP] |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Read Record  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Record  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 |  |

**⌫**

1. 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

### MF / EF.Version2

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

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

Die konkrete Befüllung ist in [gemSpec\_Karten\_Fach\_TIP] beschrieben.

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

**⌦ Card-G2-A\_3231 K\_Initialisierung: Initialisierte Attribute von MF / EF.Version2**

1. 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] |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch |  |
| *body* | Inhalt gemäß [gemSpec\_Karten\_Fach\_TIP] |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Read Binary | ALWAYS |  |
| Update Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Binary | ALWAYS |  |
| Update Binary  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 |  |

**⌫**

1. 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.

### 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 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN) |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.
2. 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] |  |
| *PUK* | PUK-Wert gemäß [gemSpec\_PINPUK\_TI] | siehe [Card-G2-A\_2373] |

**⌫**

**⌦** **Card-G2-A\_2373 K\_Personalisierung: Länge der PUK für die eGK**

1. Bei der Personalisierung der eGK MUSS eine PUK mit acht Ziffern gewählt werden.
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 K\_Initialisierung: Initialisierte Attribute von MF / MRPIN.home**

1. 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  Get Pin Status  Reset RC. P1 aus der Menge {0, 1}  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Change Reference Data, P1=0  Get Pin Status  Reset RC. P1 aus der Menge {0, 1}  Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Operational state (terminated)” kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

### 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 K\_Initialisierung: Initialisierte Attribute von MF / PrK.eGK.AUT\_CVC.E256**

1. PrK.eGK.AUT\_CVC.E256 MUSS die in Tab\_eGK\_ObjSys\_020 dargestellten initialisierten Attribute besitzen.

Tabelle 19: 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} |  |
| *numberScenarion* | ‘0’ |  |
| *accessRuleSessionkeys* | irrelevant |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| General Authenticate  Internal Authenticate | ALWAYS |  |
| Generate Asymmetric Key Pair  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| General Authenticate | ALWAYS |  |
| Internal Authenticate | SmMac(SK.CAN) |  |
|  |  |  |
| Generate Asymmetric Key Pair  P1=‘81’ | SmMac(SK.CAN)  AND SmRspEnc |  |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem privaten Schlüsselobjekt (ELC) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, General Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO 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 20: Tab\_eGK\_ObjSys\_118 Personalisierte Attribute von MF / PrK.eGK.AUT\_CVC.E256

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

**⌫**

### 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.

#### 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 K\_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**

1. PuK.RCA.CS.E256 MUSS die in Tab\_eGK\_ObjSys\_023 dargestellten initialisierten Attribute besitzen.

Tabelle 21: 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.  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.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| *oid* | ecdsa-with-SHA256  ‘2A8648CE3D040302’ = {1.2.840.10045.4.3.2} |  |
| CHAT | * OIDflags = oid\_cvc\_fl\_ti * flagList = ‘FF FFFF FFFF FFC3’ | siehe Hinweis 17: |
| *accessRulesPublicSignatureVerificationObject* | Für alle Interfacearten und alle Werte von lifeCycleStatus gilt:  Delete --> AUT\_CMS  PSO Verify Certificate --> ALWAYS |  |
| *accessRulesPublicAuthenticationObject* | Für alle Interfaces und alle Werte von lifeCycleStatus gilt:  Delete --> ALWAYS  General Authenticate --> ALWAYS  External Authenticate --> ALWAYS |  |
| 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 (falls vorhanden) | | |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate.
2. Während gemäß den Tabellen in [gemSpec\_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\_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 22: 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 | * OIDflags     = oid\_cvc\_fl\_ti * 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 |  |

**⌫**

### 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 5.3.14 beschrieben.

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

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

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

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie für die asymmetrische 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 K\_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

1. PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab\_eGK\_ObjSys\_126 dargestellten initialisierten Attribute besitzen.

Tabelle 23: 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.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| CHAT | OIDflags = oid\_cvc\_fl\_cms  flagList = ‘FF BFFF FFFF FFFF’ | siehe Hinweis 19: |
| *expirationDate* | Identisch zu „expirationDate“ von PuK.RCA.CS.E256 |  |
| Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| keyIdentifier | ‘0000 0000 0000 0013‘ |  |
| lifeCycleStatus | „Operational state (activated)“ |  |
| *publicKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Domainparameter = brainpoolP256r1 | wird personalisiert |
| *oid* | ecdsa-with-SHA256  ‘2A8648CE3D040302’ = {1.2.840.10045.4.3.2} |  |
| *accessRulesPublicSignatureVerificationObject* | Für alle Interfacearten und alle Werte von lifeCycleStatus gilt:  Delete --> AUT\_CMS  PSO Verify Certificate --> ALWAYS |  |
| *accessRulesPublicAuthenticationObject* | Für alle Interfaces und alle Werte von lifeCycleStatus gilt:  Delete --> ALWAYS  General Authenticate --> ALWAYS |  |
| 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 (falls vorhanden) | | |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate, Terminate.
2. Während gemäß den Tabellen in [gemSpec\_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 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 24: 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  flagList = ‘FF BFFF FFFF FFFF’ |  |
| *expirationDate*  *Option\_Erstellung \_von\_Testkarten* | Identisch zu „expirationDate“ des personalisierten PuK.RCA.CS.E256 |  |

**⌫**

### Symmetrische Kartenadministration

Die hier beschriebene Variante der Administration 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 5.3.13 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.

#### 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 25: 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 21: |
| 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Mutual Authenticate | ALWAYS |  |
| General Authenticate | ALWAYS | siehe Hinweis 21: |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind: Activate, Deactivate, Delete, External Authenticate, General Authenticate, Get Security Status Key, Internal Authenticate, Mutual Authenticate, Terminate.
2. 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 26: 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] |  |

**⌫**

#### 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 K\_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256**

SK.CMS.AES256 MUSS die in Tab\_eGK\_ObjSys\_028 dargestellten initialisierten Attribute besitzen.

Tabelle 27: 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** | | |
| *accessRules* | identisch zu SK.CMS.AES128 |  |

**⌫**

**⌦ 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 28: 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] |  |

**⌫**

#### 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 K\_Initialisierung: Initialisierte Attribute von MF /SK.VSD.AES128**

SK.VSD.AES128 MUSS die in Tab\_eGK\_ObjSys\_029 dargestellten initialisierten Attribute besitzen.

Tabelle 29: 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** | | |
| *accessRules* | identisch zu SK.CMS.AES128 |  |

**⌫**

**⌦ 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 30: 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] |  |

**⌫**

#### 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 K\_Initialisierung: Initialisierte Attribute von MF / SK.VSD.AES256**

SK.VSD.AES256 MUSS die in Tab\_eGK\_ObjSys\_030 dargestellten initialisierten Attribute besitzen.

Tabelle 31: 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** | | |
| *accessRules* | identisch zu SK.CMS.AES128 |  |

**⌫**

**⌦ 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 32: 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] |  |

**⌫**

### 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**

1. Wird die kontaktlose Schnittstelle genutzt, dann MUSS SK.CAN vorhanden sein und die in Tab\_eGK\_ObjSys\_093 dargestellten initialisierten Attribute besitzen.

Tabelle 33: 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 |  |

**⌫**

1. 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 34: 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**

1. Bei Nutzung der kontaktlosen Schnittstelle MUSS die Personalisierung für das Attribut *can* von SK.CAN eine sechsstellige Ziffernfolge gemäß [gemSpec\_CAN\_TI] setzen.
2. **⌫**

## 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 35: 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 |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Activate | AUT\_CMS |  |
| Deactivate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| AUT\_CMS |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| 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 |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Activate | AUT\_CMS |  |
| Deactivate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| AUT\_CMS |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4 relevant.
3. 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

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

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

**⌦ Card-G2-A\_2395 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Einwilligung**

EF.Einwilligung MUSS die in Tab\_eGK\_ObjSys\_034 dargestellten initialisierten Attribute besitzen.

Tabelle 36: 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 Rekord |  |
| *maxRecordLength* | 69 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList*  *alle Rekords* | *Rekords aktiviert, Inhalt der Rekords*  *‘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  Deactivate Record | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.24]  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.2.3.4.10)])* |  |
| Read Record  Search Record | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.25]  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.2.3.4.10)])* |  |
| Update Record | PWD(PIN.CH)   AND   flagTI.27  *(informativ: OR [PWD(PIN.CH)   AND   (C.2.3.4)]* | Siehe Hinweis 27: |
| Erase Record  Delete Record | PWD(PIN.CH)   AND   flagTI.25  *(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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate Record  Deactivate Record | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)  OR   [PWD(PIN.CH)   AND   flagTI.24]  }  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.2.3.4.10)])* |  |
| Read Record  Search Record | SmMac(SK.CAN)  AND SmRspEnc  AND {   PWD(MRPIN.home)      OR   [PWD(PIN.CH)   AND   flagTI.25]  }  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.2.3.4.10)])* |  |
| Update Record | SmMac(SK.CAN)  AND SmCmdEnc  AND [PWD(PIN.CH)   AND   flagTI.27]  *(informativ: OR [PWD(PIN.CH)   AND   (C.2.3.4)])* | Siehe Hinweis 27: |
| Erase Record  Delete Record | SmMac(SK.CAN)  AND [PWD(PIN.CH)   AND   flagTI.25]  *(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 |  |

**⌫**

1. 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
2. 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.

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

Diese Datei enthält die geschützten Versichertendaten. Die Details sind in Tab\_eGK\_ObjSys\_035 beschrieben.

**⌦ Card-G2-A\_2396 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.GVD**

EF.GVD MUSS die in Tab\_eGK\_ObjSys\_035 dargestellten initialisierten Attribute besitzen.

Tabelle 37: 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)  OR [PWD(PIN.CH)   AND  flagTI.29]  OR flagTI.30  OR {AUT\_VSD}  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.7.10)*  *OR C2.3.4.5.8.9)])* |  |
| Erase Binary  Set Logical EOF  Update Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT\_CMS |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {   PWD(MRPIN.home)    OR   [PWD(PIN.CH) AND flagTI.29]    OR   flagTI.30  }  OR {AUT\_VSD}  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.7.10)*  *OR C2.3.4.5.8.9)])* |  |
| Erase Binary  Set Logical EOF  Update Binary  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 |  |

**⌫**

1. 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.

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

Diese Datei enthält Protokollierungsinformationen über Zugriffe auf die eGK.

**⌦ Card-G2-A\_2397 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Logging**

EF.Logging MUSS die in Tab\_eGK\_ObjSys\_036 dargestellten initialisierten Attribute besitzen.

Tabelle 38: 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 Rekord |  |
| *maxRecordLength* | 46 Oktett |  |
| *flagRecordLCS* | False |  |
| *recordList*  *alle Rekords* | *Rekords aktiviert, Inhalt der Rekords*  *‘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 | [PWD(PIN.CH)   AND   flagTI.31]  OR flagTI.32  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.10)*  *OR C2.3.4.5.7.8.9)])* |  |
| Read Record  Search Record | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.33]  *(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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Append Record | SmMac(SK.CAN)  AND SmCmdEnc  AND {   [PWD(PIN.CH)   AND   flagTI.31]    OR   flagTI.32  }  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.10)*  *OR C2.3.4.5.7.8.9)])* |  |
| Read Record  Search Record | SmMac(SK.CAN)  AND SmRspEnc  AND {   PWD(MRPIN.home)    OR   [PWD(PIN.CH)   AND   flagTI.33]  }  *(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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem linear variablen EF arbeiten, sind: Activate, Activate Record, Append Record, Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record, Write Record.

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

Diese Datei enthält die persönlichen Daten des Karteninhabers.

**⌦ Card-G2-A\_2398 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.PD**

EF.PD MUSS die in Tab\_eGK\_ObjSys\_037 dargestellten initialisierten Attribute besitzen.

Tabelle 39: 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  Set Logical EOF  Update Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT\_CMS |  |
| Read Binary | [SmMac(SK.CAN)  AND SmRspEnc]  OR AUT\_VSD |  |
| Erase Binary  Set Logical EOF  Update Binary  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 |  |

**⌫**

1. 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.

### MF / DF.HCA / EF.Prüfungsnachweis

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

**⌦ Card-G2-A\_2399 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Prüfungsnachweis**

EF.Prüfungsnachweis MUSS die in Tab\_eGK\_ObjSys\_038 dargestellten initialisierten Attribute besitzen.

Tabelle 40: 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  Erase Binary  Set Logical EOF  Update Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT\_CMS |  |
| Read Binary  Erase Binary  Set Logical EOF  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND SmRspEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.

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

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

**⌦ Card-G2-A\_2400 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Standalone**

EF.Standalone MUSS die in Tab\_eGK\_ObjSys\_039 dargestellten initialisierten Attribute besitzen.

Tabelle 41: 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  Erase Binary  Set Logical EOF  Update Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT\_CMS |  |
| Read Binary  Erase Binary  Set Logical EOF  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND SmRspEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. 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.

### 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 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.StatusVD**

EF.StatusVD MUSS die in Tab\_eGK\_ObjSys\_040 dargestellten initialisierten Attribute besitzen.

Tabelle 42: 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** | | |
| *accessRules* | identisch zu MF / DF.HCA / EF.PD |  |

**⌫**

### MF / DF.HCA / EF.TTN

Diese Datei enthält die Information über die Testteilnahme des Versicherten.

**⌦ Card-G2-A\_2402 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.TTN**

EF.TTN MUSS die in Tab\_eGK\_ObjSys\_041 dargestellten initialisierten Attribute besitzen.

Tabelle 43: Tab\_eGK\_ObjSys\_041 Initialisierte Attribute von MF / DF.HCA / EF.TTN

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | linear fixes Elementary File |  |
| *fileIdentifier* | ‘D0 0F’ |  |
| *shortFileIdentifier* | ‘0F’= 15 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *maxNumRecords* | 5 Rekord |  |
| *maxRecordLength* | 15 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList*  *alle Rekords* | *Rekord aktiviert, Inhalt des Rekords*  *‘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 | | |
| Delete | AUT\_CMS |  |
| Read Record | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.35]  OR flagTI.36  OR AUT\_CMS  OR AUT\_VSD  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.10)*  *OR C2.3.4.5.7.8.9)])* |  |
| Update Record | AUT\_CMS  OR 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete | AUT\_CMS |  |
| Read Record | SmMac(SK.CAN)  AND SmRspEnc  AND {   PWD(MRPIN.home)    OR   [PWD(PIN.CH)   AND   flagTI.35]    OR   flagTI.36  }  OR AUT\_CMS  OR AUT\_VSD  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.10)*  *OR C2.3.4.5.7.8.9)])* |  |
| Update Record | AUT\_CMS  OR AUT\_VSD |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. 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

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

Diese Datei enthält die Versichertendaten.

**⌦ Card-G2-A\_2403 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.VD**

EF.VD MUSS die in Tab\_eGK\_ObjSys\_042 dargestellten initialisierten Attribute besitzen.

Tabelle 44: 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** | | | |
| *accessRules* | identisch zu MF / DF.HCA / EF.PD | |  |

**⌫**

### 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 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / EF.Verweis**

EF.Verweis MUSS die in Tab\_eGK\_ObjSys\_043 dargestellten initialisierten Attribute besitzen.

Tabelle 45: 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 Rekord |  |
| *maxRecordLength* | 20 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList*  *alle Rekords* | *Rekord aktiviert, Inhalt des Rekords*  *‘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  Deactivate Record | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.24]  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.2.3.4.10))* |  |
| Read Record  Search Record  Update Record | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.28]  *(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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Activate Record  Deactivate Record | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)      OR   [PWD(PIN.CH)   AND   flagTI.24]  }  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.2.3.4.10))* |  |
| Read Record  Search Record  Update Record | SmMac(SK.CAN)  AND SmCmdEnc  AND SmRspEnc  AND {   PWD(MRPIN.home)      OR   [PWD(PIN.CH)   AND   flagTI.28]  }  *(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 |  |

**⌫**

1. 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

### Anwendung Notfalldatensatz (DF.NFD)

Diese Anwendung enthält einen Notfalldatensatz.

**⌦ Card-G2-A\_2405 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD**

DF.NFD MUSS die in Tab\_eGK\_ObjSys\_044 dargestellten initialisierten Attribute besitzen.

Tabelle 46: 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.NFD)   AND  flagTI.14]  *(informativ: [PWD(MRPIN.NFD)  AND   (C.1.10))* |
| Deactivate | [PWD(MRPIN.NFD)   AND  flagTI.14]  *(informativ: [PWD(MRPIN.NFD)  AND   (C.1.10))* |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Activate | PWD(MRPIN.NFD)   AND  flagTI.14  *(informativ: OR [PWD(MRPIN.NFD)  AND   (C.1.10))* |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| PWD(MRPIN.NFD)   AND  flagTI.14  *(informativ: OR [PWD(MRPIN.NFD)  AND   (C.1.10))* |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND [PWD (MRPIN.NFD)   AND  flagTI.14] *(informativ: OR [PWD(MRPIN.NFD)  AND   (C.1.10))* |
| Deactivate | SmMac(SK.CAN)  AND [PWD (MRPIN.NFD)   AND  flagTI.14] *(informativ: OR [PWD(MRPIN.NFD)  AND   (C.1.10))* |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Activate | SmMac(SK.CAN)  AND [PWD (MRPIN.NFD)   AND  flagTI.14]  *(informativ: [PWD(MRPIN.NFD)  AND   (C.1.10))* |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND [PWD (MRPIN.NFD)   AND  flagTI.14]  *(informativ: [PWD(MRPIN.NFD)  AND   (C.1.10))* |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.11 relevant.
3. 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

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

Diese Datei enthält einen Notfalldatensatz.

**⌦ Card-G2-A\_2406 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 47: 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  OR [PWD(MRPIN.NFD\_READ) AND flagTI.17]  *(informativ: C2.7*  *[PWD(MRPIN.NFD\_READ) AND (C.3.4.10)])* | | siehe Hinweis 39: |
| Erase Bianry  Set Logical EOF  (P1P2 = ‘90 00’)  Update Binary  Write Binary | [PWD(MRPIN.NFD)   AND   flagTI.15  *(informativ: [PWD(MRPIN.NFD) AND (C.2.10)])* | | siehe Hinweis 40: |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {   flagTI.18    OR   [PWD(MRPIN.NFD\_READ) AND flagTI.17]  }  *(informativ: C2.7*  *[PWD(MRPIN.NFD\_READ) AND (C.3.4.10)])* | | siehe Hinweis 39: |
| Erase Bianry  Set Logical EOF  (P1P2 = ‘90 00’)  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND PWD(MRPIN.NFD)   AND   flagTI.15]  *(informativ: [PWD(MRPIN.NFD) AND (C.2.10)])* | | siehe Hinweis 40: |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | |
| alle | herstellerspezifisch | |  |

**⌫**

1. 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.
2. Profil.10 kennzeichnet die Rolle einer "Umgebung zur Wahrnehmung der Rechte des Versicherten" (UzWdRdV) im Kontrollbereich eines Leistungserbringers, die zum Zugriff auf die Notfalldaten berechtigt ist. Dies ist der Unterschied zum Profil Profil.1 (E-Kiosk).
3. Das Lösch- und Schreibrecht mit Profil Profil.10 ist beschränkt auf das Wiederherstellen der Daten aus einem Backup. Diese Beschränkung ist außerhalb der eGK durchzusetzen.

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

Diese Datei enthält die Information über den Status des Notfalldatensatzes.

**⌦ Card-G2-A\_2407 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 48: 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  OR [PWD(MRPIN.NFD\_READ) AND flagTI.17]  *(informativ: OR C2.7*  *OR [PWD(MRPIN.NFD\_READ) AND (C.3.4.10)])* | | siehe Hinweis 39: |
| Erase Bianry  Set Logical EOF  (P1P2 = ’8E 00’)  Update Binary  Write Binary | [PWD(MRPIN.NFD)   AND   flagTI.15  *(informativ: OR [PWD(MRPIN.NFD) AND (C.2.10)])* | | siehe Hinweis 40: |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {   flagTI.18    OR   [PWD(MRPIN.NFD\_READ) AND flagTI.17]  }  *(informativ: OR C2.7*  *OR [PWD(MRPIN.NFD\_READ) AND (C.3.4.10)])* | | siehe Hinweis 39: |
| Erase Bianry  Set Logical EOF  (P1P2 = ’8E 00’)  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND PWD(MRPIN.NFD)   AND   flagTI.15]  *(informativ: OR [PWD(MRPIN.NFD) AND (C.2.10)])* | | siehe Hinweis 40: |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | |
| alle | herstellerspezifisch | |  |

**⌫**

#### MF / DF.HCA / DF.NFD / MRPIN.NFD

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

**⌦ Card-G2-A\_2408 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.NFD**

MRPIN.NFD MUSS die in Tab\_eGK\_ObjSys\_047 dargestellten initialisierten Attribute besitzen.

Tabelle 49: Tab\_eGK\_ObjSys\_047 Initialisierte Attribute von MF / DF.HCA / DF.NFD / 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’)  Enable Verification Requirement (P1=’0’) | ALWAYS |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| 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 | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | ALWAYS |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| 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 „Termination state“ kontaktbehaftet | | |
| andere | NEVER |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | SmMac(SK.CAN)  AND SmCmdEnc) |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | SmMac(SK.CAN)  AND SmCmdEnc) |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

#### MF / DF.HCA / DF.NFD / 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 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.NFD\_READ**

MRPIN.NFD\_READ MUSS die in Tab\_eGK\_ObjSys\_092 dargestellten initialisierten Attribute besitzen.

Tabelle 50: Tab\_eGK\_ObjSys\_092 Initialisierte Attribute von MF / DF.HCA / DF.NFD / 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 | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Change Reference Data, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

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

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

**⌦ Card-G2-A\_2410 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.DPE**

DF.DPE MUSS die in Tab\_eGK\_ObjSys\_049 dargestellten initialisierten Attribute besitzen.

Tabelle 51: 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 ist eine der beiden Varianten erlaubt |
| PWD(MRPIN.home)  OR [PWD(MRPIN.DPE)   AND   flagTI.19]  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |
| Deactivate | PWD(MRPIN.home)  OR [PWD(MRPIN.DPE)   AND   flagTI.19]  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Activate | PWD(MRPIN.home)  OR [PWD(MRPIN.DPE)   AND   flagTI.19]  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| PWD(MRPIN.home)  OR [PWD(MRPIN.DPE)   AND   flagTI.19]  *(informativ: OR [PWD(MRPIN.NFD)   AND   C.1.10])* |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.DPE)   AND   flagTI.19]  }  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |
| Deactivate | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.DPE)   AND   flagTI.19]  }  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Activate | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.DPE)   AND   flagTI.19]  }  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.DPE)   AND   flagTI.19]  }  *(informativ: OR [PWD(MRPIN.DPE)   AND   C.1.10])* |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekten in 5.4.12 relevant.
3. 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

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

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

**⌦ Card-G2-A\_2411 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 52: 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(MRPIN.DPE\_READ)   AND  flagTI.22] OR flagTI.23  OR PWD(MRPIN.home)  *(informativ: [PWD(MRPIN.DPE\_READ)   AND   (C.1.10)]*  *OR C.2*  *OR PWD(MRPIN.home)* | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’9B 00’)  Update Binary  Write Binary | PWD(MRPIN.DPE)   AND   flagTI.20  *(informativ: OR [PWD(MRPIN.DPE)   AND   (C.1.2.10)])* | |  |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {[PWD(MRPIN.DPE\_READ)   AND  flagTI.22]    OR flagTI.23    OR PWD(MRPIN.home)  }  *(informativ:[PWD(MRPIN.DPE\_READ)   AND   (C.1.10)]*  *OR C.2*  *OR PWD(MRPIN.home)* | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’9B 00’)  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND [PWD(MRPIN.DPE)   AND   flagTI.20]  *(informativ: OR [PWD(MRPIN.DPE)   AND   (C.1.2.10)])* | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | |
| alle | herstellerspezifisch | |  |

**⌫**

1. 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.

#### 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 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 53: 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(MRPIN.DPE\_READ)   AND  flagTI.22] OR flagTI.23  OR PWD(MRPIN.home)  *(informativ: [PWD(MRPIN.DPE\_READ)   AND   (C.1.10)]*  *OR C.2*  *OR PWD(MRPIN.home)* | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’98 00’)  Update Binary  Write Binary | PWD(MRPIN.DPE)   AND   flagTI.20  *(informativ: OR [PWD(MRPIN.DPE)   AND   (C.1.2.10)])* | |  |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {[PWD(MRPIN.DPE\_READ)   AND  flagTI.22]    OR flagTI.23    OR PWD(MRPIN.home)  }  *(informativ:[PWD(MRPIN.DPE\_READ)   AND   (C.1.10)]*  *OR C.2*  *OR PWD(MRPIN.home)* | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’98 00’)  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND [PWD(MRPIN.DPE)   AND   flagTI.20]  *(informativ: OR [PWD(MRPIN.DPE)   AND   (C.1.2.10)])* | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | |
| alle | herstellerspezifisch | |  |

**⌫**

#### MF / DF.HCA / DF.DPE / MRPIN.DPE

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

**⌦ Card-G2-A\_2413 K\_ K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.DPE / MRPIN.DPE**

MRPIN.DPE MUSS die in Tab\_eGK\_ObjSys\_052 dargestellten initialisierten Attribute besitzen.

Tabelle 54: Tab\_eGK\_ObjSys\_052 Initialisierte Attribute von MF / DF.HCA / DF.DPE / 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’)  Enable Verification Requirement (P1=’0’) | ALWAYS |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Reset RC. P1 aus der Menge {0, 1}  Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | ALWAYS |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Reset RC. P1 aus der Menge {0, 1}  Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | SmMac(SK.CAN)  AND SmCmdEnc) |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1}  Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | SmMac(SK.CAN)  AND SmCmdEnc) |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1}  Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

#### MF / DF.HCA / DF.DPE / MRPIN.DPE\_READ

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

**⌦ Card-G2-A\_3232 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.DPE\_READ**

MRPIN.DPE\_READ MUSS die in Tab\_eGK\_ObjSys\_180 dargestellten initialisierten Attribute besitzen.

Tabelle 55: Tab\_eGK\_ObjSys\_180 Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.DPE\_READ

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Multireferenz Passwortobjekt |  |
| *pwdIdentifier* | ‘08’ = 8 |  |
| *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 | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Change Reference Data, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

### Anwendung Gesundheitsdatendienst (GDD)

Diese Anwendung enthält Daten zum Gesundheitsdatendienst des Versicherten.

**⌦ Card-G2-A\_2415 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.GDD**

DF.GDD MUSS die in Tab\_eGK\_ObjSys\_054 dargestellten initialisierten Attribute besitzen.

Tabelle 56: 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)  OR [PWD(MRPIN.GDD)   AND   flagTI.39]  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |
| Deactivate | PWD(MRPIN.home)  OR [PWD(MRPIN.GDD)   AND   flagTI.39]  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Activate | PWD(MRPIN.home)  OR [PWD(MRPIN.GDD)   AND   flagTI.39]  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| PWD(MRPIN.home)  OR [PWD(MRPIN.GDD)   AND   flagTI.39]  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.GDD)   AND   flagTI.39]  }  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |
| Deactivate | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.GDD)   AND   flagTI.39]  }  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Activate | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.GDD)   AND   flagTI.39]  }  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.GDD)   AND   flagTI.39]  }  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.10)])* |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.13 relevant.
3. 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

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

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

**⌦ Card-G2-A\_2416 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 57: 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 Rekord |  |
| *maxRecordLength* | 60 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList* | 17 Records aktiviert, Inhalt der Rekords  '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  Erase Record  Delete Record  Read Record  Search Record  Update Record | PWD(MRPIN.home)  OR [PWD(MRPIN.GDD)   AND  flagTI.40]  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.2.3.4.10)])* | siehe Hinweis 53: |
| 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Append Record  Erase Record  Delete Record  Read Record  Search Record  Update Record | SmMac(SK.CAN)  AND SmCmdEnc  AND SmRspEnc  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.GDD)   AND  flagTI.40]  }  *(informativ: OR [PWD(MRPIN.GDD)   AND   (C.1.2.3.4.10)])* | siehe Hinweis 53: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem linear variablen EF arbeiten, sind: Activate, Activate Record, Append Record, Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record, Write Record.
2. 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 MRPIN.GDD verlangt.

#### 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 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 58: 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 Rekord |  |
| *maxRecordLength* | 60 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList* | 17 Records aktiviert, Inhalt der Rekords  '000000e164f0467ffe5d379d0b8bb7cb232302ecd446eee98852d785614ef5f0acdb23' |  |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch |  |
| *accessRules* | identisch zu MF / DF.HCA / DF.GDD / EF.EinwilligungGDD |  |

**⌫**

#### MF / DF.HCA / DF.GDD / MRPIN.GDD

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

**⌦ Card-G2-A\_2417 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.GDD / MRPIN.GDD**

MRPIN.GDD MUSS die in Tab\_eGK\_ObjSys\_056 dargestellten initialisierten Attribute besitzen.

Tabelle 59: Tab\_eGK\_ObjSys\_056 Initialisierte Attribute von MF / DF.HCA / DF.GDD / 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’)  Enable Verification Requirement (P1=’0’) | ALWAYS |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| 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 | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | ALWAYS |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| 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 „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | SmMac(SK.CAN)  AND SmCmdEnc) |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Disable Verification Requirement (P1=’0’)  Enable Verification Requirement (P1=’0’) | SmMac(SK.CAN)  AND SmCmdEnc) |  |
| Disable Verification Requirement (P1=’1’)  Enable Verification Requirement (P1=’1’) | NEVER |  |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

### Anwendung Organspendeerklärung (DF.OSE)

Diese Anwendung enthält die Daten zur Organspendeerklärung.

**⌦ Card-G2-A\_3233 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.OSE**

DF.OSE MUSS die in Tab\_eGK\_ObjSys\_184 dargestellten initialisierten Attribute besitzen.

Tabelle 60: 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 ist eine der beiden Varianten erlaubt |
| PWD(MRPIN.home)  OR [PWD(MRPIN.OSE) AND flagTI.44] |
| Deactivate | PWD(MRPIN.home)  OR [PWD(MRPIN.OSE) AND flagTI.44] |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Activate | [PWD(MRPIN.home)  OR [PWD(MRPIN.OSE) AND flagTI.44] |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| PWD(MRPIN.home)  OR [PWD(MRPIN.OSE) AND flagTI.44] |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | Herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.OSE))   AND   flagTI.44]  } |
| Deactivate | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.OSE))   AND   flagTI.44]  } |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Activate | SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.OSE))   AND   flagTI.44]  } |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {   PWD(MRPIN.home)    OR   [PWD(MRPIN.OSE))   AND   flagTI.44]  } |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.14 relevant.
3. 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

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

Diese Datei enthält einen Datensatz zur Organspendeerklärung.

**⌦ Card-G2-A\_3234 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 61: 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  OR [PWD(MRPIN.OSE AND flagTI.41]  OR PWD(MRPIN.home)] | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’81 00’)  Update Binary  Write Binary | [PWD(MRPIN.OSE)   AND   flagTI.43] | |  |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {flagTI. 42  OR [PWD(MRPIN.OSE AND flagTI. 41]  OR PWD(MRPIN.home)]} | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’81 00’)  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND [PWD(MRPIN.OSE)   AND   flagTI. 43] | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | |
| alle | herstellerspezifisch | |  |

**⌫**

1. 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.

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

Diese Datei enthält die Information über den Status der Organspendeerklärung.

**⌦ Card-G2-A\_3235 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 62: 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  OR [PWD(MRPIN.OSE AND flagTI.41]  OR PWD(MRPIN.home)] | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’82 00’)  Update Binary  Write Binary | [PWD(MRPIN.OSE)   AND   flagTI.43] | |  |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {flagTI. 42  OR [PWD(MRPIN.OSE AND flagTI. 41]  OR PWD(MRPIN.home)]} | |  |
| Erase Bianry  Set Logical EOF  (P1P2 = ’82 00’)  Update Binary  Write Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND [PWD(MRPIN.OSE)   AND   flagTI. 43] | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |

**⌫**

#### MF / DF.HCA / DF.OSE / 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 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.OSE / MRPIN.OSE**

MRPIN.OSE MUSS die in Tab\_eGK\_ObjSys\_187 dargestellten initialisierten Attribute besitzen.

Tabelle 63: Tab\_eGK\_ObjSys\_187 Initialisierte Attribute von MF / DF.HCA / DF.OSE / 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 | | |
| 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 „Termination state“ kontaktbehaftet | | |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

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

### Anwendung AMTS Datenmanagement (DF.AMTS), (AMTS\_angelegt)

Diese Anwendung enthält die Daten zum AMTS Datenmanagement.und ist mit den im Folgenden beschriebenen Objekten angelegt, wenn die Variante AMTS\_angelegt umgesetzt wird.

**⌦ Card-G2-A\_3240 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS (AMTS\_angelegt)**

DF.AMTS MUSS die in Tab\_eGK\_ObjSys\_189 dargestellten initialisierten Attribute besitzen.

Tabelle 64: 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]  OR PWD(MRPIN.home) |
| Deactivate | [PWD(MRPIN.AMTS) AND flagTI.45]  OR PWD(MRPIN.home) |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Activate | [PWD(MRPIN.AMTS) AND flagTI.45]  OR PWD(MRPIN.home) |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| [PWD(MRPIN.AMTS) AND flagTI.45]  OR PWD(MRPIN.home) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| alle | Herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {[PWD(MRPIN.AMTS) AND flagTI.45]  OR  PWD(MRPIN.home)  } |
| Deactivate | SmMac(SK.CAN)  AND {[PWD(MRPIN.AMTS) AND flagTI.45]  OR  PWD(MRPIN.home)  } |  |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Activate | SmMac(SK.CAN)  AND {[PWD(MRPIN.AMTS) AND flagTI.45]  OR  PWD(MRPIN.home)  } |  |
| Deactivate | NEVER | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| SmMac(SK.CAN)  AND {[PWD(MRPIN.AMTS) AND flagTI.45]  OR  PWD(MRPIN.home)  } |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**



Abbildung 7: Abb\_eGK\_ObjSys\_011 Dateistruktur der Anwendung AMTS Datenmanagement

#### MF / DF.HCA / DF.AMTS / EF.EinwilligungAMTS (AMTS\_angelegt)

Diese Datei enthält die Information über die Einwilligungen zur freiwilligen Anwendung AMTS Datenmanagement.

**⌦ Card-G2-A\_3241 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.EinwilligungAMTS (AMTS\_angelegt)**

EF.EinwilligungAMTS MUSS die in Tab\_eGK\_ObjSys\_190 dargestellten initialisierten Attribute besitzen.

Tabelle 65: Tab\_eGK\_ObjSys\_190 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.EinwilligungAMTS

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | linear variables Elementary File |  |
| *fileIdentifier* | ´E0 04´ |  |
| *shortFileIdentifier* | ’04’ = 4 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *numberOfOctet* | ´00CF´ Oktett = 207 Oktett |  |
| *maxNumRecords* | 3 Rekord |  |
| *maxRecordLength* | 69 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList* | alle Rekords aktiviert, drei Rekords vorhanden, Inhalt jedes Rekords: ‘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  Search Record | PWD(MRPIN.home)  OR [PWD(MRPIN.AMTS)   AND  flagTI.46]  OR [PWD(PIN.AMTS\_REP)   AND  flagTI.46] |  |
| Append Record  Erase Record  Delete Record  Update Record | [PWD(MRPIN.AMTS)   AND  flagTI.47] |  |
| 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Record  Search Record | SmMac(SK.CAN)  AND SmCmdEnc  AND SmRspEnc  AND {  PWD(MRPIN.home)    OR [PWD(MRPIN.AMTS)   AND  flagTI.46]    OR [PWD(PIN.AMTS\_REP)   AND  flagTI.46] } |  |
| Append Record  Erase Record  Delete Record  Update Record | SmMac(SK.CAN)  AND SmCmdEnc  AND [PWD(MRPIN.AMTS)   AND  flagTI.47] |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

#### MF / DF.HCA / DF.AMTS / EF.AMTS (AMTS\_angelegt)

Diese Datei enthält einen Datensatz zum AMTS Datenmanagement.

**⌦ Card-G2-A\_3244 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.AMTS (AMTS\_angelegt)**

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* | | ´34 F8´ Oktett = 13.560 Oktett |  |
| *positionLogicalEndOfFile* | | ´34 F8´ | 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] | |  |
| Erase Binary  Update Binary | [PWD(MRPIN.AMTS)   AND   flagTI.47]  OR [PWD(PIN.AMTS\_REP)   AND   flagTI.47] | |  |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {  [PWD(MRPIN.AMTS**)** AND flagTI.46]  OR [PWD(PIN.AMTS\_REP**)** AND flagTI.46]  } | |  |
| Erase Binary  Update Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND {  [PWD(MRPIN.AMTS)   AND   flagTI.47]  OR [PWD(PIN.AMTS\_REP)   AND   flagTI.47]  } | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | |
| alle | herstellerspezifisch | |  |

**⌫**

#### MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS (AMTS\_angelegt)

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 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS (AMTS\_angelegt)**

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 Rekord |  |
| *maxRecordLength* | 120 Oktett |  |
| *flagRecordLCS* | True |  |
| *recordList* | alle Rekords aktiviert, fünf Rekords vorhanden, Inhalt jedes Rekords: ‘00’ |  |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch |  |
| *accessRules* | identisch zu MF / DF.HCA / DF.AMTS / EF.EinwilligungAMTS |  |

**⌫**

#### MF / DF.HCA / DF.AMTS / EF.StatusAMTS (AMTS\_angelegt)

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

**⌦ Card-G2-A\_3246 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.StatusAMTS (AMTS\_angelegt)**

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] | |  |
| Update Binary | [PWD(MRPIN.AMTS)   AND   flagTI.47]  OR [PWD(PIN.AMTS\_REP)   AND   flagTI.47] | |  |
| 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 (falls vorhanden) | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | |
| Delete | AUT\_CMS | |  |
| Read Binary | SmMac(SK.CAN)  AND SmRspEnc  AND {  [PWD(MRPIN.AMTS**)** AND flagTI.46]  OR [PWD(PIN.AMTS\_REP) AND flagTI.46]  } | |  |
| Update Binary | SmMac(SK.CAN)  AND SmCmdEnc  AND {  [PWD(MRPIN.AMTS)   AND   flagTI.47]  OR [PWD(PIN.AMTS\_REP)   AND   flagTI.47]  } | |  |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | |
| alle | NEVER | |  |

**⌫**

#### MF / DF.HCA / DF.AMTS / MRPIN.AMTS (AMTS\_angelegt)

Dieses Multireferenz-Passwortobjekt wird zur Freischaltung von Inhalten der Anwendung AMTS Datenmanagement verwendet. Dieses Multireferenz-Passwortobjekt kann nicht abgeschaltet werden.

**⌦ Card-G2-A\_3247 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / MRPIN.AMTS (AMTS\_angelegt)**

MRPIN.AMTS MUSS die in Tab\_eGK\_ObjSys\_194 dargestellten initialisierten Attribute besitzen.

Tabelle 69: Tab\_eGK\_ObjSys\_194 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / 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 | | |
| 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 | | |
| 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 „Termination state“ kontaktbehaftet | | |
| Alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN) |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Change RD, P1=0 | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac(SK.CAN) |  |
| Reset RC. P1 aus der Menge {0, 1} | SmMac(SK.CAN)  AND SmCmdEnc |  |
| Verify | SmMac(SK.CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Alle | herstellerspezifisch |  |

**⌫**

#### MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP (AMTS\_angelegt)

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 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP (AMTS\_angelegt)**

PIN.AMTS\_REP MUSS die in Tab\_eGK\_ObjSys\_195 dargestellten initialisierten Attribute besitzen.

Tabelle 70: Tab\_eGK\_ObjSys\_195 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / 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 (MRPIN.AMTS) |  | |
| Get Pin Status | | ALWAYS |  | |
| Reset RC. P1=´02´ | | PWD (MRPIN.AMTS) |  | |
| Verify | | 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 (falls vorhanden) | | | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | | | |
| Change RD, P1=´01´ | | SmMac(SK.CAN)  AND SmCmdEnc  AND PWD(MRPIN.AMTS) |  | |
| Get Pin Status | | SmMac(SK.CAN) |  | |
| Reset RC. P1=´02´ | | SmMac(SK.CAN)  AND SmCmdEnc  AND PWD (MRPIN.AMTS) |  | |
| Verify | | SmMac(SK.CAN)  AND SmCmdEnc |  | |
| andere | | NEVER |  | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | | | |
| alle | | NEVER |  | |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | | | |
| alle | | herstellerspezifisch |  | |

**⌫**

**⌦ Card-G2-A\_3249 K\_Personalisierung: Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP (AMTS\_angelegt)**

Bei der Personalisierung von PIN.AMTS\_REP MÜSSEN die in Tab\_eGK\_ObjSys\_196 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 71: Tab\_eGK\_ObjSys\_196 Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |

**⌫**

**⌦ Card-G2-A\_3335 K\_Personalisierung: Option des PIN-Brief-Versands für MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP (AMTS\_angelegt)**

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.

**⌫**

#### MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256 (AMTS\_angelegt)

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

**⌦ Card-G2-A\_3263 K\_Initialisierung: Initialisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256 (AMTS\_angelegt)**

PrK.AMTS.ENC.E256 MUSS die in Tab\_eGK\_ObjSys\_197 dargestellten Werte besitzen.

Tabelle 72: 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  PSO Transcipher | [PWD(MRPIN.AMTS) AND flagTI.46]  OR [PWD(PIN.AMTS\_REP) AND flagTI.46] |  |
| Generate Asymmetric Key Pair  mit P1 = ´81´ | [PWD(MRPIN.AMTS) AND (flagTI.46 OR flagTI.47)]  OR [PWD(PIN.AMTS\_REP) AND (flagTI.46 OR flagTI.47)] |  |
| Generate Asymmetric Key Pair  mit P1 = ´C0´ | PWD(MRPIN.AMTS) AND flagTI.47 |  |
| 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Decipher  PSO Transcipher | SmMac(CAN)  AND SmRspEnc  AND {  [PWD(MRPIN.AMTS) AND flagTI.46]  OR [PWD(PIN.AMTS\_REP) AND flagTI.46]  } |  |
| Generate Asymmetric Key Pair  mit P1 = ´81´ | SmMac(CAN)  AND SmRspEnc  AND {  [PWD(MRPIN.AMTS) AND (flagTI.46 OR flagTI.47)]  OR [PWD(PIN.AMTS\_REP) AND (flagTI.46 OR flagTI.47)]  } |  |
| Generate Asymmetric Key Pair  mit P1 = ´C0´ | SmMac(CAN)  AND SmRspEnc  AND {  PWD(MRPIN.AMTS) AND flagTI.47  } |  |
| 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 K\_Personalisierung: Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256 (AMTS\_angelegt)**

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 73: 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 |  |

**⌫**

## 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 74: 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 |  |
| 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Load Application | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier ist in [EN14890–1] festgelegt.
3. 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

### 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 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 75: 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  Erase Binary  Set Logical EOF  Update Binary  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete  Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_CMS |  |
| Read Binary | SmMac (CAN)  AND SmRspEnc  OR AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. 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 K\_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048**

Bei der Initialisierung von EF.C.CH.AUT.R2048 MÜSSEN die in Tab\_eGK\_ObjSys\_146 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 76: 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 |  |

**⌫**

### 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 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 77: 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* | *‘0*7 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  Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_CMS |  |
| Read Binary | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.8]  OR flagTI.9  OR AUT\_CMS  *(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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete  Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_CMS |  |
| Read Binary | SmMac (CAN)  AND SmRspEnc  AND {   PWD(MRPIN.home)    OR   [PWD(PIN.CH)   AND   flagTI.8]    OR   flagTI.9  }  OR AUT\_CMS  *(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 |  |

**⌫**

1. 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 78: 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 |  |

**⌫**

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

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.ENC1.R2048 zu PrK.CH.ENC.R2048 (siehe 5.5.7).

**⌦ Card-G2-A\_2427 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 79: 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Read Binary | SmMac (CAN)  AND SmRspEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. 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 80: 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 |  |

**⌫**

### 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 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 81: 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  Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_CMS |  |
| Read Binary | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.10]  OR flagTI.11  OR AUT\_CMS  *(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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Delete  Erase Binary  Set Logical EOF  Update Binary  Write Binary | AUT\_CMS |  |
| Read Binary | SmMac (CAN)  AND SmRspEnc  AND {   PWD(MRPIN.home)    OR   [PWD(PIN.CH)   AND   flagTI.10]    OR   flagTI.11  }  OR AUT\_CMS  *(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 |  |

**⌫**

1. 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 82: 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 |  |

**⌫**

### 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 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 83: 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, sign9796\_2\_DS2, signPSS} |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Internal Authenticate  PSO Comp Digital Sig. | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND flagTI.12]  *(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.9.10)])* |  |
| Generate Asymmetric Key Pair  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Internal Authenticate  PSO Comp Digital Sig. | SmMac (CAN)  AND {PWD(MRPIN.home)    OR [PWD(PIN.CH)   AND flagTI.12]  }  *(informativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.9.10)])* |  |
| Generate Asymmetric Key Pair  P1=‘81’ | SmMac(SK.CAN)  AND SmRspEnc |  |
| Delete | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO 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 84: 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 |  |

**⌫**

### 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 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 85: 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, sign9796\_2\_DS2, signPSS} |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Internal Authenticate  PSO Comp Digital Sig. | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.8]  OR flagTI.9  *(informativ: OR [PWD(PIN.CH) AND (C.1.10)]*  *OR C.2.3.4.5.8.9)* |  |
| Generate Asymmetric Key Pair  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Internal Authenticate  PSO Comp Digital Sig. | SmMac (CAN)  AND { PWD(MRPIN.home)    OR [PWD(PIN.CH)   AND   flagTI.8]    OR flagTI.9  }  *(informativ: OR [PWD(PIN.CH) AND (C.1.10)]*  *OR C.2.3.4.5.8.9)* |  |
| Generate Asymmetric Key Pair  P1=‘81’ | SmMac(SK.CAN)  AND SmRspEnc |  |
| Delete | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO 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 86: Tab\_eGK\_ObjSys\_159 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048

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

**⌫**

### 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 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 87: 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, rsaDecipherPKCS1\_V1\_5} |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| PSO Decipher  PSO Transcipher | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.13]  *(alternativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.10)])* |  |
| Generate Asymmetric Key Pair  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Decipher  PSO Transcipher | SmMac (CAN)  AND SmCmdEnc  AND SmRspEnc  AND { PWD(MRPIN.home)    OR [PWD(PIN.CH)   AND   flagTI.13]  }  *(alternativ: OR [PWD(PIN.CH) AND (C.1.2.3.4.5.10)])* |  |
| Generate Asymmetric Key Pair  P1=‘81’ | SmMac(SK.CAN)  AND SmRspEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO 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 88: Tab\_eGK\_ObjSys\_162 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048

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

**⌫**

### 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 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 89: 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, rsaDecipherPKCS1\_V1\_5} |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| PSO Decipher  PSO Transcipher | PWD(MRPIN.home)  OR [PWD(PIN.CH)   AND   flagTI.10]  OR flagTI.11  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.9.10)]*  *OR C.2.3.5)* |  |
| Generate Asymmetric Key Pair  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| PSO Decipher  PSO Transcipher | SmMac (CAN)  AND SmCmdEnc  AND SmRspEnc  AND { PWD(MRPIN.home)    OR [PWD(PIN.CH)   AND   flagTI.10]    OR flagTI.11  }  *(informativ: OR [PWD(PIN.CH)   AND   (C.1.9.10)]*  *OR C.2.3.5)* |  |
| Generate Asymmetric Key Pair  P1=‘81’ | SmMac(SK.CAN)  AND SmRspEnc |  |
| Delete | AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO 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 90: Tab\_eGK\_ObjSys\_168 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048

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

**⌫**

## Beschreibung kryptographischer Objekte, CIA\_ESIGN

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

Im Fall der eGK enthält die hier beschriebene Anwendung nur EF.CIA\_Info, das den Pro­file Identifier bereitstellt, welcher auf [DIN66291-4] verweist. Mit diesem Profile Identifier wird der Außenwelt mitgeteilt, dass alle FIDs, Schlüssel-IDs etc. in [DIN66291-4] definiert sind. Ein EF.OD ist folglich nicht nötig.

**⌦ Card-G2-A\_2452 K\_Initialisierung: Initialisierte Attribute von MF / DF.CIA\_ESIGN**

DF.CIA\_ESIGN MUSS die in Tab\_eGK\_ObjSys\_079 dargestellten initialisierten Attribute besitzen.

Tabelle 91: Tab\_eGK\_ObjSys\_079 Initialisierte Attribute von MF / DF.CIA\_ESIGN

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘E828BD080F A000000167455349474E’ | siehe Hinweis 72: |
| *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 |
| alle | 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 |  |
| andere | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [ISO7816-15] sowie als PIX den applicationIdentifier von DF.ESIGN (siehe Tab\_eGK\_ObjSys\_059).
3. Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im 5.6 nicht berücksichtigt zu werden.



Abbildung 9: Abb\_eGK\_ObjSys\_007 Objektstruktur der Anwendung DF.CIA.ESIGN

### MF / DF.CIA\_ESIGN / EF.CIA\_Info

Die Datei EF.CIA\_Info enthält die Versionsangabe der CIO–Beschreibung und die Kennung des referenzierten Profils.

**⌦ Card-G2-A\_2453 K\_Initialisierung: Initialisierte Attribute von MF / DF.CIA\_ESIGN / EF.CIA\_Info**

EF.CIA\_Info MUSS die in Tab\_eGK\_ObjSys\_080 dargestellten initialisierten Attribute besitzen.

Tabelle 92: Tab\_eGK\_ObjSys\_080 Initialisierte Attribute von MF / DF.CIA\_ESIGN / EF.CIA\_Info

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘50 32’ | siehe Hinweis 74: |
| *shortFileIdentifier* | ‘12’= 18 | siehe Hinweis 74: |
| *numberOfOctet* | ‘0017’ Oktett = 23 Oktett |  |
| *positionLogical EndOfFile* | ‘0017’ Oktett = 23 Oktett |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True, falls Option\_logische\_Kanäle vorhanden ist, sonst herstellerspezifisch |  |
| *body* | ‘30 15  | 02 01 01  | 03 01 00  | a6 0d  | | 0c 0b 44494e2056203636323931’ | siehe Hinweis 76:  Version = 1  keine cardFlags  profilIndication  UTF8: „DIN V 66291“ |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | SmMac (CAN)  AND SmRspEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Update Binary, Set Logical Eof, Terminate, Write Binary.
2. Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.
3. ASN.1 Werte: ciaInfoExample CardInfo ::= {   
     version v2,   
     cardflags {   },   
     profileIndication {   
     "DIN V 66291"   
     }   
     }

# 

# 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 \_005) 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 bzw. bestätigungsfähig nach Signaturgesetz 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.

**⌫**

## 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 93: 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: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Load Application | herstellerspezifisch | sieheHinweis 79: |
| 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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind: Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.
2. Der Wert des Attributes applicationIdentifier ist in [DIN66291-4] festgelegt.
3. 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.
4. Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im 6.1 nicht berücksichtigt werden.



Abbildung 10: Abb\_eGK\_ObjSys\_009 Objektstruktur der vollständigen Signaturanwendung DF.QES

### 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 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 94: 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 83: |
| *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 81: |
| Read Binary | ALWAYS |  |
| Update Binary | herstellerspezifisch | sieheHinweis 81: |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | herstellerspezifisch | sieheHinweis 81: |
| Read Binary | SmMac (CAN)  AND SmRspEnc |  |
| Update Binary | herstellerspezifisch | sieheHinweis 81: |
| 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 |  |

**⌫**

1. 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.
2. 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.
3. 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 95: 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 |  |

**⌫**

### 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 K\_Initialisierung: Initialisierte Attribute von MF / DF.QES / PIN.QES**

PIN.QES MUSS die in Tab\_eGK\_ObjSys\_088 dargestellten initialisierten Attribute besitzen.

Tabelle 96: 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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=0 | SmMac (CAN)  AND SmCmdEnc |  |
| Get Pin Status | SmMac (CAN)  AND SmCmdEnc |  |
| Reset RC. P1 = 1 | SmMac (CAN)  AND SmCmdEnc |  |
| Verify | SmMac (CAN)  AND SmCmdEnc |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

**⌫**

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

**⌦ Card-G2-A\_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 97: Tab\_eGK\_ObjSys\_177 Personalisierte Attribute von MF / DF.QES / PIN.QES

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | Wird gegebenenfalls personalisiert, siehe Hinweis 85: |
| *PUK* | PUK-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |

**⌫**

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

### MF / DF.QES / 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 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 98: 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 87: |
| *privateKey* | hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | True |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  {sign9796\_2\_DS2, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln für die Kontaktschnittstelle | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  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 (falls vorhanden) | | |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktlos | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘81’ | SmMac(SK.CAN)  AND SmRspEnc |  |
| PSO Comp Dig Sig | SmMac (CAN)  AND SmCmdEnc  AND SmRspEnc  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 |  |

**⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: Activate; Deactivate; Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, Terminate.
2. 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 99: Tab\_eGK\_ObjSys\_178 Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048

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

**⌫**

## 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.

1. – Verzeichnisse

A1 – Abkürzungen

| **Kürzel** | **Erläuterung** |
| --- | --- |
| AID | Application Identifier |
| BCD | Binary Coded Decimal |
| BER | Basic Encoding Rules |
| CAN | Card Access Number |
| CMS | Card Management System, System zur Administration von Karten und Applikationen |
| CHAT | Certificate Holder Autorisation Template 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, 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 |

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

[Abbildung 1: Abb\_eGK\_ObjSys\_001 Objektstruktur einer eGK auf oberster Ebene 21](#_Toc465414243)

[Abbildung 2: Abb\_eGK\_ObjSys\_002 Dateistruktur der Gesundheitsanwendung 47](#_Toc465414244)

[Abbildung 3: Abb\_eGK\_ObjSys\_003 Dateistruktur der Anwendung Notfalldatensatz 60](#_Toc465414245)

[Abbildung 4: Abb\_eGK\_ObjSys\_004 Dateistruktur der Anwendung Datensatz Persönliche Erklärungen 67](#_Toc465414246)

[Abbildung 5: Abb\_eGK\_ObjSys\_005 Dateistruktur der Anwendung Gesundheitsdatendienst 75](#_Toc465414247)

[Abbildung 6: Abb\_eGK\_ObjSys\_010 Dateistruktur der Anwendung Organspendeerklärung 80](#_Toc465414248)

[Abbildung 7: Abb\_eGK\_ObjSys\_011 Dateistruktur der Anwendung AMTS Datenmanagement 86](#_Toc465414249)

[Abbildung 8: Abb\_eGK\_ObjSys\_006 Objektstruktur der Anwendung DF.ESIGN 96](#_Toc465414250)

[Abbildung 9: Abb\_eGK\_ObjSys\_007 Objektstruktur der Anwendung DF.CIA.ESIGN 110](#_Toc465414251)

[Abbildung 10: Abb\_eGK\_ObjSys\_009 Objektstruktur der vollständigen Signaturanwendung DF.QES 114](#_Toc465414252)

A4 – Tabellenverzeichnis

[Tabelle 1 Tab\_eGK\_ObjSys\_001: Zuordnung der Bezeichnungen für PINs 10](#_Toc465414253)

[Tabelle 2 Tab\_eGK\_ObjSys\_002: Liste der Komponenten, an welche dieses Dokument Anforderungen stellt 11](#_Toc465414254)

[Tabelle 3: Tab\_eGK\_ObjSys\_004 ATR-Codierung 20](#_Toc465414255)

[Tabelle 4: Tab\_eGK\_ObjSys\_006 Initialisierte Attribute von MF 21](#_Toc465414256)

[Tabelle 5: Tab\_eGK\_ObjSys\_007 Initialisierte Attribute von MF / EF.ATR 22](#_Toc465414257)

[Tabelle 6: Tab\_eGK\_ObjSys\_106 Initialisierte Attribute von MF / EF.CardAccess 23](#_Toc465414258)

[Tabelle 7: Tab\_eGK\_ObjSys\_009 Initialisierte Attribute von MF / EF.C.CA\_eGK.CS.E256 24](#_Toc465414259)

[Tabelle 8: Tab\_eGK\_ObjSys\_110 Personalisierte Attribute von MF / EF.C.CA\_eGK.CS.E256 25](#_Toc465414260)

[Tabelle 9: Tab\_eGK\_ObjSys\_012 Initialisierte Attribute von MF/EF.C.eGK.AUT\_CVC.E256 26](#_Toc465414261)

[Tabelle 10: Tab\_eGK\_ObjSys\_112 Personalisierte Attribute von MF / EF.C.eGK.AUT\_CVC.E256 26](#_Toc465414262)

[Tabelle 11: Tab\_eGK\_ObjSys\_014 Initialisierte Attribute von MF / EF.DIR 27](#_Toc465414263)

[Tabelle 12: Tab\_eGK\_ObjSys\_015 Initialisierte Attribute von MF / EF.GDO 28](#_Toc465414264)

[Tabelle 13: Tab\_eGK\_ObjSys\_182 Personalisiertes Attribut von MF / EF.GDO 29](#_Toc465414265)

[Tabelle 14: Tab\_eGK\_ObjSys\_016 Initialisierte Attribute von MF / EF.Version 29](#_Toc465414266)

[Tabelle 15: Tab\_eGK\_ObjSys\_183 Initialisierte Attribute von MF / EF.Version2 31](#_Toc465414267)

[Tabelle 16: Tab\_eGK\_ObjSys\_017 Initialisierte Attribute von MF / PIN.CH 32](#_Toc465414268)

[Tabelle 17: Tab\_eGK\_ObjSys\_117 Personalisierte Attribute von MF / PIN.CH 33](#_Toc465414269)

[Tabelle 18: Tab\_eGK\_ObjSys\_018 Initialisierte Attribute von MF / MRPIN.home 33](#_Toc465414270)

[Tabelle 19: Tab\_eGK\_ObjSys\_020 Initialisierte Attribute von MF / PrK.eGK.AUT\_CVC.E256 34](#_Toc465414271)

[Tabelle 20: Tab\_eGK\_ObjSys\_118 Personalisierte Attribute von MF / PrK.eGK.AUT\_CVC.E256 35](#_Toc465414272)

[Tabelle 21: Tab\_eGK\_ObjSys\_023 Initialisierte Attribute von MF / PuK.RCA.CS.E256 36](#_Toc465414273)

[Tabelle 22: Tab\_eGK\_ObjSys\_188 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten 37](#_Toc465414274)

[Tabelle 23: Tab\_eGK\_ObjSys\_126 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 39](#_Toc465414275)

[Tabelle 24: Tab\_eGK\_ObjSys\_121 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 40](#_Toc465414276)

[Tabelle 25: Tab\_eGK\_ObjSys\_027 Initialisierte Attribute von MF / SK.CMS.AES128 41](#_Toc465414277)

[Tabelle 26: Tab\_eGK\_ObjSys\_122 Personalisierte Attribute von MF / SK.CMS.AES128 42](#_Toc465414278)

[Tabelle 27: Tab\_eGK\_ObjSys\_028 Initialisierte Attribute von MF / SK.CMS.AES256 42](#_Toc465414279)

[Tabelle 28: Tab\_eGK\_ObjSys\_123 Personalisierte Attribute von MF / SK.CMS.AES256 43](#_Toc465414280)

[Tabelle 29: Tab\_eGK\_ObjSys\_029 Initialisierte Attribute von MF / SK.VSD.AES128 43](#_Toc465414281)

[Tabelle 30: Tab\_eGK\_ObjSys\_124 Personalisierte Attribute von MF / SK.VSD.AES128 44](#_Toc465414282)

[Tabelle 31: Tab\_eGK\_ObjSys\_030 Initialisierte Attribute von MF / SK.VSD.AES256 44](#_Toc465414283)

[Tabelle 32: Tab\_eGK\_ObjSys\_125 Personalisierte Attribute von MF / SK.VSD.AES256 45](#_Toc465414284)

[Tabelle 33: Tab\_eGK\_ObjSys\_093 Initialisierte Attribute von MF / SK.CAN 45](#_Toc465414285)

[Tabelle 34: Tab\_eGK\_ObjSys\_181 Personalisierte Attribute von MF / SK.CAN 46](#_Toc465414286)

[Tabelle 35: Tab\_eGK\_ObjSys\_033 Initialisierte Attribute von MF / DF.HCA 46](#_Toc465414287)

[Tabelle 36: Tab\_eGK\_ObjSys\_034 Initialisierte Attribute von MF / DF.HCA / EF.Einwilligung 48](#_Toc465414288)

[Tabelle 37: Tab\_eGK\_ObjSys\_035 Initialisierte Attribute von MF / DF.HCA / EF.GVD 49](#_Toc465414289)

[Tabelle 38: Tab\_eGK\_ObjSys\_036 Initialisierte Attribute von MF / DF.HCA / EF.Logging 50](#_Toc465414290)

[Tabelle 39: Tab\_eGK\_ObjSys\_037 Initialisierte Attribute von MF / DF.HCA / EF.PD 52](#_Toc465414291)

[Tabelle 40: Tab\_eGK\_ObjSys\_038 Initialisierte Attribute von MF / DF.HCA / EF.Prüfungsnachweis 53](#_Toc465414292)

[Tabelle 41: Tab\_eGK\_ObjSys\_039 Initialisierte Attribute von MF / DF.HCA / EF.Standalone 54](#_Toc465414293)

[Tabelle 42: Tab\_eGK\_ObjSys\_040 Initialisierte Attribute von MF / DF.HCA / EF.StatusVD 55](#_Toc465414294)

[Tabelle 43: Tab\_eGK\_ObjSys\_041 Initialisierte Attribute von MF / DF.HCA / EF.TTN 55](#_Toc465414295)

[Tabelle 44: Tab\_eGK\_ObjSys\_042 Initialisierte Attribute von MF / DF.HCA / EF.VD 57](#_Toc465414296)

[Tabelle 45: Tab\_eGK\_ObjSys\_043 Initialisierte Attribute von MF / DF.HCA / EF.Verweis 57](#_Toc465414297)

[Tabelle 46: Tab\_eGK\_ObjSys\_044 Initialisierte Attribute von MF / DF.HCA / DF.NFD 58](#_Toc465414298)

[Tabelle 47: Tab\_eGK\_ObjSys\_045 Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.NFD 60](#_Toc465414299)

[Tabelle 48: Tab\_eGK\_ObjSys\_046 Initialisierte Attribute von MF / DF.HCA / DF.NFD / EF.StatusNFD 61](#_Toc465414300)

[Tabelle 49: Tab\_eGK\_ObjSys\_047 Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.NFD 63](#_Toc465414301)

[Tabelle 50: Tab\_eGK\_ObjSys\_092 Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.NFD\_READ 65](#_Toc465414302)

[Tabelle 51: Tab\_eGK\_ObjSys\_049 Initialisierte Attribute von MF / DF.HCA / DF.DPE 66](#_Toc465414303)

[Tabelle 52: Tab\_eGK\_ObjSys\_050 Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.DPE 67](#_Toc465414304)

[Tabelle 53: Tab\_eGK\_ObjSys\_051 Initialisierte Attribute von MF / DF.HCA / DF.DPE / EF.StatusDPE 69](#_Toc465414305)

[Tabelle 54: Tab\_eGK\_ObjSys\_052 Initialisierte Attribute von MF / DF.HCA / DF.DPE / MRPIN.DPE 70](#_Toc465414306)

[Tabelle 55: Tab\_eGK\_ObjSys\_180 Initialisierte Attribute von MF / DF.HCA / DF.NFD / MRPIN.DPE\_READ 72](#_Toc465414307)

[Tabelle 56: Tab\_eGK\_ObjSys\_054 Initialisierte Attribute von MF / DF.HCA / DF.GDD 73](#_Toc465414308)

[Tabelle 57: Tab\_eGK\_ObjSys\_055 Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.EinwilligungGDD 75](#_Toc465414309)

[Tabelle 58: Tab\_eGK\_ObjSys\_057 Initialisierte Attribute von MF / DF.HCA / DF.GDD / EF.VerweiseGDD 76](#_Toc465414310)

[Tabelle 59: Tab\_eGK\_ObjSys\_056 Initialisierte Attribute von MF / DF.HCA / DF.GDD / MRPIN.GDD 77](#_Toc465414311)

[Tabelle 60: Tab\_eGK\_ObjSys\_184 Initialisierte Attribute von MF / DF.HCA / DF.OSE 79](#_Toc465414312)

[Tabelle 61: Tab\_eGK\_ObjSys\_185 Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.OSE 81](#_Toc465414313)

[Tabelle 62: Tab\_eGK\_ObjSys\_186 Initialisierte Attribute von MF / DF.HCA / DF.OSE / EF.StatusOSE 82](#_Toc465414314)

[Tabelle 63: Tab\_eGK\_ObjSys\_187 Initialisierte Attribute von MF / DF.HCA / DF.OSE / MRPIN.OSE 83](#_Toc465414315)

[Tabelle 64: Tab\_eGK\_ObjSys\_189 Initialisierte Attribute von MF / DF.HCA / DF.AMTS 84](#_Toc465414316)

[Tabelle 65: Tab\_eGK\_ObjSys\_190 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.EinwilligungAMTS 86](#_Toc465414317)

[Tabelle 66: Tab\_eGK\_ObjSys\_191 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.AMTS 87](#_Toc465414318)

[Tabelle 67: Tab\_eGK\_ObjSys\_192 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.VerweiseAMTS 88](#_Toc465414319)

[Tabelle 68: Tab\_eGK\_ObjSys\_193 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / EF.StatusAMTS 89](#_Toc465414320)

[Tabelle 69: Tab\_eGK\_ObjSys\_194 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / MRPIN.AMTS 90](#_Toc465414321)

[Tabelle 70: Tab\_eGK\_ObjSys\_195 Initialisierte Attribute von MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP 91](#_Toc465414322)

[Tabelle 71: Tab\_eGK\_ObjSys\_196 Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PIN.AMTS\_REP 93](#_Toc465414323)

[Tabelle 72: Tab\_eGK\_ObjSys\_197 Initialisierte Attribute von MF /DF.HCA / DF.AMTS PrK.AMTS.ENC.E256 93](#_Toc465414324)

[Tabelle 73: Tab\_eGK\_ObjSys\_198 Personalisierte Attribute von MF / DF.HCA / DF.AMTS / PrK.AMTS.ENC.E256 95](#_Toc465414325)

[Tabelle 74: Tab\_eGK\_ObjSys\_059 Initialisierte Attribute von MF / DF.ESIGN 95](#_Toc465414326)

[Tabelle 75: Tab\_eGK\_ObjSys\_060 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048 97](#_Toc465414327)

[Tabelle 76: Tab\_eGK\_ObjSys\_146 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUT.R2048 98](#_Toc465414328)

[Tabelle 77: Tab\_eGK\_ObjSys\_061 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048 98](#_Toc465414329)

[Tabelle 78: Tab\_eGK\_ObjSys\_148 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.AUTN.R2048 99](#_Toc465414330)

[Tabelle 79: Tab\_eGK\_ObjSys\_062 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048 100](#_Toc465414331)

[Tabelle 80: Tab\_eGK\_ObjSys\_150 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENC.R2048 101](#_Toc465414332)

[Tabelle 81: Tab\_eGK\_ObjSys\_063 Initialisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048 101](#_Toc465414333)

[Tabelle 82: Tab\_eGK\_ObjSys\_154 Personalisierte Attribute von MF / DF.ESIGN / EF.C.CH.ENCV.R2048 102](#_Toc465414334)

[Tabelle 83: Tab\_eGK\_ObjSys\_064 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048 103](#_Toc465414335)

[Tabelle 84: Tab\_eGK\_ObjSys\_156 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUT.R2048 104](#_Toc465414336)

[Tabelle 85: Tab\_eGK\_ObjSys\_067 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048 104](#_Toc465414337)

[Tabelle 86: Tab\_eGK\_ObjSys\_159 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.AUTN.R2048 106](#_Toc465414338)

[Tabelle 87: Tab\_eGK\_ObjSys\_070 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048 106](#_Toc465414339)

[Tabelle 88: Tab\_eGK\_ObjSys\_162 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENC.R2048 107](#_Toc465414340)

[Tabelle 89: Tab\_eGK\_ObjSys\_076 Initialisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048 107](#_Toc465414341)

[Tabelle 90: Tab\_eGK\_ObjSys\_168 Personalisierte Attribute von MF / DF.ESIGN / PrK.CH.ENCV.R2048 109](#_Toc465414342)

[Tabelle 91: Tab\_eGK\_ObjSys\_079 Initialisierte Attribute von MF / DF.CIA\_ESIGN 109](#_Toc465414343)

[Tabelle 92: Tab\_eGK\_ObjSys\_080 Initialisierte Attribute von MF / DF.CIA\_ESIGN / EF.CIA\_Info 111](#_Toc465414344)

[Tabelle 93: Tab\_eGK\_ObjSys\_086 Initialisierte Attribute von MF / DF.QES 113](#_Toc465414345)

[Tabelle 94: Tab\_eGK\_ObjSys\_087 Initialisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048 115](#_Toc465414346)

[Tabelle 95: Tab\_eGK\_ObjSys\_175 Personalisierte Attribute von MF / DF.QES / EF.C.CH.QES.R2048 116](#_Toc465414347)

[Tabelle 96: Tab\_eGK\_ObjSys\_088 Initialisierte Attribute von MF / DF.QES / PIN.QES 116](#_Toc465414348)

[Tabelle 97: Tab\_eGK\_ObjSys\_177 Personalisierte Attribute von MF / DF.QES / PIN.QES 118](#_Toc465414349)

[Tabelle 98: Tab\_eGK\_ObjSys\_089 Initialisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048 118](#_Toc465414350)

[Tabelle 99: Tab\_eGK\_ObjSys\_178 Personalisierte Attribute von MF / DF.QES / PrK.CH.QES.R2048 119](#_Toc465414351)

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

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

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
| --- | --- |
| [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] | gematik: Befüllvorschriften für die Plattformanteile der Karten der TI |
| [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 |

A5.2 – Weitere Dokumente

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
| --- | --- |
| [DIN\_EN\_1867] | EN 1867:1997  Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers  DIN EN 1867:1997  Maschinenlesbare Karten – Anwendungen im Gesundheitswesen – Benummerungssystem und Registrierungsverfahren für Kartenausgeberschlüssel |
| [DIN66291-4] | DIN V66291-4 (2002): Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG/SigV Teil 4: Grundlegende Sicherheitsdienste |
| [ISO3166-1] | ISO/IEC 3166-1:1997 Codes for the representations of names of countries – Part 1: Country codes |
| [ISO7816-15] | ISO/IEC 7816-15: 2004 Identification cards - Integrated circuit cards - Part 15: Cryptographic information application |
| [ISO7816-4] | ISO/IEC 7816-4: 2005 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange |
| [ISO8825-1] | ISO/IEC 8825-1: 1995 Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)  <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf> |
| [EN14890–1] | EN 14890-1: 2008 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 Key words for use in RFCs to Indicate Requirement Levels <http://www.apps.ietf.org/rfc/rfc2119.html> |
| [SD5] | ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19  Register of IC manufacturers  <http://www.pkicc.de/cms/media/pdfs/IC_manufacturer_ISO_SD5_1962006.pdf> |
| [TR-03110-2] | Technische Richtlinie TR-03116-2  Worked Example for Extended Access Control (EAC)  PACE, Chip Authentication and Terminal Authentication, Version 1.02 |