gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

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	P71

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			festgelegt, Iteration 2b, Streichen von EF.VerweisNFD und EF.VerweisDPE	
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

1 Einordnung des Dokuments

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

1.1 Zielsetzung

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

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

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

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

1.2 Zielgruppe

Das Dokument richtet sich an

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung des Dokuments

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

1.5 Methodik

1.5.1 Nomenklatur

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

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

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

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

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

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

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

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:

a. Für Kommandonachrichten ohne Kommandodaten ist der Term SmCmdEnc sinnlos.
b. Für Antwortnachrichten ohne Antwortdaten ist der Term SmRspEnc sinnlos.
c. Die Spezifikation ist wie folgt zu interpretieren:
    1. Falls eine Kommandonachricht keine Kommandodaten enthält, 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.
d. 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

1.5.2 Verwendung von Schlüsselworten

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

Sie werden im Dokument wie folgt dargestellt:

⌦ **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.

1.5.3 Komponentenspezifische Anforderungen

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

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

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

2 Optionen

In den Kapiteln 5.3.13 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**

Da die eGK Online administriert wird, MUSS ein Kartenherausgeber bei der Personalisierung Schlüssel für mindestens eines der beiden Verfahren

a. asymmetrische Authentifizierung für CMS/VSD
b. symmetrische Authentifizierung für CMS/VSD

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

⌦ **Card-G2-A_3228 K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten**

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

3 Lebenszyklus von Karte und Applikation

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

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

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

4 Anwendungsübergreifende Festlegungen

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

4.1 Unterstützung optionaler Funktionspakete

4.1.1 USB-Schnittstelle (optional)

⌦ **Card-G2-A_2861 K_eGK: USB-Schnittstelle**

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

⌦ **Card-G2-A_2974 K_eGK: Vorhandensein einer USB-Schnittstelle**

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

4.1.2 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

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

⌦ **Card-G2-A_2977 K_eGK: Zusatzanforderungen für kontaktlose Schnittstelle**

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.⌫

⌦ **Card-G2-A_2978 K_Initialisierung: Kontaktlose Schnittstelle wird nicht genutzt**

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.⌫

Card-G2-A_2979 K_Initialisierung: Kontaktlose Schnittstelle im COS nicht vorhanden

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.⌫

Card-G2-A_2980 K_Personalisierung: Absicherung der kontaktlosen Schnittstelle

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.⌫

Card-G2-A_2339 K_Personalisierung: Druck der CAN auf die eGK bei Verwendung der optionalen kontaktlosen Schnittstelle

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.⌫

Card-G2-A_3204 K_Personalisierung und K_Initialisierung: Konformität kontaktlose Schnittstelle

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.⌫

4.1.3 Logische Kanäle (optional)

Card-G2-A_2981 K_eGK: logische_Kanäle

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

Card-G2-A_2982 K_Initialisierung: Anzeige von logischen Kanälen

Falls das COS die Option_logische_Kanäle

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

4.1.4 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

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

4.2 Reservierung Speicherplatz

4.2.1 AMTS

⌦ **Card-G2-A_3272 K_Initialisierung: Vorgaben für AMTS**

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

a. AMTS_vorbereitet

b. AMTS_angelegt⌫

⌦ **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.⌫

4.2.2 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.⌫

4.2.3 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.⌫

4.3 Attributstabellen

⌦ **Card-G2-A_2333 K_Initialisierung: Änderung von Zugriffsregeln**

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

⌦ **Card-G2-A_2334 K_Initialisierung: Eigenschaften aller Objekte in SE#1**

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

Card-G2-A_2857 K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs

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

Card-G2-A_2858 K_Initialisierung: Eigenschaften der Objekte in anderen SEs

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

Card-G2-A_2335 K_Initialisierung: Ordnerattribute

Enthält eine Tabelle mit Ordnerattributen

a. keinen applicationIdentifier (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.
b. einen oder mehrere AID, dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
c. keinen *fileIdentifier* (FID),
    1. so DARF dieser Ordner NICHT mittels eines *fileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.1] selektierbar sein, es sei denn, es handelt sich um den Ordner *root*, dessen optionaler *fileIdentifier* den Wert '3F00' besitzen MUSS.
    2. so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden. ⌫

4.3.1 Attribute einer Datei (EF)

Card-G2-A_2336 K_Initialisierung: Dateiattribute

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

Card-G2-A_2667 K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile"

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

4.4 Zugriffsregeln für besondere Kommandos

Card-G2-A_2337 K_Initialisierung: Zugriffsregeln für besondere Kommandos

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

a. Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kommandos Get Challenge, LIST PUBLIC KEY, Manage Security Environment und Select stets ALWAYS sein.
b. Falls 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.

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

4.5 Attributswerte und Personalisierung

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

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

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

Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:

⌦ Card-G2-A_3242 K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung

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

5 Spezifikation grundlegender Applikationen

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

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

5.1 Attribute des Objektsystems

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

⌦ **Card-G2-A_2341 K_Initialisierung: Wert des Attributes *root***

Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_eGK_ObjSys_006 sein.⌫

⌦ **Card-G2-A_2342 K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset**

Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A_2345, Card-G2-A_2346, Card-G2-A_2347 und Card-G2-A_2985 entsprechen.⌫

⌦ **Card-G2-A_2343 K_Personalisierung: Wert des Attributes iccsn8**

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

⌦ **Card-G2-A_2344 K_Initialisierung: Inhalt persistentPublicKeyList**

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

⌦ **Card-G2-A_3180 K_Initialisierung: Größe persistentPublicKeyList**

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

⌦ **Card-G2-A_3265 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.⌫

5.1.1 Answer To Reset

⌦ Card-G2-A_2345 K_Personalisierung und K_Initialisierung: ATR-Codierung

Die ATR-Kodierung MUSS die in Tab_eGK_ObjSys_004 dargestellten Werte besitzen.

Tabelle 3: Tab_eGK_ObjSys_004 ATR-Codierung

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

⌫

⌦ Card-G2-A_2346 K_Personalisierung und K_Initialisierung: TC1 Byte im ATR

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

⌦ Card-G2-A_2985 K_Personalisierung und K_Initialisierung: Historical Bytes im ATR

Das Attribut answerToReset SOLL keine Historical Bytes enthalten. ⌫

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

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

5.2 Allgemeine Struktur

Abb_eGK_ObjSys_001 zeigt die allgemeine Struktur der eGK.

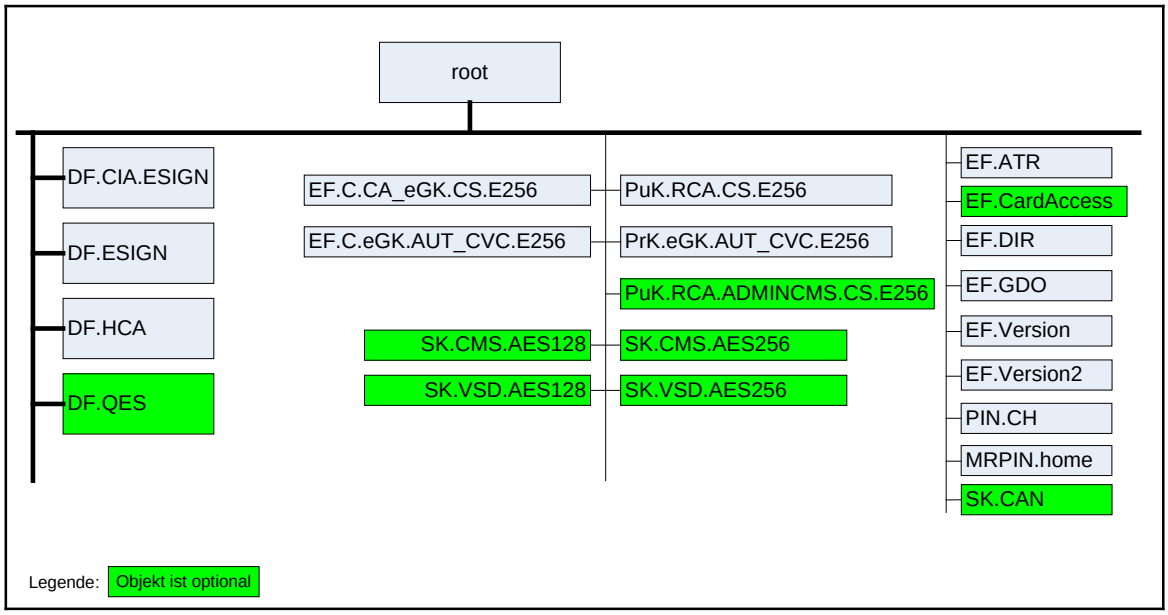

Abbildung 1: Abb_eGK_ObjSys_001 Objektstruktur einer eGK auf oberster Ebene

5.3 Root, die Wurzelapplikation (MF)

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

⌧ **Card-G2-A_2351 K_Initialisierung: Initialisierte Attribute von MF**

MF MUSS die in Tab_eGK_ObjSys_006 dargestellten initialisierten Attribute besitzen.

Tabelle 4: Tab_eGK_ObjSys_006 Initialisierte Attribute von MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D276 0001 4480 00’	
fileIdentifier	‘3F 00’	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	

⌫

Hinweis 2: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

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

5.3.1 MF / EF.ATR

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

⌦ **Card-G2-A_2352 K_Initialisierung: Initialisierte Attribute von MF / EF.ATR**

EF.ATR MUSS die in Tab_eGK_ObjSys_007 dargestellten initialisierten Attribute besitzen.

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

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 01'	siehe Hinweis 5:
shortFileIdentifier	'1D'= 29	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	True	
flagChecksum	True	
numberOfOctet	herstellerspezifisch	
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
shareable	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	
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	

⌫

Hinweis 4: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

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

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

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

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

5.3.2 MF / EF.CardAccess (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

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	

⌫

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

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

⌦ **Card-G2-A_2359 K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_eGK.CS.E256**

EF.C.CA_eGK.CS.E256 MUSS die in Tab_eGK_ObjSys_009 dargestellten initialisierten Attribute besitzen.

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

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 07'	
shortFileIdentifier	'07'= 7	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	True	
flagChecksum	False	
numberOfOctet	'00DC' Oktett = 220 Oktett	
positionLogicalEndOfFile	'0'	
shareable	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
UPDATE BINARY	AUT_CMS	
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
alle	herstellerspezifisch	

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

⌫

Hinweis 6: KOMMANDOS, DIE GEMÄß [GEMSPEC_COS] MIT EINEM TRANSPARENTEN EF ARBEITEN, SIND: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

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

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

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

Attribute	Wert	Bemerkung
positionLogi-calEndOfFile	'00DC' Oktett = 220 Oktett	
body	C.CA_eGK.CS.E256 gemäß [gemSpec_PKI#6.7.1]	
body Option_Erstellung_von_Testkarten	C.CA_eGK.CS.E256 gemäß [gemSpec_PKI#6.7.1] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]

⌫

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

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

⌦ **Card-G2-A_2363 K_Personalisierung: CHR in MF / EF.C.eGK.AUT_CVC.E256**

Für die CHR in diesem Zertifikat MUSS CHR = '00 09' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus Card-G2-A_2370.⌫

⌦ **Card-G2-A_2364 K_Initialisierung: Initialisierte Attribute von MF / EF.C.eGK.AUT_CVC.E256**

EF.C.eGK.AUT_CVC.E256 MUSS die in Tab_eGK_ObjSys_012 dargestellten initialisierten Attribute besitzen.

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

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 06'	
shortFileIdentifier	'06'= 6	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	True	
flagChecksum	False	
numberOfOctet	'00DE' Oktett = 222 Oktett	
positionLogicalEndOfFile	'0'	
shareable	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch	
body	kein Inhalt	wird personalisiert
Zugriffsregeln		
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**
positionLogi-calEndOfFile	'00DE' Oktett = 222 Oktett	
body	C.eGK.AUT_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.eGK.AUT_CVC.E256	

⌫

5.3.5 MF / EF.DIR

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

⌦ **Card-G2-A_2367 K_Initialisierung: Initialisierte Attribute von MF / EF.DIR**

EF.DIR MUSS die in Tab_eGK_ObjSys_014 dargestellten initialisierten Attribute besitzen.

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

Attribute	Wert	Bemerkung
Objekttyp	linear variables Elementary File	
fileIdentifier	'2F 00'	
shortFileIdentifier	'1E'= 30	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	True	
flagChecksum	True	
maxNumRecords	20 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	AUT_CMS	

DELETE RECORD UPDATE RECORD		
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	

⌫

Hinweis 7: Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind: ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, DELETE RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, TERMINATE, UPDATE RECORD, WRITE RECORD.

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

5.3.6 MF / EF.GDO

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

⌦ **Card-G2-A_2369 K_Initialisierung Attribute von MF / EF.GDO**

EF.GDO MUSS die in Tab_eGK_ObjSys_015 dargestellten Attribute besitzen.

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

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 02'	
shortFileIdentifier	'02'= 2	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	False	
flagChecksum	True	
numberOfOctet	'00 0C' Oktett = 12 Oktett	
positionLogicalEndOfFile	Wildcard	
shareable	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch	
body	Wildcard	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Operational state (terminated)" kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (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	

⌫

Hinweis 9: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_2370 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]	

⌫

5.3.7 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**

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	

⌫

Hinweis 10: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, DELETE RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD, TERMINATE

5.3.8 MF / EF.Version2

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

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

Die konkrete Befüllung ist in [gemSpec_Karten_Fach_TIP] 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**

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	

⌫

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

5.3.9 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	

⌫

Hinweis 12: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

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

⌦ **Card-G2-A_3210 K_Personalisierung: Personalisierte Attribute von MF / PIN.CH**

Bei der Personalisierung von PIN.CH MÜSSEN die in Tab_eGK_ObjSys_117 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

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

Attribute	Wert	Bemerkung
secret	PIN-Wert gemäß [gemSpec_PINPUK_TI]	
PUK	PUK-Wert gemäß [gemSpec_PINPUK_TI]	siehe [Card-G2-A_2373]

⌫

⌦ **Card-G2-A_2373 K_Personalisierung: Länge der PUK für die eGK**

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

5.3.10 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**

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	

⌫

Hinweis 14: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

5.3.11 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**

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	

⌫

Hinweis 15: 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	

⌫

5.3.12 Sicherheitsanker zum Import von CV-Zertifikaten

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

5.3.12.1 MF / PuK.RCA.CS.E256

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

⌧ **Card-G2-A_2380 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**

PuK.RCA.CS.E256 MUSS die in Tab_eGK_ObjSys_023 dargestellten initialisierten Attribute besitzen.

Tabelle 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	• $OIDf_{lags}$ = 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	

⌫

Hinweis 16: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, PSO Verify Certificate, TERMINATE.

Hinweis 17: 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 Attribute-NotSet 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	• OID_{flags} = 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	

⌫

5.3.13 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.

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

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie für die asymmetrische 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**

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	OID_{flags} = 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	

Hinweis 18: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, PSO Verify Certificate, TERMINATE.

Hinweis 19: 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	

⌫

5.3.14 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.

5.3.14.1 MF / SK.CMS.AES128

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

⌦ **Card-G2-A_2388 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128**

SK.CMS.AES128 MUSS die in Tab_eGK_ObjSys_027 dargestellten initialisierten Attribute besitzen.

Tabelle 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	

⌫

Hinweis 20: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GET SECURITY STATUS KEY, INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE, TERMINATE.

Hinweis 21: 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]	

⌫

5.3.14.2 MF / SK.CMS.AES256

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

⌦ **Card-G2-A_2389 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]	

5.3.14.3 MF / SK.VSD.AES128

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

Card-G2-A_2390 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]	

⌫

5.3.14.4 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]	

⌫

5.3.15 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**

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	

⌫

Hinweis 22: 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**

Bei Nutzung der kontaktlosen Schnittstelle MUSS die Personalisierung für das Attribut *can* von SK.CAN eine sechsstellige Ziffernfolge gemäß [gemSpec_CAN_TI] setzen.⌫

5.4 Gesundheitsanwendung, Health Care Application (DF.HCA)

⌦ **Card-G2-A_2394 K_Initialisierung: Initialisierte Attribute von MF / DF.HCA**

DF.HCA MUSS die in Tab_eGK_ObjSys_033 dargestellten initialisierten Attribute besitzen.

Tabelle 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 AUT_CMS	herstellerspezifisch ist eine der beiden Varianten erlaubt
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 AUT_CMS	herstellerspezifisch ist eine der beiden Varianten erlaubt
DEACTIVATE	AUT_CMS	
LOAD APPLICATION	AUT_CMS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktlos		
ACTIVATE	AUT_CMS	
DEACTIVATE	ALWAYS AUT_CMS	herstellerspezifisch ist eine der beiden Varianten erlaubt
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
alle	herstellerspezifisch	

⌫

Hinweis 23: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 24: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4 relevant.

Hinweis 25: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.

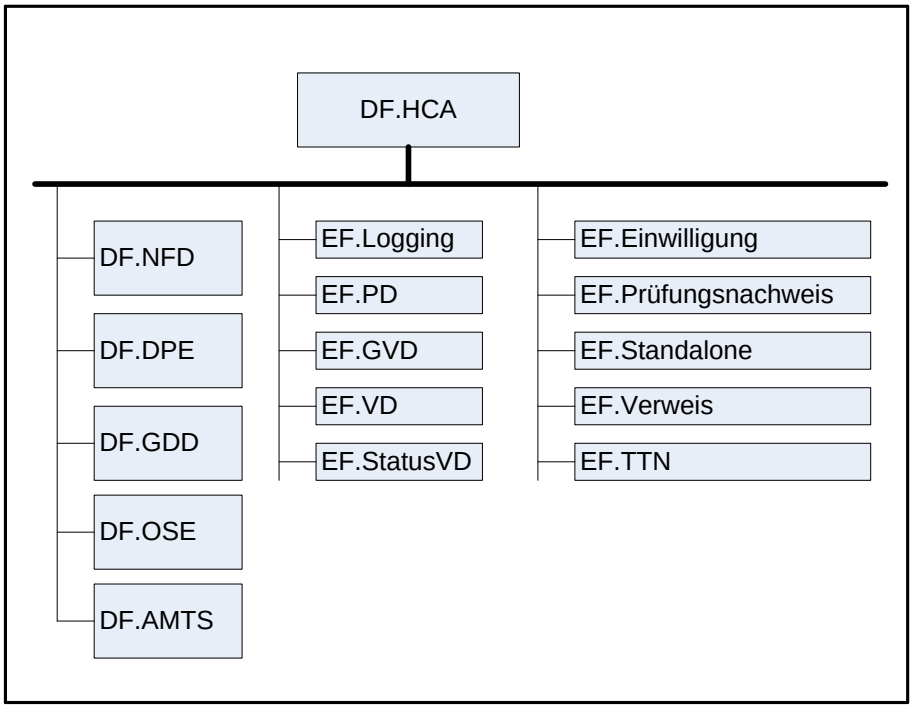

Abbildung 2: Abb_eGK_ObjSys_002 Dateistruktur der Gesundheitsanwendung

5.4.1 MF / DF.HCA / EF.Einwilligung

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

⌧ **Card-G2-A_2395 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	

⌫

Hinweis 26: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate

Hinweis 27: Eine Einwilligung wird anwendungsspezifisch eingetragen. Da die Einwilligung nur im Beisein eines Leistungserbringers eingetragen werden kann, wird für die Freischaltung des Schreibrechts die Eingabe der PIN.CH verlangt.

5.4.2 MF / DF.HCA / EF.GVD

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

⌦ **Card-G2-A_2396 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	

⌫

Hinweis 28: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

5.4.3 MF / DF.HCA / EF.Logging

Diese Datei enthält Protokollierungsinformationen über Zugriffe auf die eGK.

⌦ **Card-G2-A_2397 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	

⌫

Hinweis 29: Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind: ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, DELETE RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, TERMINATE, UPDATE RECORD, WRITE RECORD.

5.4.4 MF / DF.HCA / EF.PD

Diese Datei enthält die persönlichen Daten des Karteninhabers.

Card-G2-A_2398 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	

Hinweis 30: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

5.4.5 MF / DF.HCA / EF.Prüfungsnachweis

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

⌧ **Card-G2-A_2399 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	

⌫

Hinweis 31: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

5.4.6 MF / DF.HCA / EF.Standalone

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

⌦ **Card-G2-A_2400 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	

⌫

Hinweis 32: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

5.4.7 MF / DF.HCA / EF.StatusVD

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

⌦ **Card-G2-A_2401 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	

⌫

5.4.8 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	

⌫

Hinweis 33: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate

5.4.9 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	

⌫

5.4.10 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	

⌫

Hinweis 34: Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate

5.4.11 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	

⌫

Hinweis 35: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 36: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.11 relevant.

Hinweis 37: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.

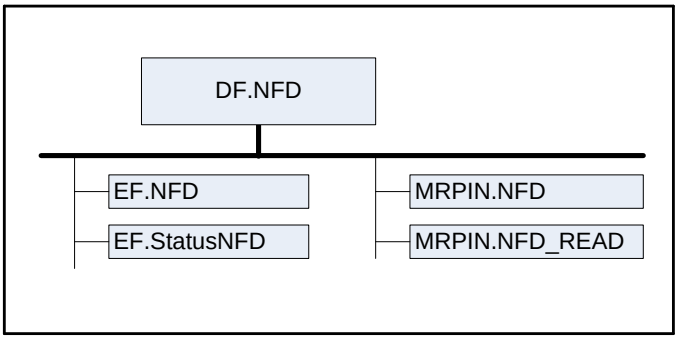

Abbildung 3: Abb_eGK_ObjSys_003 Dateistruktur der Anwendung Notfalldatensatz

5.4.11.1 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	

⌫

Hinweis 38: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

Hinweis 39: 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).

Hinweis 40: 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.

5.4.11.2 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	

⌫

5.4.11.3 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	NEVER	

Attribute	Wert	Bemerkung
(P1='1') ENABLE VERIFICATION REQUIREMENT (P1='1')		
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	

⌫

Hinweis 41: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

5.4.11.4 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	

⌫

Hinweis 42: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

5.4.12 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	

⌫

Hinweis 43: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 44: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekten in 5.4.12 relevant.

Hinweis 45: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.

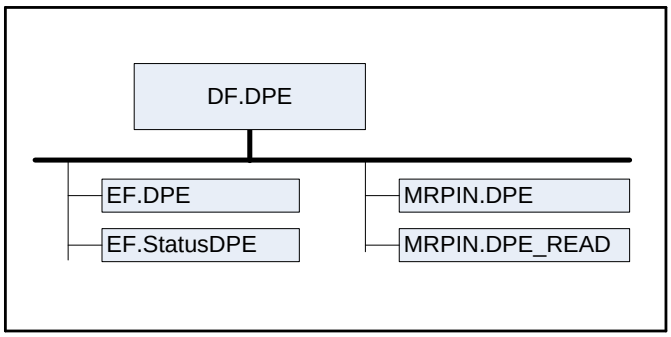

Abbildung 4: Abb_eGK_ObjSys_004 Dateistruktur der Anwendung Datensatz Persönliche Erklärungen

5.4.12.1 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	

Hinweis 46: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

5.4.12.2 MF / DF.HCA / DF.DPE / EF.StatusDPE

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

⌧ **Card-G2-A_2412 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	

⌫

5.4.12.3 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')	AND SmMac(SK.CAN) SmCmdEnc)	
DISABLE VERIFICATION REQUIREMENT (P1='1') ENABLE VERIFICATION REQUIREMENT (P1='1')	NEVER	
CHANGE RD, P1=0	AND SmMac(SK.CAN) SmCmdEnc	
GET PIN STATUS	AND SmMac(SK.CAN) SmCmdEnc	
RESET RC. P1 aus der Menge {0, 1} VERIFY	AND SmMac(SK.CAN) SmCmdEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktlos		
DISABLE VERIFICATION REQUIREMENT (P1='0') ENABLE VERIFICATION REQUIREMENT (P1='0')	AND SmMac(SK.CAN) SmCmdEnc)	
DISABLE VERIFICATION REQUIREMENT (P1='1') ENABLE VERIFICATION REQUIREMENT (P1='1')	NEVER	
CHANGE RD, P1=0	AND SmMac(SK.CAN) SmCmdEnc	
GET PIN STATUS	AND SmMac(SK.CAN) SmCmdEnc	
RESET RC. P1 aus der Menge {0, 1} VERIFY	AND SmMac(SK.CAN) SmCmdEnc	

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

⌫

Hinweis 47: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

5.4.12.4 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	

⌫

Hinweis 48: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

5.4.13 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

	PWD(MRPIN.home) OR [PWD(MRPIN.GDD) AND flagTI.39] *(informativ: OR [PWD(MRPIN.GDD) AND (C.1.10)])*	ist eine der beiden Varianten erlaubt
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	

⌫

Hinweis 49: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 50: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.13 relevant.

Hinweis 51: Da sich weder dieser Ordner noch darüberliegende Ebenen terminieren lassen, ist dieser Zustand für die Spezifikation im Allgemeinen irrelevant.

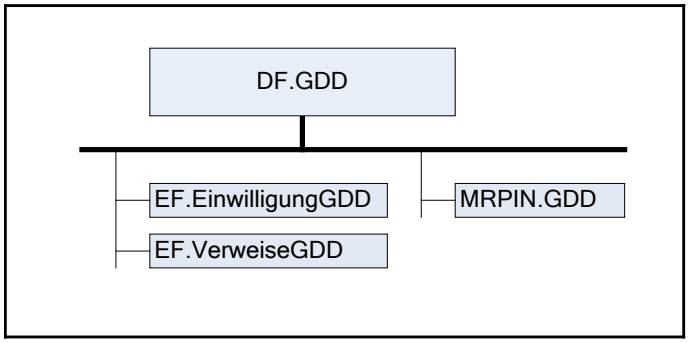

Abbildung 5: Abb_eGK_ObjSys_005 Dateistruktur der Anwendung Gesundheitsdatendienst

5.4.13.1 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)"	
flagTransaction-Mode	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	

⌫

Hinweis 52: Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF arbeiten, sind: ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, DELETE RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, TERMINATE, UPDATE RECORD, WRITE RECORD.

Hinweis 53: 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.

5.4.13.2 MF / DF.HCA / DF.GDD / EF.VerweiseGDD

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

⌦ **Card-G2-A_2418 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	

⌫

5.4.13.3 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	

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

5.4.14 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	

⌫

Hinweis 55: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 56: Da sich dieser Ordner deaktivieren lässt, ist dieser Zustand für Objekte in 5.4.14 relevant.

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

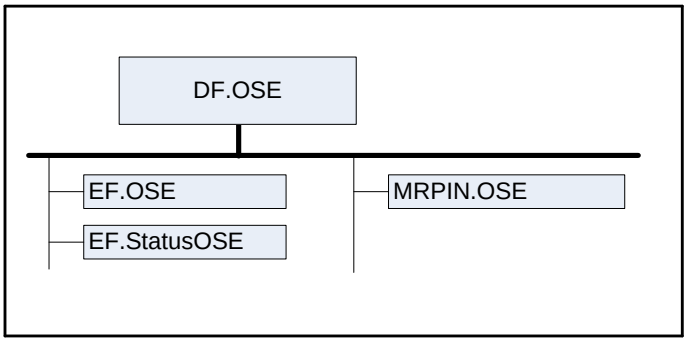

Abbildung 6: Abb_eGK_ObjSys_010 Dateistruktur der Anwendung Organspendeerklärung

5.4.14.1 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	

⌫

Hinweis 58: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

5.4.14.2 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	

⌫

5.4.14.3 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	

⌫

Hinweis 59: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

5.4.15 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
	OR [PWD(MRPIN.AMTS) AND flagTI.45] 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 [PWD(MRPIN.AMTS) AND flagTI.45] OR PWD(MRPIN.home)	herstellerspezifisch ist eine der beiden Varianten erlaubt
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 AND SmMac(SK.CAN) {[PWD(MRPIN.AMTS) AND flagTI.45] OR PWD(MRPIN.home) }	herstellerspezifisch ist eine der beiden Varianten erlaubt
DEACTIVATE	AND SmMac(SK.CAN) {[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	AND SmMac(SK.CAN) {[PWD(MRPIN.AMTS) AND flagTI.45] OR PWD(MRPIN.home) }	
DEACTIVATE	NEVER AND SmMac(SK.CAN) {[PWD(MRPIN.AMTS) AND flagTI.45] OR PWD(MRPIN.home) }	herstellerspezifisch ist eine der beiden Varianten erlaubt
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state" kontaktlos		
alle	herstellerspezifisch	

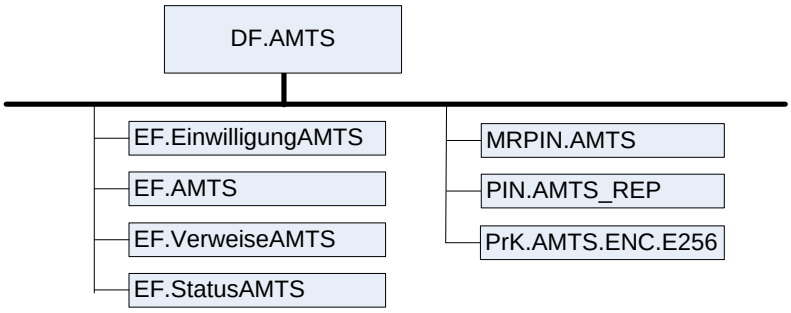

Abbildung 7: Abb_eGK_ObjSys_011 Dateistruktur der Anwendung AMTS Datenmanagement

5.4.15.1 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)“	
flagTransaction-Mode	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	

⌫

5.4.15.2 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	

⌫

5.4.15.3 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	

⌫

5.4.15.4 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	

⌫

5.4.15.5 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	

⌫

5.4.15.6 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.⌫

5.4.15.7 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	

⌫

5.5 DF.ESIGN (Krypto-Anwendung ESIGN)

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

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

⌦ **Card-G2-A_2420 K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN**

DF.ESIGN MUSS die in Tab_eGK_ObjSys_059 dargestellten initialisierten Attribute besitzen.

Tabelle 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	

⌫

Hinweis 60: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 61: Der Wert des Attributes applicationIdentifier ist in [EN14890–1] festgelegt.

Hinweis 62: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren oder terminieren lassen, sind diese Zustände für Objekte in 5.5 im Allgemeinen irrelevant.

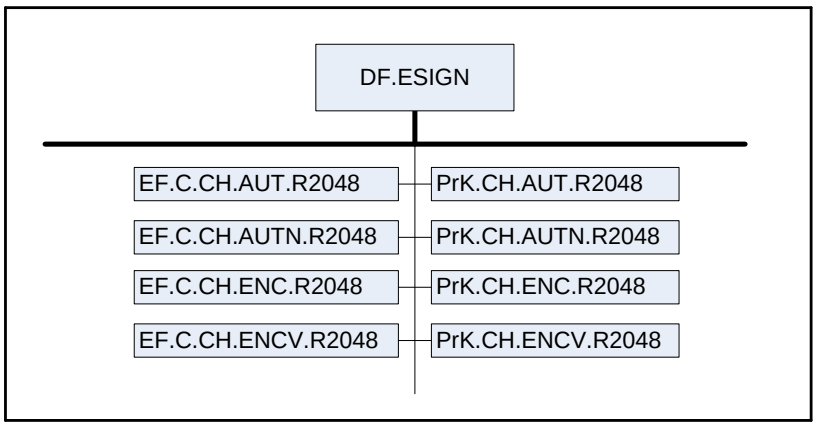

Abbildung 8: Abb_eGK_ObjSys_006 Objektstruktur der Anwendung DF.ESIGN

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

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

⌦ **Card-G2-A_2421 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	

⌫

Hinweis 63: 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
positionLogi-calEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.CH.AUT.R2048 gemäß [gemSpec_PKI#5.1.3.1] passend zu dem privaten Schlüssel in PrK.CH.AUT.R2048	

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

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

Card-G2-A_2424 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	*‘07* 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	
shareable	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet		
DELETE 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	

⌫

Hinweis 64: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_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	

⌫

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

Diese Datei enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.CH.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	

⌫

Hinweis 65: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_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	

⌫

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

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

⌦ **Card-G2-A_2434 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	

⌫

Hinweis 66: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

⌦ **Card-G2-A_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	

⌫

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

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

⌦ **Card-G2-A_2437 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	

⌫

Hinweis 67: 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	

⌫

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

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

⌦ **Card-G2-A_2440 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 Modulus-länge 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	

⌫

Hinweis 68: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: ACTIVATE; DEACTIVATE; DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, TERMINATE.

⌦ **Card-G2-A_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	

⌫

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

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

⌦ **Card-G2-A_2443 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 Modulus-länge 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	SmMac (CAN)	

PSO Transcipher	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	

⌫

Hinweis 69: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: ACTIVATE; DEACTIVATE; DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, TERMINATE.

⌦ **Card-G2-A_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	

⌫

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

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

⌦ **Card-G2-A_2449 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 Modulus-länge 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	

⌫

Hinweis 70: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: ACTIVATE; DEACTIVATE; DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, TERMINATE.

⌦ **Card-G2-A_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	

⌫

5.6 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	

⌫

Hinweis 71: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis 72: Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [ISO7816-15] sowie als PIX den applicationIdentifier von DF.ESIGN (siehe Tab_eGK_ObjSys_059).

Hinweis 73: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im 5.6 nicht berücksichtigt zu werden.

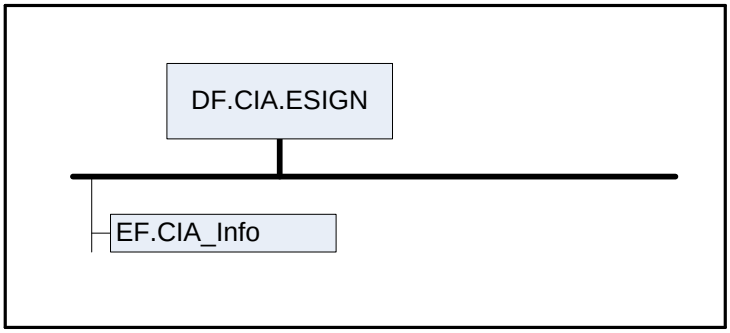

Abbildung 9: Abb_eGK_ObjSys_007 Objektstruktur der Anwendung DF.CIA.ESIGN

5.6.1 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	

⌫

Hinweis 74: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

Hinweis 75: Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.

Hinweis 76: ASN.1 Werte: ciaInfoExample CardInfo ::= {
version v2,

```
        cardflags {   },
        profileIndication {
                "DIN V 66291"
        }
}
```

6 Qualifizierte elektronische Signatur

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

- Es gibt kein DF.QES. Damit ist dieses Kapitel nicht relevant. Es ist möglich, eine entsprechende Anwendung mittels LOAD APPLICATION (siehe [gemSpec_COS]) nachzuladen. Entsprechende Rechte sind derzeit in der Anwendung *root* (siehe Tab_eGK_ObjSys _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.⌫

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

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

⌦ **Card-G2-A_2459 K_Initialisierung: Initialisierte Attribute von MF / DF.QES**

DF.QES MUSS die in Tab_eGK_ObjSys_086 dargestellten initialisierten Attribute besitzen.

Tabelle 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	

⌫

Hinweis 77: Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, GET RANDOM, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

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

Hinweis 79: Die konkrete Zugriffsregel muss durch den Objektsystemhersteller, der diese Option umsetzt, in Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS) festgelegt werden.

Hinweis 80: Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im 6.1 nicht berücksichtigt werden.

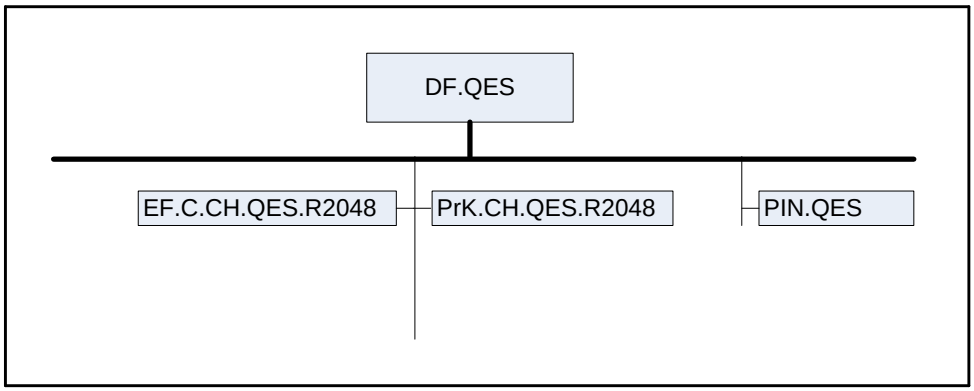

Abbildung 10: Abb_eGK_ObjSys_009 Objektstruktur der vollständigen Signaturanwendung DF.QES

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

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

⌧ **Card-G2-A_2460 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	

⌫

Hinweis 81: Die konkrete Zugriffsregel muss durch den Objektsystemhersteller, der diese Option umsetzt, in Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS) festgelegt werden.

Hinweis 82: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY, SET LOGICAL EOF, TERMINATE, WRITE BINARY.

Hinweis 83: 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	

⌫

6.1.2 MF / DF.QES / PIN.QES

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

⌦ **Card-G2-A_2463 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	

⌫

Hinweis 84: 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

⌫

Hinweis 85: 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.

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

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

⌦ **Card-G2-A_2464 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 ASYM-METRIC 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	

⌫

Hinweis 86: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt (RSA) arbeiten, sind: ACTIVATE; DEACTIVATE; DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Compute Digital Signature, PSO Decipher, PSO Transcipher, TERMINATE.

Hinweis 87: 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	

⌫

6.2 Optionen für unvollständige QES-Anwendung

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

Anhang A – 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 krypto-graphischen Diensten
CIO	Cryptographic Information Object, Objekt mit Informationen zu einem kryptogra-phischen 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)

Kürzel	Erläuterung
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

A4 – Tabellenverzeichnis

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)

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	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