Einführung der Gesundheitskarte

Spezifikation der elektronischen Gesundheitskarte

Teil 2: Grundlegende Applikationen

Version:	2.2.0
Stand:	25.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Diese Version unterscheidet sich in folgenden Punkten von der Version 2.1.0:

- ZDA–VP Kennungen in Tabelle 52 ergänzt
- Transportschutz für PIN.CH und PIN.home bei Auslieferung geändert
- informative Zugriffsrechtematrizen nach Anhang D verschoben (rein editorisch)
- Zugriffsrechte wegen Kommentaren geändert
- Kapitel 7.3.2.1 Punkt 1: Schlüsselnamen korrigiert
- Zugriffsregeln in Kapiteln 6.2.7 und 6.2.8 präzisiert
- Zugriffsregeln in Kapiteln 6.3.6, 6.3.8, 6.3.9, 6.3.14 und 6.4.8 an neue Vorgaben angepasst
- (N30) und (N31) präzisiert, weil die Nummerierung der vierten Ebene Probleme zu bereiten scheint.
- • Zusätzliche Begriffe für PIN.CH und PIN.home, siehe Tabelle 2
- Begriff Rezept durch Verordnung ersetzt
- Profil 9 aufgenommen (siehe Tabelle 65) und Zugriffsrechte entsprechend geändert
- Tabelle 62 Kodierung CHA Werte geändert
- Wert für CHR im CV–Zertifikat festgelegt in Kapitel 6.2.3 und 7.7.5
- Tabelle 54: Es ist möglich C.CH:QES im Feld zu ändern.
- PIN.QES in Tabelle 48: Zugriffsregel im Falle Nachladen geändert
- Folgende Dateien sind nicht mehr löschbar:
  a) EF.ASD Tabelle 51
  b) EF.CVC.ZDA_eGK.CS Tabelle 55
  c) EF.CVC.ZDA_eGK.AUT Tabelle 56
- Schlüssel PrK.eGK.ZDA_AUT (Tabelle 58) und SK.Admin (Tabelle 59) sind auch im Zustand LCS=activated nutzbar
- Tabelle 5AID des MFs geändert
- Tabelle 15 OID korrigiert
- Tabelle 65 an neue Zugriffsregeln angepasst

- SK.CAMS in SK.CMS umbenannt, SK.VSDDCAMS in SK.VSDDCMS umbenannt, dabei Abbildung 1 angepasst
- Folgende Umbenennungen durchgeführt:
  a) EF.StatusVerordnung EF.StatusVerordnungen
  b) EF.eVerordnungContainer EF.eVerordnungsContainer
  c) EF.eVorordnungTicket EF.eVerordnungsTickets
- In Zugriffsregeln Ausdrücke wie C.2.3 geklammert, wo dies notwendig ist.
- EF.Testteilnahme gemäß Vorgabe AB vom 14.3.2008 eingefügt

Inhaltliche Änderungen gegenüber der Version 2.1.0 sind gelb markiert.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemSpec_eGK_P2] gematik (**25.03.2008**): Einführung der Gesundheitskarte – Spezifikation elektronische Gesundheitskarte; Teil 2: Grundlegende Applikationen Version 2.2.0, www.gematik.de

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1	08.06.05		1. gematik-Version	gematik, AG3
0.2	01.07.05		Ergänzung der KVK-Anwendung Änderung der Versichertendaten	gematik, AG3
0.3	17.07.05		Update der Notation Vervollständigung der KVK-Anwendung Ergänzung des SEARCH-Kommando Überarbeitung der eSign-Anwendung Überarbeitung der Zugriffsregeln	gematik, AG3
0.4	06.08.05		Anpassung ICCSN an EU-Richtlinie SE-Nutzung geändert Echtheitsprüfung der eGK mit Chiffrierung Zeitstempel Freischaltung PrK.CH.ENC nach externer Authentisierung mit VODD Bearbeitung eingegangener Kommentare editorielle Verbesserungen und einige Präzisierungen Anhang F und G und Literatur-Kapitel gelöscht (veraltet)	gematik, AG3
0.9	31.08.05		Auslagerung aller Sicherheitsverfahren in ein gesondertes Dokument	gematik, AG3

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Überarbeitung auf Konsistenz Einarbeitung Nachladen qualifizierter elektronischer Signatur Einarbeiten der Verfahren zur Nutzung des Schlüssels PrK.CH.ENC	
0.95	11.10.05		Einarbeitung Kommentare gSP3 Kennzeichnung offener Punkte Abtrennung Sicherheitsverfahren in eigenes Dokument	gematik, AG3
0.99	06.11.05		Re-Integration der asymmetrischen und symmetrischen Authentisierungsverfahren	gematik, AG3
1.0.0	12.12.05		Unterstützung passiver Patientenrechte (Lesen @home nach Eingabe von PIN.home) Abbildung von Rollen auf Profile CVC-Verfahren harmonisiert Erweiterung Versichertendaten Aktualisierung QES-Nachladeverfahren	gematik, AG3
1.1.0	25.01.06		Einarbeitung Kommentare, redaktionelle Überarbeitung (u. a. Abk.Verzeichnis und Referenzliste in Anhang H ausgelagert), Entfernen des EF.KVK	gematik, AG3
1.1.1	26.4.06		Einarbeitung Nachladen QES Einarbeitung EF.Status	gematik, AG3
1.1.17	02.08.06		Einarbeitung neue Struktur des Dokumentes in Bezug auf Aktivieren QES, Anpassung an Fachkonzepte, Einarbeitung SK.COMBI	gematik, AG3
1.1.25	27.08.06		Einarbeitung Kommentare aus öffentlicher Kommentierung	gematik, AG3
1.1.34	31.08.06		Einarbeitung deactivate record für eRezept und deactivate file für Notfalldaten	gematik, AG3
1.1.37	02.09.06		Anpassung Dokumentenstruktur	gematik, AG3
1.2.0	03.09.06		freigegeben	gematik
1.2.1	07.09.06		freigegeben nach QS	gematik
1.2.2	04.04.07 … 08.05.07		SRQs eingearbeitet Zugriffsregeln geändert EF.Version angelegt	gematik, AG7
1.2.3	10.05.07 … 18.05.07		Zugriffsregeln geändert PIN.CH ist auch im SE#02 verifizierbar Inhalt von EF.StatusPIN wird extern festgelegt Inhalt von EF.Einwilligung wird extern festgelegt Kommandotabellen in Kapitel 8 korrigiert	gematik, AG7
1.2.4, 1.2.5	25.05.07		Einige Zugriffsregeln geändert	gematik, AG7
1.3.0	25.05.07		freigegeben zur Vorkommentierung	gematik

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.3.1	17.07.07		Einarbeitung Kommentare	gematik, AG7
1.4.0	01.08.07		freigegeben	gematik
1.4.1	15.08.07	1.2, Abb.1	Ergänzung um Speicherstrukturen	gematik, AG7
1.5.0	24.08.07		freigegeben	gematik
1.5.1	27.08.07		Ergänzung um Hinweis auf noch nicht konsentierte Zugriffsbedingungen für DF.HCA	gematik, AG7
1.5.2	06.11.07		Änderung Schlüssellängen und Zertifikatsformate; Entfallen der Profile CHA 8 bis 10, Synchronisation zu Teil 1, Anpassung von Zugriffsregeln an fachliche Vorgaben, editorische Überarbeitung	SPE/DK
1.6.0	08.11.07		freigegeben zur Vorkommentierung	gematik
1.6.1	06.12.07		Kommentare eingearbeitet	SPE/DK
1.6.2	10.12.07		Anpassung Profil 8, entfernen Profile 9 und 10	SPE/DK
2.0.0	13.12.07		freigegeben	gematik
2.1.0	20.12.07		Leserecht von Profil 7 ohne PIN.CH für EF.GVD gestrichen	gematik
2.1.1	15.01.08 … 14.02.08		• Datenerhalt integriert • Profil 9 aufgenommen • Zugriffsrechtematrix geändert • Tabelle 62 Kodierung CHA Werte geändert • Objekte umbenannt CVC.eGK.AUT **à** C.eGK.AUT_CVC CVC.CA_eGK.CS **à** C.CA_eGK.CS PrK.eGK.AUT **à** PrK.eGK.AUT_CVC • Rezept durch Verordnung ersetzt	gematik, AFI
2.1.2	10.03.08		• Datenerhalt entfernt	SPE/DK, AFI
2.1.3	20.03.08		• EF.TTN eingefügt und Zugriffsregeln angepasst	SPE/DK HA
2.2.0	25.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Die Dokumentation für die elektronische Gesundheitskarte besteht aus mehreren technischen Spezifikationen, ergänzenden Dokumenten und organisatorischen Festlegungen. Die Spezifikationen beschreiben den Aufbau und die Funktionsweise der eGK als solche. Die ergänzenden Dokumente definieren die in den Spezifikationen beschriebenen Verfahren sowie die Handhabung der Zertifikate.

1.1 Technische Spezifikationen zur eGK

- **Die Spezifikation der elektronischen Gesundheitskarte**
  Teil 1: Spezifikation der elektrischen Schnittstelle

  Im Teil 1 werden die Basiskommandos, die Grundfunktionen des Betriebssystems sowie die grundlegenden Sicherheitsfunktionen und -algorithmen (hard facts) detailliert beschrieben.

  Diese Spezifikation ist Grundlage der Entwicklung der Kommandostrukturen und Funktionen für eGK-konforme Chipkartenbetriebssysteme; sie ist somit die Grundarchitektur für die ROM-Maske des Halbleiters.

- **Die Spezifikation der elektronischen Gesundheitskarte**
  Teil 2: Anwendungsspezifische Strukturen

  Im Teil 2 werden die anwendungsspezifischen Strukturen der eGK beschrieben. Dieser Teil enthält die Spezifikationen für 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 der elektronischen Gesundheitskarte**
  Teil 3: Äußere Gestaltung

  Der Teil 3 beschreibt die äußere Gestaltung der eGK. Es werden die Bereiche auf der eGK festgelegt, in denen Lichtbild des Versicherten, Texte und Logos vorgesehen sind, und die dazugehörenden Formate definiert. Die Kartenrückseite wird entsprechend den Vorgaben für die europäische Krankenversicherungskarte (EHIC) bedruckt.

1.2 Ergänzende Dokumente zur eGK

- **Speicherstrukturen der eGK für Gesundheitsanwendungen**

  Das Dokument fasst die Daten und Datenstrukturen zusammen, die für die Realisierung der Fachanwendungen wie z.B. Versichertendatenmanagement, Notfalldatenmanagement, Verordnungsdatenmanagement, Verwaltung freiwilliger Anwendungen und Protokollierung maßgeblich sind.

- **Übergabeschnittstelle für die Produktion der eGK**

  In diesem Dokument werden die Daten beschrieben, die für die Herstellung der eGK im Rahmen der gesetzlichen Vorgaben notwendig sind. Die Frage, wer die Daten jeweils erzeugt und wem wie übergibt, muss zwischen Kartenherausgeber und Personalisierer bilateral vereinbart werden.

  Die Verteilung der Aufgaben zwischen den Kartenherausgebern, den Modulen des Kartensystems, den CA/ZDA und den Kartenproduzenten muss jeweils vertraglich festgelegt und dann über definierte Schnittstellen abgewickelt werden.

  Das Format der auf die eGK zu übertragenden Daten ist in XSD-Schemata festgelegt. Zu der Datenübergabeschnittstelle Personalisierung gehören XSD-Schema für

  - den Personalisierungsauftrag
  - die Rückmeldedaten zum Personalisierungsauftrag
  - die persönlichen Versichertendaten
  - die allgemeinen Versicherungsdaten
  - die geschützten Versichertendaten
  - die Typdefinitionen
  - und die Sammlung von Schlüsselausprägungen

- **Personalisierung kryptografischer Daten**

  In diesem Dokument wird für die Sicherheit der kryptografischen Daten durch alle an der Personalisierung einer eGK beteiligten Organisationen ein Mindestniveau festgelegt. Die zugehörigen Sicherheitsanforderungen beziehen sich dabei nicht nur auf die Verarbeitung der kryptografischen Daten durch eine Organisation, sondern auch auf den Transport dieser Daten zwischen den beteiligten Organisationen. Das definierte Mindestniveau für die Sicherheit ist verpflichtend für alle beteiligten Organisationen.

- **PKI für die X.509-Zertifikate Grobkonzept**

  Zur Identifikation von Personen, Objekten, Organisationen, Geräten, Rechten und Rollen werden elektronische Zertifikate verwendet, bei denen die Identität durch eine übergeordnete „vertrauenswürdige“ Instanz mittels einer elektronischen Signatur bestätigt wird.

Für die übergeordneten X.509-Zertifikate der ausstellenden Organisationen, der sog. Trust Service Provider (TSP), wird das Konzept der zentralisierten (Online-) Zertifikatsprüfung umgesetzt.

Das vorliegende Dokument trifft und erläutert die zum Vertrauensmodell der TSL notwendigen Festlegungen und verweist auf die jeweiligen weiterführenden Spezifikationen.

- **Verwendung von Zertifikaten in der Telematikinfrastruktur**

  Das Dokument beschreibt die unterschiedlichen Typen von Zertifikaten und deren Herausgabe und Nutzung in der Telematikinfrastruktur und stellt normative Vorgaben zur detaillierten Prüfung und Auswertung dieser Zertifikate auf, insbesondere bzgl. Prüfung des Vertrauensraums und des Zertifikatsstatus.

- **Festlegung einer einheitlichen X.509-Zertifikatsinfrastruktur für die Telematik im Gesundheitswesen**

  In dem Dokument werden die Vor- und Nachteile verschiedener Konzepte zur Verknüpfung von Public-Key-Infrastrukturen verglichen und ein konkreter Lösungsweg zur praktischen Umsetzung vorgeschlagen.

  Das Konzept zur flexiblen und vertrauenswürdigen Einbindung der verschiedenen Public-Key-Infrastrukturen durch die Schaffung einer „Trust Service List“ wird beschrieben. Diese ermöglicht eine zentrale Sammlung und Verteilung der Root-Zertifikate unter Einhaltung eines einheitlichen Sicherheitsniveaus.

- **PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider**

  Für die übergeordneten X.509-Zertifikate der ausstellenden Organisationen, der sog. Trust Service Provider (TSP), wird das Konzept der zentralisierten (Online-) Zertifikatsprüfung umgesetzt.

  Ein TSP muss in der gematik Trust-service Status List (gematik-TSL) eingetragen sein. Um dies beantragen zu können, muss sich der TSP vorher bei der gematik registrieren lassen.

  Das Dokument beschreibt den Prozess der Registrierung eines TSP durch die gematik.

- **Festlegungen zu den X.509-Zertifikaten der Versicherten**

  Die Inhalte aller personenbezogenen X.509-Zertifikate zur Authentifizierung (AUT und AUTN), Verschlüsselung (ENC und ENCV) und qualifizierten Signatur (QES) werden detailliert dargestellt. Das Dokument trifft die erforderlichen Festlegungen zur Versichertenidentität, zur Pseudonymisierung von AUTN und ENCV, sowie zur Schlüsselverwendung.

- **PKI für CV-Zertifikate: Grobkonzept**

  CV-Zertifikate dienen der C2C-Authentisierung von Mikroprozessorchipkarten, hier insbesondere der eGK und HBA, sowie SMC. Bei Anwendung der CV-

Zertifikate erfolgt zwischen eGK und HBA (bzw. SMC) die vorgeschriebene gegenseitige Authentikation.

Das Grobkonzept beschreibt

den grundsätzlichen Aufbau der PKI für CV-Zertifikate,

die technischen und organisatorischen Rahmenbedingungen für die Nutzung der CV-Zertifikate,

die zu realisierenden Sicherheitslevel und

die grundsätzlichen Vorgaben für die zu schaffenden Policies und die Umsetzung der Sicherheitskonzepte für die Herausgabe von CV-Zertifikaten.

- **PKI für CV-Zertifikate: Registrierung einer CVC-CA der zweiten Ebene**

  Das Dokument beschreibt den Prozess der Registrierung einer CVC-CA durch die gematik. Dabei werden die Mindestanforderungen an eine CVC-CA aus [gemPKI_Reg] konkretisiert. Zusätzlich wird der Prozess für das Beantragen und Ausstellen eines CV-Zertifikates für eine CVC-CA durch die Root-CVC-CA detailliert beschrieben.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokuments

Dieses Dokument spezifiziert 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, Verordnungen 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 Kapitel 2.5).

2.2 Zielgruppe

Das Dokument richtet sich an

- Applikationsentwickler, welche die hier spezifizierten Anwendungen herstellerspezifisch für eine bestimmtes Chipkartenbetriebssystem umsetzen,
- Kartenherausgeber, die anhand der hier spezifizierten Anwendungen die elektrische Personalisierung einer eGK planen,
- Anwendungsprogrammierer, die Programme entwickeln, welche unmittelbar mit der Chipkarte kommunizieren.

Dieses Dokument spezifiziert die verpflichtenden Anwendungen der elektronischen Gesundheitskarte.

2.3 Geltungsbereich

Der Inhalt des Dokumentes ist verbindlich für die Erstellung elektronischer Gesundheitskarten.

2.4 Arbeitsgrundlagen

Die Ausarbeitung steht in engem Zusammenhang mit den fachlichen Vorgaben und den normativen Vorgaben aus [gemSpec_eGK_P1] zur Spezifikation von Anwendungen.

2.5 Abgrenzung des Dokuments

Das Dokument [gemSpec_eGK_P1] beschreibt die Funktionalität eines eGK Betriebssystems, ohne konkret eine Konfiguration zu nennen. Dieses Dokument beschreibt die Dateistruktur einer eGK und setzt dabei die in [gemSpec_eGK_P1] spezifizierte Funktionalität voraus. Welchem Zweck die hier aufgeführten Dateien, Schlüssel und Passwörter dienen ist nicht Gegenstand dieses Dokumentes. Beispielhaft sei hier auf die in der folgenden Tabelle genannten Fachkonzepte verwiesen, die sich der hier beschriebenen Dateien, Schlüssel und Passwörter bedienen.

Tabelle 1: Fachkonzepte zur Einführung der Gesundheitskarte

Fachanwendung	Inhalt
Versichertenstammdatenmanagement (VSDM)	Bereitstellung und Pflege der Stammdaten des Versicherten in der Telematikinfrastruktur.
Verordnungsdatenmanagement (VODM)	Einrichtung, Dispensierung und Verwaltung der eVerordnungen.
Daten für die Notfallversorgung (NFDM)	Verwaltung der Notfalldaten der Versicherten.
Daten zur Prüfung der Arzneimitteltherapiesicherheit (AMTS)	Fachanwendung zur Prüfung der Arzneimittelverträglichkeit der Versicherten
Anwendungen des Versicherten (ADV)	Beschreibung der Anwendungen, die der Versicherte eigenständig nutzen kann.
Kartenmanagement (CM)	Beschreibt die fachlichen Anforderungen und die Anwendungsfälle für das Management des Kartenlebenszyklus und der Anwendungen der eGK.

2.6 Methodik

2.6.1 Nomenklatur

´1D´	Hexadezimale Zahlen und Oktettstrings werden in Hochkomma eingeschlossen
x || y	Das Symbol || steht für die Konkatenierung von Oktettstrings oder Bitstrings ´1234´ || ´5678´ = ´12345678´

- In [gemSpec_eGK_P1] 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, …).

- Gemäß [gemSpec_eGK_P1] Kapitel 11.2 wird die Notwendigkeit einer externen Authentisierung 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.
    Beispiele:

AUT(CHA.1)	C.1
AUT(CHA.7)	C.7
AUT(CHA.2) OR AUT(CHA.3)	C.2.3
PWD(pin) AND [AUT(CHA.2) OR AUT(CHA.3)]	PWD(pin) AND [C.2.3]

An der Benutzerschnittstelle werden für Benutzergeheimnisse andere Bezeichnungen verwendet, als in technischen Dokumenten. Tabelle 2 listet die Zuordnung.

Tabelle 2: Zuordnung der Bezeichnungen für PINs

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

2.6.2 Verwendung von Schüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- **MUSS** bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.
- **DARF NICHT** bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.
- **SOLL** beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **SOLL NICHT** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.

- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

Abwandlungen von „**MUSS**“ zu „**MÜSSEN**“ etc. sind der Grammatik geschuldet.

Da im Beispielsatz „*Falls Bedingung X eintritt, DARF NICHT Aktion Y ausgeführt werden*.“ die Phrase „DARF NICHT“ semantisch irreführend ist (wenn nicht Aktion Y, welche denn dann?), wird in diesem Dokument stattdessen „*Falls Bedingung X eintritt, DARF Aktion Y NICHT ausgeführt werden*.“ verwendet.

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.

2.6.3 Normative und informative Abschnitte

Abschnitte mit normativen Inhalten tragen hinter der Kapitelüberschrift den Hinweis:

(normativ)

3 Anforderungen und Annahmen

Das Kapitel wird in einer späteren Version des Dokumentes komplett überarbeitet

4 Lebenszyklus von Karte und Applikation (informativ)

Hinweis (1): Die in diesem Kapitel verwendeten Begriff Vorbereitungsphase und Nutzungsphase werden in [gemSpec_eGK_P1] Kapitel 5 definiert.

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.

5 Anwendungsübergreifende Festlegungen (normativ)

5.1 Attributstabellen

(N1) Die in diesem Dokument definierten Zugriffsregeln DÜRFEN in der Nutzungsphase (siehe Kapitel 4) NICHT verändert werden.

(N2) Der Terminus „alle SE“ bedeutet, dass Objekte sich in SE#1 wie angegeben verwenden lassen MÜSSEN. Diese Objekte KÖNNEN in anderen SE verwendet werden und MÜSSEN dort dieselben Eigenschaften wie in SE#1 besitzen.

5.1.1 Attribute eines Ordners

(N3) 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),
   i. so DARF dieser Ordner sich NICHT mittels eines *fileIdentifier* aus dem Intervall gemäß [gemSpec_eGK_P1] Kapitel 9.1.1 selektieren lassen,
   ii. so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_eGK_P1] Kapitel 9.1.1 zugeordnet werden.

5.1.2 Attribute einer Datei (EF)

(N4) Enthält eine Tabelle mit Attributen einer Datei keinen *shortFileIdentifier*, so DARF sich dieses EF NICHT mittels *shortFileIdentifier* selektieren lassen.

5.2 Zugriffsregeln für besondere Kommandos

Gemäß [gemSpec_eGK_P1] gilt:

(N5) Die Zugriffsbedingung für die Kommandos GET CHALLENGE, MANAGE SECURITY ENVIRONMENT und SELECT MUSS stets ALWAYS sein, unabhängig vom lifeCycleStatus und unabhängig vom aktuellen Security Environment.

6 Spezifikation grundlegender Applikationen (normativ)

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

- das Wurzelverzeichnis der eGK, auch root oder Master File genannt.
- die Gesundheitsanwendung DF.HCA (Health Care Application)
- die Krypto–Anwendung DF.ESIGN
- 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 7 behandelt.

6.1 Attribute des Objektsystems

Das Objektsystem gemäß [gemSpec_eGK_P1] Kapitel 10.1 enthält folgende Attribute:

(N6) Der Wert des Attributes *root* MUSS die Anwendung gemäß Tabelle 5 sein.

(N7) Der Wert des Attributes *answerToReset* MUSS gemäß Kapitel 6.1.1 sein.

(N8) Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein (siehe Kapitel 6.2.5).

(N9) Das Attribut *persistentPublicKeyList* MUSS den Schlüssel PuK.RCA.CS enthalten (siehe Tabelle 15).

6.1.1 Answer To Reset

Tabelle 3: ATR Kodierung

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_eGK_P1])
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)

(N10) Der ATR SOLL ein TC1 Byte mit dem Wert ´FF´ enthalten. In diesem Fall MUSS T0 auf den Wert ´Dx´ gesetzt werden.

(N11) Die Historical Bytes MÜSSEN gemäß [7816–4] kodiert werden.

Tabelle 4: Beispielhafte Kodierung der Historical Bytes

Zeichen	Bedeutung
CI	‘00’ gemäß [7816–4]
TPI	‘6x’ gemäß [7816–4] (x kodiert die Länge des DO), Wertfeld gemäß (N14)
TCS	‘31’ gemäß [7816–4], Wertfeld ist Card Service Data Byte gemäß [7816–4]
TCC	‘73’ gemäß [7816–4], Wertfeld ist Card Capabilities Data Bytes gemäß [7816–4], Anzeige von unterstützten logischen Kanälen, Extended Le–Feld, …)
CLS	Card Life Cycle (Default-Wert ‘00’)

6.2 Root, die Wurzelapplikation

Tabelle 5: Attribute / MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	´D276 0001 4480 00´	
FID	´3F 00´	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
LOAD APPLICATION	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac AND SmCmdEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (2): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Ordnerobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis (3): Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 6.2 nicht berücksichtigt werden.

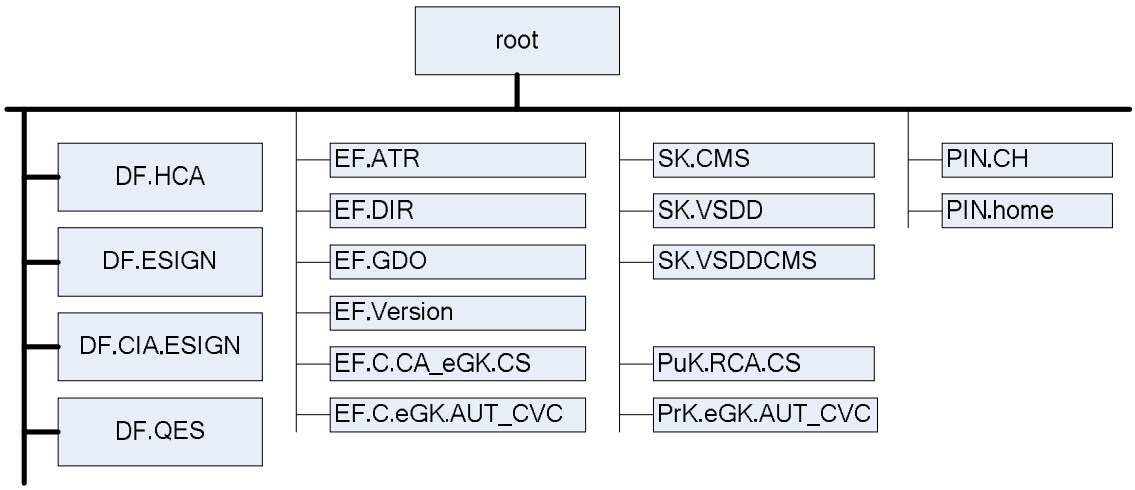

Abbildung 1: Objektstruktur einer eGK auf oberster Ebene

6.2.1 / MF / EF.ATR

Die transparente Datei EF.ATR enthält Informationen zur maximalen Größe der APDU sowie zur Identifizierung des Betriebssystems.

Tabelle 6: Attribute / MF / EF.ATR

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 01´	siehe Hinweis (5):
shortFileIdentifier	´1D´= 29	
numberOfBytes	herstellerspezifisch	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	siehe unten
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (4): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (5): Der Wert des Attributs fileIdentifier ist in [7816–4] festgelegt.

Für das Attribut body gelten folgende Festlegungen:

(N12) Der Oktettstring body MUSS DER–TLV kodierte Datenobjekte (DO) enthalten, welche lückenlos hintereinander konkateniert werden MÜSSEN.

(N13) In body MUSS an erster Stelle genau ein DO_BufferSize mit folgenden Eigenschaften enthalten sein:

a. Tag = ´E0´.

b. DO_Buffersize MUSS genau vier DO mit einem Tag ´02´ enthalten. Der Tag ´02´ bezeichnet einen Integer Wert, der gemäß [8825–1] Kapitel 8.3 kodiert werden MUSS.

c. Das erste DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine ungesicherte Kommando APDU nicht überschreiten SOLL.

d. Das zweite DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine ungesicherte Antwort nicht überschreiten SOLL.

e. Das dritte DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine gesicherte Kommando APDU nicht überschreiten SOLL.

f. Das vierte DO mit Tag ´02´ gibt die maximale Anzahl der Oktette an, die eine gesicherte Antwort nicht überschreiten SOLL.

(N14) In body MUSS an zweiter Stelle genau ein DO_CardData mit folgenden Eigenschaften enthalten sein:

a. Tag = ´66´.

b. Das Wertfeld von DO_CardData MUSS genau ein DO_PreIssuingData mit folgenden Eigenschaften enthalten sein:

i. Tag = ´46´.

ii. Das erste Oktett des Wertfeldes MUSS die Chiphersteller ID gemäß [SD5] enthalten.

iii. Die Oktette zwei bis sechs MÜSSEN die Kartenhersteller–ID enthalten. Anträge unter http://www.sit.fraunhofer.de/ bzw. http://141.12.72.35/_karten_ident/SIT/pdfs/ICCM_Antrag_2006.pdf.

iv. Weitere Oktette sind herstellerspezifisch zu kodieren und SOLLEN eine Betriebssystemversion eineindeutig referenzieren.

c. Das Wertfeld von DO_CardData KANN weitere DER–TLV kodierte Datenobjekte enthalten sein.

(N15) In body KÖNNEN weitere DER–TLV kodierte Datenobjekte enthalten sein.

6.2.2 / MF / EF.C.CA_eGK.CS

Diese Datei enthält ein CV–Zertifikat gemäß [gemSpec_eGK_P1], welches den öffentlichen Schlüssel PuK.CA_eGK.CS einer CA enthält.

Tabelle 7: Attribute / MF / EF.C.CA_eGK.CS

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 04´	
shortFileIdentifier	´04´= 4	
numberOfBytes	´014B´ Oktett = 331 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7F21 820146 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (6): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.2.3 / MF / EF.C.eGK.AUT_CVC

Diese Datei enthält ein CV–Zertifikat gemäß [gemSpec_eGK_P1], welches den öffentlichen Schlüssel PuK.eGK.AUT_CVC zu PrK.eGK.AUT_CVC (siehe Tabelle 14) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_eGK.CS (siehe Tabelle 7) prüfen.

(N16) Für die CHR in diesem Zertifikat MUSS gelten CHR = ´0000´ || ICCSN wobei die ICCSN denselben Wert besitzen MUSS wie das Wertfeld aus (N17)b.

Tabelle 8: Attribute / MF / EF.C.eGK.AUT_CVC

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 03´	
shortFileIdentifier	´03´= 3	
numberOfBytes	´0155´ Oktett = 341 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´7F21 820150 XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (7): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.2.4 / MF / EF.DIR

Die Datei EF.DIR enthält eine Liste mit Anwendungstemplates gemäß [7816–4]. Diese Liste wird dann angepasst, wenn sich die Applikationsstruktur durch Löschen oder Anlegen von Anwendungen verändert.

Tabelle 9: Attribute / MF / EF.DIR

Attribute	Wert	Bemerkung
Objekttyp	linear variables Elementary File	
fileIdentifier	´2F 00´	
shortFileIdentifier	´1E´= 30	
numberOfBytes	´00BE´ Oktett = 190 Oktett	siehe Hinweis (10):
maxNumRecords	10 Rekord	
maxRecordLength	36 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList Rekord 1 Rekord 2 Rekord 3 Rekord 4 Rekord 5 Rekord 6 …	 ´61 08 (4F 06 D27600014401)´ ´61 08 (4F 06 D27600000102)´ ´61 0C (4F 0A A000000167455349474E)´ ´61 11 (4F 0F E828BD080FA000000167455349474E)´ ´61 08 (4F 06 D27600006601)´ nicht vorhanden, MUSS mittels APPEND RECORD angelegt werden	 root, siehe 6.2 HCA, siehe 6.3 ESIGN, siehe 6.4 CIA.ESIGN, 6.5 siehe Hinweis (11):
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
APPEND RECORD	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (8): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem linear variablen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

Hinweis (9): Die Werte von fileIdentifier und shortFileIdentifier sind in [7816–4] festgelegt.

Hinweis (10): Bei der Festlegung der Dateigröße wurde eine durchschnittliche Rekordlänge von 19 Oktett zugrunde gelegt. Diese durchschnittliche Länge wird derzeit nur von einem Rekord erreicht und von keinem übertroffen.

Hinweis (11): Rekord 5 ist nur vorhanden, wenn die DF.QES (siehe Kapitel 7) vorhanden ist.

6.2.5 / MF / EF.GDO

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

Tabelle 10: Attribute / MF / EF.GDO

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´2F 02´	
shortFileIdentifier	´02´= 2	
numberOfBytes	´000C´ Oktett = 12 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´5A0AXX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (12): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Das Attribut body enthält die Seriennummer der Karte. Dabei gilt:

(N17) In body MUSS genau ein DER–TLV kodiertes Datenobjekt DO_ICCSN mit folgenden Eigenschaften enthalten sein:

a. Tag = ´5A´ und Längenfeld = ´0A´.

b. Für das Wertfeld MUSS gelten:

i. Das erste Oktett MUSS den Major Industry Identifer (MII) mit dem Wert ´80´ enthalten, welcher eine Gesundheitskarte kennzeichnet (siehe [EN 1867]).

ii. Die nächsten drei Nibble MÜSSEN den Country Code Deutschlands mit dem Wert ´276´enthalten (siehe [3166]).

iii. Die nächsten fünf Nibble MÜSSEN den Issuer Identifer enthalten.

iv. Die restlichen 5 Oktette MÜSSEN BCD kodiert eine Seriennummer enthalten.

Hinweis (13): Die Kennung eines Kartenherausgebers (Issuer Identifier) erlaubt in Verbindung mit dem Ländercode eine weltweit eineindeutige Identifizierung des Kartenherausgebers. In Verbindung mit der Seriennummer ist es deshalb möglich, eine Karte weltweit eineindeutig zu referenzieren.

Hinweis (14): Die Kennung des Kartenherausgebers entsprechend [EN 1867] wird in Deutschland im Auftrag des DIN durch GS1 Germany GmbH, Köln (www.gs1-germany.de) verge-

ben. Der Kartenherausgeber ist gewöhnlich der rechtmäßige Besitzer der ausgegebenen Karte.

6.2.6 / MF / EF.Version

Der Verwendungszweck wird in [gemeGK_Fach] beschrieben.

Tabelle 11: Attribute / MF / EF.Version

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´2F 10´	
shortFileIdentifier	´10´= 16	
maxNumRecords	4 Rekord	
maxRecordLength	5 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList Rekord 1 Rekord 2 Rekord 3 Rekord 4	siehe [gemeGK_Fach] und Hinweis (16): ´XX…YY´ ´XX…YY´ ´XX…YY´ ´000 000 0000´	Dokumentenversion: [gemSpec_eGK_P1] diesem Dokument [gemeGK_Fach] RFU
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ RECORD SEARCHRECORD	ALWAYS	
UPDATE RECORD	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (15): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem linear fixen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

Hinweis (16): Eine Versionsnummer wird wie folgt zum Inhalt eines Rekords in EF.Version konvertiert: Die erste und zweite Zahl werden in drei Stellen BCD kodiert. Die dritte Zahl in vier Stellen BCD kodiert.
*Beispiel: Versionsnummer 5.9.10 **à** ´0050090010´ = ´005´ || ´009 || ´0010´.*

6.2.7 / MF / PIN.CH

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

Tabelle 12: Attribute / MF / PIN.CH

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	siehe Hinweis (18):
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword, Leer–PIN_1, Leer–PIN_2, Transport–PIN_0000}	siehe Hinweis (19):
flagEnabled	True	
startSsec	unendlich	alle SE
PUK	…	wird personalisiert
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD	ALWAYS (transportStatus ungleich regularPassword)	siehe Hinweis (20):
CHANGE RD, P1=0	ALWAYS (transportStatus gleich regularPassword)	siehe Hinweis (21):
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (17): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Passwortobjekt arbeiten, sind:
CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER, VERIFY

Hinweis (18): Gemäß [gemSpec_eGK_P1] kontrolliert das Betriebssystem der eGK lediglich die Mindestlänge. Die Maximallänge von PIN.CH und PIN.home beträgt acht Stellen. Die Einhaltung der Bedingung für die Maximallänge wird nicht vom COS der eGK kontrolliert.

Hinweis (19): Zitat Anforderungsmeldung A_0473:
Bei Ausgabe einer eGK UND wenn der Karteninhaber keine freiwillige Anwendungen nutzt, MUSS die Auslieferung an den Versicherten mit einem der folgenden Verfahren erfolgen:
** Echt-PIN-Verfahren mit PIN-Brief: (Versand der eGK mit kartenindividuellen Echt-PINs für Privat-PIN und für Praxis-PIN mit gesonderter Zusendung der zugehörigen PIN-Briefe.)*
** Transport-PIN-Verfahren mit Leer-PIN: (Versand der eGK ohne nutzbare Privat-PIN und Praxis-PIN. Vor der ersten Nutzung müssen die PINs vom Karteninhaber initialisiert werden.)*
Bei Ausgabe einer eGK UND wenn der Karteninhaber freiwillige Anwendungen nutzt, MUSS die Auslieferung an den Versicherten mit dem folgenden Verfahren erfolgen:
** Echt-PIN-Verfahren mit PIN-Brief: (Versand der eGK mit kartenindividuellen Echt-PINs für Privat-PIN und für Praxis-PIN mit gesonderter Zusendung der zugehörigen PIN-Briefe.)*

Hinweis (20): Diese Tabellenzeile gilt für den Fall transportStatus ungleich regularPassword.

Hinweis (21): Diese Tabellenzeile gilt für den Fall transportStatus gleich regularPassword.

(N18) Bei der Personalisierung MUSS eine PUK mit acht Ziffern gewählt werden.

6.2.8 / MF / PIN.home

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

Tabelle 13: Attribute / MF / PIN.home

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´02´ = 2	
secret	…	wird personalisiert
minimumLength	6	siehe Hinweis (18):
startRetryCounter	3	
retryCounter	3	
transportStatus	ein Wert aus der Menge {regularPassword, Leer–PIN_1, Leer–PIN_2, Transport–PIN_0000}	siehe Hinweis (19): siehe Hinweis (20):
flagEnabled	True	
startSsec	unendlich	alle SE
PUK	…	wird personalisiert
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD	ALWAYS (transportStatus ungleich regularPassword)	siehe Hinweis (20):
CHANGE RD, P1=0	ALWAYS (transportStatus gleich regularPassword)	siehe Hinweis (21):
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (22): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Passwortobjekt arbeiten, sind:
CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER, VERIFY

(N19) Bei der Personalisierung MUSS eine PUK mit acht Ziffern gewählt werden.

6.2.9 / MF / PrK.eGK.AUT_CVC

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

Tabelle 14: Attribute / MF / PrK.eGK.AUT_CVC

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´10´ = 16	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	Werte gemäß [gemSpec_eGK_P1] rsaRoleAuthentication falls SE#1 rsaSessionkey4SM falls SE#2	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
INTERNAL AUTH.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (23): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE

6.2.10 / MF / PuK.RCA.CS

Dieses Objekt enthält den öffentlichen Schlüssel der Root–CA, welche an der Wurzel der der CVC–Hierarchie steht. Er wird zur Prüfung von CV–Zertikaten der zweiten Ebene benötigt.

Tabelle 15: Attribute / MF / PuK.RCA.CS

Attribute	Wert	Bemerkung
Objekttyp	öffentliches RSA Signaturprüfobjekt	
keyIdentifier	´XX…YY´, acht Oktette	wird personalisiert
publicKey	…, Moduluslänge 2048 Bit	wird personalisiert
oid	´2B24 0304 0202 04´ = {1 3 36 3 4 2 2 4}	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Verify Cert.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (24): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind:
PSO Verify Certificate

6.2.11 / MF / SK.CMS

Dieser Schlüssel wird benötigt, um gewisse administrative Aufgaben am Objektsystem auszuführen.

Tabelle 16: Attribute / MF / SK.CMS

Attribute	Wert	Bemerkung
Objekttyp	3TDES Authentisierungsobjekt	
keyIdentifier	´13´ = 19	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	desSessionkey4SM, siehe [gemSpec_eGK_P1]	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTAUL AUTH.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (25): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE

6.2.12 / MF / SK.VSDD

Dieser Schlüssel wird benötigt, um gewisse administrative Aufgaben an den Inhalten der Dateien mit Versichertendaten auszuführen.

Tabelle 17: Attribute / MF / SK.VSDD

Attribute	Wert	Bemerkung
Objekttyp	3TDES Authentisierungsobjekt	
keyIdentifier	´12´ = 18	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	desSessionkey4SM, siehe [gemSpec_eGK_P1]	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTAUL AUTH.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (26): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE

6.2.13 / MF / SK.VSDDCMS

Dieser Schlüssel vereinigt die Möglichkeiten von SK.CMS (siehe Tabelle 16) und SK.VSDD (siehe Tabelle 17).

Tabelle 18: Attribute / MF / SK.VSDDCMS

Attribute	Wert	Bemerkung
Objekttyp	3TDES Authentisierungsobjekt	
keyIdentifier	´14´ = 20	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	desSessionkey4SM, siehe [gemSpec_eGK_P1]	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTAUL AUTH.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (27): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE

6.3 Gesundheitsanwendung, Health Care Application (HCA)

Tabelle 19: Attribute / MF / DF.HCA

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	´D276000001 02´	
fileIdentifier	–	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
DEACTIVATE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
LOAD APPLICATION	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac AND SmCmdEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
DEACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	

Hinweis (28): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Ordnerobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis (29): Da sich dieser Ordner deaktivieren lässt, sind für diesen Zustand bei den Objekten im Kapitel 6.3 entsprechende Zugriffsregeln zu berücksichtigen.

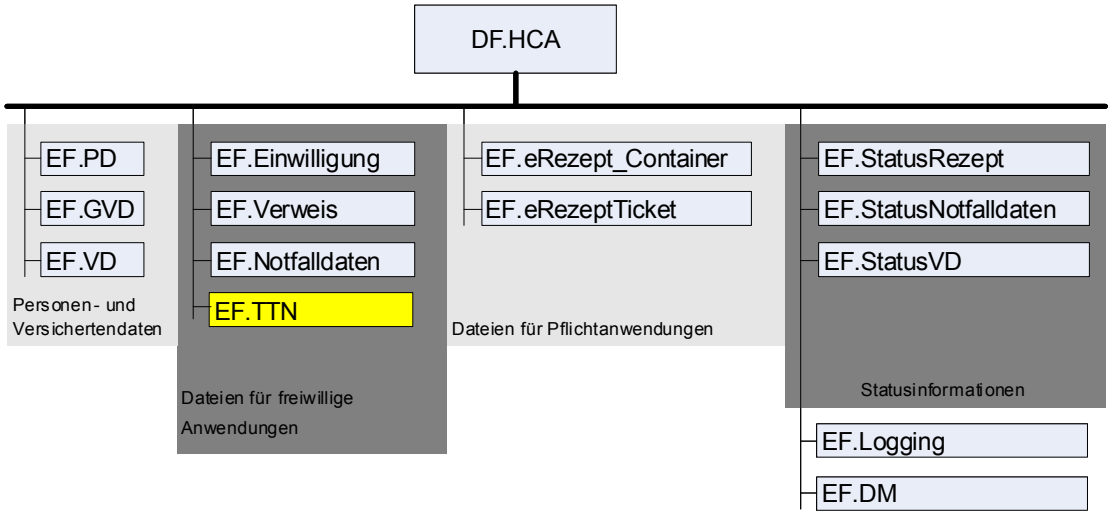

Abbildung 2: Objektstruktur der Gesundheitsanwendung

6.3.1 / MF / DF.HCA / EF.DM

In dieser Datei wird ein benutzerspezifisches Geheimnis gespeichert, welches nur in geschützten Umgebungen auslesbar ist. Wird dieses Geheimnis dem Benutzer angezeigt, so ist dies als Indiz zu werten, dass eine geschützte Umgebung vorliegt.

Tabelle 20: Attribute / MF / DF.HCA / EF.DM

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 04´	
shortFileIdentifier	´04´= 4	
numberOfBytes	´0008´ Oktett = 8 Oktett	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	SmMac AND SmRspEnc	
UPDATE BINARY	PWD(PIN.home)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
alle	NEVER	

Hinweis (30): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:

ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.2 MF / DF.HCA / EF.TTN

Diese Datei enthält die Information über die Testteilnahme des Versicherten. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 21: Attribute / MF / DF.HCA / EF.TTN

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´D0 0F´	
shortFileIdentifier	´0F´= 15	
maxNumRecords	5 Rekord	
maxRecordLength	15 Oktett	
flagRecordLCS	True	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList alle Rekords	Rekord aktiviert, Inhalt des Rekords ´00…00´	Initialwert gemäß [gemeGK_Fach]
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ RECORD	[PWD(PIN.home] OR [PWD(PIN.CH) AND C.1] OR C.2.3.4.5.6.7.8.9	
UPDATE RECORD	[AUT(SK.VSDD) OR AUT(SK.VSDDCAMS) OR AUT(SK.CAMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (31): Kommandos, die gemäß [gem_Spec_eGK_P1] mit einem linear fixen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

6.3.3 / MF / DF.HCA / EF.Einwilligung

Diese Datei enthält die Information über die Einwilligungen zu freiwilligen Anwendungen. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 22: Attribute / MF / DF.HCA / EF.Einwilligung

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´D0 05´	
shortFileIdentifier	´05´= 5	
maxNumRecords	10 Rekord	
maxRecordLength	69 Oktett	
flagRecordLCS	True	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList alle Rekords	Rekord aktiviert, Inhalt des Rekords ´00…00´	Initialwert gemäß [gemeGK_Fach]
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIV. RECORD DEAC. RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4)]	
READ RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4.6)]	
UPDATE RECORD	PWD(PIN.CH) AND (C.2.3.4)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (32): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem linear fixen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

6.3.4 / MF / DF.HCA / EF.GVD

Diese Datei enthält die geschützten Versichertendaten. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 23: Attribute / MF / DF.HCA / EF.GVD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 03´	
shortFileIdentifier	´03´= 3	
numberOfBytes	´01C2´ Oktett = 450 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ BINARY	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1] OR C.2.3.4.5.6.7.8.9 OR {[AUT(SK.VSDD) OR AUT(SK.VSDDCMS)] AND SmMac AND SmRspEnc }	
UPDATE BINARY	[AUT(SK.VSDD) OR AUT(SK.VSDDCMS)] AND SmMac AND SmCmdEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (33): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.5 / MF / DF.HCA / EF.Logging

Diese Datei enthält Protokollierungsinformationen über Zugriffe auf die eGK. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 24: Attribute / MF / DF.HCA / EF.Logging

Attribute	Wert	Bemerkung
Objekttyp	zyklisches Elementary File	
fileIdentifier	´D0 06´	
shortFileIdentifier	´06´= 6	
maxNumRecords	50 Rekord	
maxRecordLength	46 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList alle Rekords	Rekord aktiviert, Inhalt des Rekords ´00…00´	Initialwert gemäß [gemeGK_Fach]
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
APPEND RECORD	[PWD(PIN.CH) AND C.1] OR C.2.3.4.5.6.7.8.9	
READ RECORD SEARCH RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (34): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem zyklischen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

6.3.6 / MF / DF.HCA / EF.Notfalldaten

Diese Datei enthält den Notfalldatensatz. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 25: Attribute / MF / DF.HCA / EF.Notfalldaten

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 0B´	
shortFileIdentifier	´0B´= 11	
numberOfBytes	´2328´ Oktett = 9.000 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´0000 XX…YY´, siehe [gemeGK_Fach]	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
DEACTIVATE	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
READ BINARY	C.2.7 OR [PWD(PIN.CH) AND (C.3.4)]	
UPDATE BINARY	PWD(PIN.CH) AND (C.2)	
ERASE BIBARY	PWD(PIN.CH) AND (C.2.3.4)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
DEACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
SELECT	ALWAYS	
alle	NEVER	

Hinweis (35): Mögliche Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (36): Das Aktivieren einer bereits aktivierten Datei bzw. das Deaktivieren einer bereits deaktivierten Datei ist aus Sicherheitssicht unproblematisch.

6.3.7 / MF / DF.HCA / EF.PD

Diese Datei enthält die persönlichen Daten des Karteninhabers. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 26: Attribute / MF / DF.HCA / EF.PD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 01´	
shortFileIdentifier	´01´= 1	
numberOfBytes	´0352´ Oktett = 850 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ BINARY	ALWAYS	
UPDATE BINARY	[AUT(SK.VSDD) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (37): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.8 / MF / DF.HCA / EF.StatusNotfalldaten

Diese Datei enthält die Information über den Status des Notfalldatensatzes. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 27: Attribute / MF / DF.HCA / EF.StatusNotfalldaten

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 0E´	
shortFileIdentifier	´0E´= 14	
numberOfBytes	´0019´ Oktett = 25 Oktett	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, siehe [gemeGK_Fach]	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
DEACTIVATE	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
READ BINARY	C.2.7 OR [PWD(PIN.CH) AND (C.3.4)]	
UPDATE BINARY	PWD(PIN.CH) AND (C.2)	
ERASE BINARY	PWD(PIN.CH) AND (C.2.3.4)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
DEACTIVATE	ALWAYS	herstellerspezifisch ist eine der beiden Varianten erlaubt
	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
SELECT	ALWAYS	
andere	NEVER	

Hinweis (38): Mögliche Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (39): Das Aktivieren einer bereits aktivierten Datei bzw. das Deaktivieren einer bereits deaktivierten Datei ist aus Sicherheitssicht unproblematisch.

6.3.9 / MF / DF.HCA / EF.StatusVerordnungen

Diese Datei enthält die Information über den Status der Daten im Container eVerordnungsTickets und im Container eVerordnungsContainer. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 28: Attribute / MF / DF.HCA / EF.StatusVerordnungen

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 0D´	
shortFileIdentifier	´0D´= 13	
numberOfBytes	´0019´ Oktett = 25 Oktett	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, siehe [gemeGK_Fach]	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6	
UPDATE BINARY	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6 OR {[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac }	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (40): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.10 / MF / DF.HCA / EF.StatusVD

Diese Datei enthält die Information über den Status der Daten in EF.PD, EF.VD und EF.GVD. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 29: Attribute / MF / DF.HCA / EF.StatusVD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 0C´	
shortFileIdentifier	´0C´= 12	
numberOfBytes	´0019´ Oktett = 25 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, siehe [gemeGK_Fach]	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ BINARY	ALWAYS	
UPDATE BINARY	[AUT(SK.VSDD) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (41): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.11 / MF / DF.HCA / EF.VD

Diese Datei enthält die Versichertendaten. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 30: Attribute / MF / DF.HCA / EF.VD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 02´	
shortFileIdentifier	´02´= 2	
numberOfBytes	´04E2´ Oktett = 1.250 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ BINARY	ALWAYS	
UPDATE BINARY	[AUT(SK.VSDD) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (42): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.12 / 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. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 31: Attribute / MF / DF.HCA / EF.Verweis

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´D0 09´	
shortFileIdentifier	´09´= 9	
maxNumRecords	10 Rekord	
maxRecordLength	20 Oktett	
flagRecordLCS	True	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList alle Rekords	Rekord aktiviert, Inhalt des Rekords ´00…00´	Initialwert gemäß [gemeGK_Fach]
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIV. RECORD DEAC. RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4)]	
READ RECORD SEARCHRECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4.6.9)]	
UPDATE RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4.9)]	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (43): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem linear fixen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

6.3.13 / MF / DF.HCA / EF.eVerordnungsContainer

Dieser Container enthält die Daten der eVerordnungen. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 32: Attribute / MF / DF.HCA / EF.eVerordnungsContainer

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 08´	
shortFileIdentifier	´08´= 8	
numberOfBytes	´7530´ Oktett = 30.000 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´00…00´, siehe [gemeGK_Fach]	Auslieferungszustand
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
READ BINARY	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6	
UPDATE BINARY	C.2.3.5.6	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (44): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.3.14 / MF / DF.HCA / EF.eVerordnungsTickets

Dieser Container enthält die Daten der Tickets für die eVerordnungen. Die Details sind in [gemeGK_Fach] beschrieben.

Tabelle 33: Attribute / MF / DF.HCA / EF.eVerordnungsTickets

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	´D0 07´	
shortFileIdentifier	´07´= 7	
maxNumRecords	8 Rekord	
maxRecordLength	165 Oktett	
flagRecordLCS	True	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
recordList alle Rekords	Rekord aktiviert, Inhalt des Rekords ´00…00´	Initialwert gemäß [gemeGK_Fach]
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIV. RECORD DEAC. RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1]	
ERASE RECORD	PWD(PIN.home)	
READ RECORD SEARCHRECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6	
UPDATE RECORD	C.2.3.5.6	
ERASE RECORD	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	

Hinweis (45): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem linear fixen EF arbeiten, sind:
ACTIVATE, ACTIVATE RECORD, APPEND RECORD DEACTIVATE, DEACTIVATE RECORD, DELETE, APPEND RECORD, ERASE RECORD, READ RECORD, SEARCH RECORD, SELECT, UPDATE RECORD

6.4 Krypto–Anwendung ESIGN

Die allgemeine ESIGN Anwendung ist in [prEN 14890–1] 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 kryptografische Sicherung von Daten
- die Schlüssel–Chiffrierungsfunktion im Kontext elektronischer Verordnungen.

Tabelle 34: Attribute / MF / DF.ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	´A000000167 455349474E´	siehe Hinweis (47):
fileIdentifier	–	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (46): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Ordnerobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis (47): Der Wert des Attributes applicationIdentifier ist in [prEN 14890–1] festgelegt.

Hinweis (48): Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 6.2 nicht berücksichtigt zu werden.

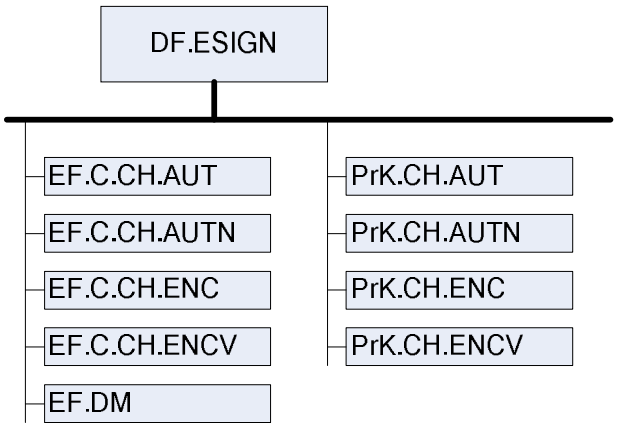

Abbildung 3: Objektstruktur der Anwendung DF.ESIGN

6.4.1 / MF / DF.ESIGN / EF.C.CH.AUT

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.CH.AUT zu PrK.CH.AUT (siehe Kapitel 6.4.6). Vorgaben zum Zertifikat finden sich in [gemX.509_eGK].

Tabelle 35: Attribute / MF / DF.ESIGN / EF.C.CH.AUT

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C5 00´	
shortFileIdentifier	´01´= 1	
numberOfBytes	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
UPDATE BINARY	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (49): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.4.2 / MF / DF.ESIGN / EF.C.CH.AUTN

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.CH.AUTN zu PrK.CH.AUTN (siehe Kapitel 6.4.7). Vorgaben zum Zertifikat finden sich in [gemX.509_eGK].

Tabelle 36: Attribute / MF / DF.ESIGN / EF.C.CH.AUTN

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C5 09´	
shortFileIdentifier	´09´= 9	
numberOfBytes	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1] OR C.2.3.4.5.6.8.9 OR {[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac AND SmRspEnc }	
UPDATE BINARY	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac AND SmCmdEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (50): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.4.3 / MF / DF.ESIGN / EF.C.CH.ENC

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.CH.ENC zu PrK.CH.ENC (siehe Kapitel 6.4.8). Vorgaben zum Zertifikat finden sich in [gemX.509_eGK].

Tabelle 37: Attribute / MF / DF.ESIGN / EF.C.CH.ENC

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C2 00´	
shortFileIdentifier	´02´= 2	
numberOfBytes	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
UPDATE BINARY	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (51): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.4.4 / MF / DF.ESIGN / EF.C.CH.ENCV

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.CH.ENCV zu PrK.CH.ENCV (siehe Kapitel 6.4.9). Vorgaben zum Zertifikat finden sich in [gemX.509_eGK].

Tabelle 38: Attribute / MF / DF.ESIGN / EF.C.CH.ENCV

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C5 0A´	
shortFileIdentifier	´0A´= 10	
numberOfBytes	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6 OR {[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac AND SmRspEnc }	
UPDATE BINARY	[AUT(SK.CMS) OR AUT(SK.VSDDCMS)] AND SmMac AND SmCmdEnc	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (52): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.4.5 / MF / DF.ESIGN / EF.DM

In dieser Datei wird ein benutzerspezifisches Geheimnis gespeichert, welches nur in geschützten Umgebungen auslesbar ist. Wird dieses Geheimnis dem Benutzer angezeigt, so ist dies als Indiz zu werten, dass eine geschützte Umgebung vorliegt.

Tabelle 39: Attribute / MF / DF.ESIGN / EF.DM

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 04´	
shortFileIdentifier	´04´= 4	
numberOfBytes	´0008´ Oktett = 8 Oktett	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	SmMac AND SmRspEnc	
UPDATE BINARY	PWD(PIN.home)	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (53): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

6.4.6 / MF / DF.ESIGN / PrK.CH.AUT

Der öffentliche Teil zu diesem privaten Schlüssel befindet sich in EF.C.CH.AUT, siehe Kapitel 6.4.1.

Tabelle 40: Attribute / MF / DF.ESIGN / PrK.CH.AUT

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´02´ = 2	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {rsaClientAuthentication, sign9796_2_DS2, signPKCS1_V1_5, signPSS}	für SE#1, SE#2
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4.5.6.9)]	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (54): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE

6.4.7 / MF / DF.ESIGN / PrK.CH.AUTN

Der öffentliche Teil zu diesem privaten Schlüssel befindet sich in EF.C.CH.AUTN, siehe Kapitel 6.4.2.

Tabelle 41: Attribute / MF / DF.ESIGN / PrK.CH.AUTN

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´06´ = 6	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	rsaClientAuthentication, siehe [gemSpec_eGK_P1]	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
INTERNAL AUTH. PSO Comp Dig Sig	PWD(PIN.home) OR [PWD(PIN.CH) AND C.1] OR C.2.3.4.5.6.8.9	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (55): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE

6.4.8 / MF / DF.ESIGN / PrK.CH.ENC

Der öffentliche Teil zu diesem privaten Schlüssel befindet sich in EF.C.CH.ENC, siehe Kapitel 6.4.3.

Tabelle 42: Attribute / MF / DF.ESIGN / PrK.CH.ENC

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´03´ = 3	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5}	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Decipher	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4.5.6)]	
PSO Transcipher	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.2.3.4.5.6)]	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (56): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

6.4.9 / MF / DF.ESIGN / PrK.CH.ENCV

Der öffentliche Teil zu diesem privaten Schlüssel befindet sich in EF.C.CH.ENCV, siehe Kapitel 6.4.4.

Tabelle 43: Attribute / MF / DF.ESIGN / PrK.CH.ENCV

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	´07´ = 7	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {rsaDecipherOaep, rsaDecipherPKCS1_V1_5}	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Decipher	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6	
PSO Transcipher	PWD(PIN.home) OR [PWD(PIN.CH) AND (C.1.9)] OR C.2.3.5.6	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (57): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

6.5 Beschreibung kryptographischer Objekte, CIA_ESIGN

In [prEN 14890–1] 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 [DIN 66291–4] verweist. Mit diesem Profile Identifier wird der Außenwelt mitgeteilt, dass alle FIDs, Schlüssel-IDs etc. in [DIN 66291–4] definiert sind. Ein EF.OD ist folglich nicht nötig.

Tabelle 44: Attribute / MF / DF.CIA_ESIGN

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	´E828BD080F A000000167455349474E´	siehe Hinweis (59):
FID	–	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (58): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Ordnerobjekt arbeiten sind:
ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis (59): Der Wert des Attributes applicationIdentifier enthält eine RID gemäß [7816–15] sowie als PIX den applicationIdentifier von DF.ESIGN (siehe Tabelle 34).

Hinweis (60): Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 6.2 nicht berücksichtigt zu werden.

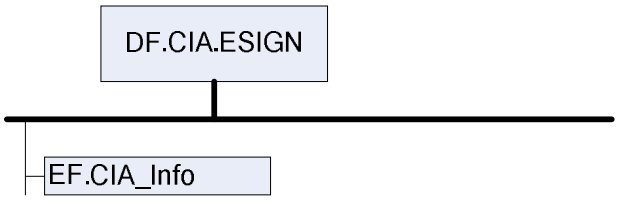

Abbildung 4: Objektstruktur der Anwendung DF.CIA.ESIGN

6.5.1 / MF / DF.CIA_ESIGN / EF.CIA_Info

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

Tabelle 45: Attribute / MF / DF.CIA_ESIGN / EF.CIA_Info

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´50 32´	siehe Hinweis (62):
shortFileIdentifier	´12´= 18	siehe Hinweis (62):
numberOfBytes	´0017´ Oktett = 23 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´30 15 | 02 01 01 | 03 01 00 | a6 0d | | 0c 0b 44494e2056203636323931´	siehe unten Version = 1 keine cardFlags profilIndication UTF8: „DIN V 66291“
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (61): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (62): Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [7816–15] festgelegt.

Hinweis (63): ASN.1 Werte:

```
ciaInfoExample CardInfo ::= {
        version v2,
        cardflags {  },
        profileIndication {
                "DIN V 66291"
        }
}
```

7 Qualifizierte elektronische Signatur (normativ)

Im Hinblick auf den Zustand der QES-Anwendung bei eGK–Ausgabe sind 3 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_eGK_P1]) nachzuladen. Entsprechende Rechte sind derzeit in der Anwendung *root* (siehe Tabelle 5) vorhanden. Bei diesem Nachladen ist es vom technischen Standpunkt aus möglich jeden der im Folgenden genannten Punkte zu erreichen. Ob dies aus sicherheitstechnischen Aspekten ratsam, bzw. bestätigungsfähig nach Signaturgesetz ist, ist nicht Gegenstand dieses Dokumentes.
- Die QES–Anwendung ist komplett angelegt und sofort nutzbar. Dieser Zustand wird in 7.1 beschrieben. PrK.CH.QES (siehe Tabelle 49) ist nutzbar und EF.C.CH.QES (siehe Tabelle 47) enthält ein Zertifikat.
- Die QES–Anwendung mit den benötigten Dateien inklusive der Zugriffsregeln ist angelegt. Im Gegensatz zum vorherigen Punkt ist aber in EF.C.CH.QES kein für Signaturzwecke nutzbares Zertifikat eingetragen. Möglicherweise fehlt auch das Schlüsselmaterial in PrK.CH.QES. Um diese Anwendung nutzbar zu machen, sind zuvor noch gewisse Schritte auszuführen. Welche das sind, hängt vom Auslieferungszustand der QES–Anwendung ab. Die dabei möglichen Optionen werden in Kapitel 7.2 beschrieben

7.1 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.

Der Fall einer noch nicht komplettierten QES–Anwendung wird in Kapitel 7.7 behandelt.

Tabelle 46: Attribute / MF / DF.QES

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	´D276000066 01´	siehe Hinweis (65):
FID	–	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (64): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Ordnerobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis (65): Der Wert des Attributes applicationIdentifier ist in [DIN 66291–4] festgelegt.

Hinweis (66): Da sich weder dieser Ordner noch der übergeordnete Ordner deaktivieren lassen, braucht dieser Zustand für Objekte im Kapitel 7.1 nicht berücksichtigt zu werden.
ACHTUNG: Die Situation in Kapitel7.7 ist dagegen komplett anders. Dort ist das Aktivieren der QES Anwendung Teil des Konzeptes zur Komplettierung dieser Anwendung.

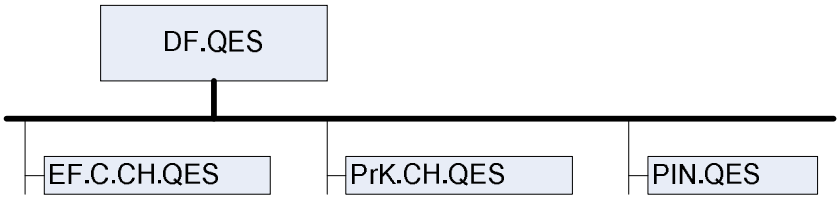

Abbildung 5: Objektstruktur der vollständigen Signaturanwendung

7.1.1 / MF / DF.QES / EF.C.CH.QES

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel zu PrK.CH.QES siehe Kapitel 7.1.3. Vorgaben zum Zertifikat finden sich in [gemX.509_eGK].

Tabelle 47: Attribute / MF / DF.QES / EF.C.CH.QES

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C0 00´	siehe Hinweis (68):
shortFileIdentifier	´10´= 16	
numberOfBytes	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, Zertifikat für PrK.CH.QES	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (67): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (68): Der Wert des Attributes fileIdentifier ist in [DIN 66291–4] festgelegt.

7.1.2 / MF / DF.QES / PIN.QES

Dieses Benutzergeheimnis wird zur Freischaltung der Signaturfunktionalität mit dem Schlüssel PrK.CH.QES (siehe Kapitel 7.1.3) benötigt.

Tabelle 48: Attribute / MF / DF.QES / PIN.QES

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
pwdIdentifier	´01´ = 1	
secret	…	wird personalisiert
minimumLength	6	siehe Hinweis (70):
startRetryCounter	3	
retryCounter	3	
transportStatus	…	wird personalisiert
flagEnabled	True	
startSsec	1	alle SE
PUK	…	wird personalisiert
pukUsage	10	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=0	ALWAYS	siehe Hinweis (71):
GET PIN STATUS	ALWAYS	
RESET RC., P1=1	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=1	ALWAYS	siehe Hinweis (72):
alle	NEVER	

Hinweis (69): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Passwortobjekt arbeiten, sind:
CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER, VERIFY

Hinweis (70): Gemäß [gemSpec_eGK_P1] kontrolliert das Betriebssystem der eGK lediglich die Mindestlänge. Die Maximallänge der PIN.QES beträgt acht Stellen. Die Einhaltung der Bedingung für die Maximallänge wird nicht von der eGK kontrolliert.

Hinweis (71): Die oben angegebene Zugriffsart für das Kommando CHANGE REFERENCE DATA gilt nur für den Fall, dass kein Transportschutz für dieses Passwortobjekt besteht. Je nach verwendetem Transportschutzverfahren KANN zur Aufhebung des Transportschutzes auch eine andere CHANGE REFERENCE DATA Variante verwendet werden.

Hinweis (72): Diese Zugriffsregel gilt nur für den Fall, dass DF.QES bei Auslieferung noch nicht komplett ist. Der Karteninhaber hat dann die Möglichkeit ohne Kenntnis des alten Wertes einen beliebigen Wert frei zu wählen und das beliebig oft. Im Rahmen der Komplettierung von DF.QES wird der LCS so geändert, dass dann nur noch mit Kenntnis des alten Wertes eine Änderung möglich ist.

7.1.3 / MF / DF.QES / PrK.CH.QES

Dieser private Schlüssel erstellt qualifizierte Signaturen. Der zugehörige öffentliche Teil findet sich in EF.C.CH.QES, siehe Kapitel 7.1.1.

Tabelle 49: Attribute / MF / DF.QES / PrK.CH.QES

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Signierobjekt	
keyIdentifier	´04´ = 4	siehe Hinweis (74):
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GEN. ASYM KEY P.	nicht Gegenstand dieser Spezifikation	
PSO Comp Dig Sig	PWD(PIN.QES)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

Hinweis (73): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Signierobjekt arbeiten, sind:
GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature

Hinweis (74): Der Wert des Attributes keyIdentifier ist in [DIN 66291–4] festgelegt.

7.2 Optionen für unvollständige QES–Anwendung

Die Unterkapitel 7.2 bis einschließlich 7.9 befinden sich derzeit in der Abstimmung mit der T7 Gruppe. Deshalb ist es möglich, dass sich deren Inhalt ändert.

Dieses Unterkapitel behandelt die verschiedenen Optionen, zwischen denen es einem ZDA möglich ist zu wählen, wenn die eGK im Auslieferungszustand keine nutzbare QES–Anwendung enthält.

Zunächst ist festzuhalten, dass die QES–Anwendung im hier behandelten Fall erst nutzbar ist, wenn gewisse Schritte erfolgreich ausgeführt wurden. Weil diese Schritte sicherheitsrelevant sind, ist technisch zu verhindern, dass sie von Unberechtigten ausführbar sind. Mit anderen Worten: Nur ein ZDA ist in der Lage, die notwendigen Schritte auszuführen. Deshalb sind in den Prozess folgende ZDAs eingebunden:

- ZDA–VP: ZDA, der die Vorpersonalisierung durchführt, dies kann auch ein von einem ZDA beauftragter Dritter gemäß § 4 Abs. 5 SigG sein.
- ZDA–NL: ZDA gemäß § 2 Nr. 8 SigG, der die Komplettierung der QES-Anwendung durchführt.

In Kapitel 7.3 werden die Optionen zum Aufbau eines geschützten Kommunikationskanals beschrieben. Dieser geschützte Kanal stellt sicher, dass nur Berechtigte die antizipierten Schritte ausführen. Als Optionen stehen dem ZDA–VP zur Verfügung:

- „TC.sym.DF“ gemäß Kapitel 7.3.1,
- „TC.asym.PrkMF.PukMF“ gemäß Kapitel 7.3.2.1,
- „TC.asym.PrkMF.PukDF“ gemäß Kapitel 7.3.2.1 und
- „TC.asym.PrkDF.PukDF“ gemäß Kapitel 7.3.2.1.

Die Option, dass der private Schlüssel DF–spezifisch ist und der öffentliche Schlüssel einer Root–CA des MFs zugeordnet ist, wird hier lediglich der Vollständigkeit halber erwähnt und nicht weiter betrachtet.

Des Weiteren hat der ZDA–VP die Wahl, ob das Schlüsselmaterial des Signaturschlüssels bei der Auslieferung vorhanden ist oder nicht. Dies wird in Kapitel 7.4 behandelt. Als Optionen stehen dem ZDA–VP zur Verfügung:

- „qesKeyNotAvailable“ gemäß Kapitel 7.4.1,
- „qesPukReadable“ gemäß Kapitel 7.4.2.1 und
- „qesPukCertificate“ gemäß Kapitel 7.4.2.1.

Falls ein Brief an den Karteninhaber der eGK zu versenden ist, der Daten zur Benutzerverifikation enthält (PIN / PUK Brief), so werden in den Kapiteln 7.5 und 7.5.1 Verfahren beschrieben, wie der ZDA–NL in den Besitz dieser Werte gelangt. Als Optionen stehen dem ZDA–VP die in [gemSpec_eGK_P1] Kapitel 9.2.5 definierten Verfahren zur Verfügung. Falls dabei ein Verfahren aus der Menge {

- „Transport–PIN_Zufallszahl“ (siehe Kapitel 7.5.1),
- „Transport–PIN_abgeleitet“ (siehe Kapitel 7.5.2)

} eingesetzt wird, dann beschreiben die zuvor referenzierten Kapitel, wie der ZDA–NL Kenntnis vom Wert der Transport–PIN erhält.

Aus dem technischen Blickwinkel der eGK ist es einem ZDA–VP möglich aus jedem der Unterkapitel 7.3, 7.4, 7.5 und 7.5.1 eine Option auszuwählen, wobei die jeweilige Auswahl in einem Unterkapitel völlig unabhängig von der Wahl in anderen Unterkapiteln ist. Es ist nicht Gegenstand dieses Dokumentes festzulegen, ob alle theoretisch möglichen Kombinationsmöglichkeiten auch in der Praxis genutzt werden.

7.3 Aufbau eines Trusted Channels

Dieses Unterkapitel behandelt die zur Wahl stehenden Möglichkeiten zum Aufbau eines geschützten Kommunikationskanals zwischen einer eGK und einem ZDA–NL. Grundsätzlich ist dabei zwischen symmetrischen (siehe Kapitel 7.3.1) und asymmetrischen Verfahren (siehe Kapitel 7.3.2) zu unterscheiden.

7.3.1 Trusted Channel mittels symmetrischer Schlüssel

Wird für den Aufbau des geschützten Kommunikationskanals die Option TC.sym.DF gewählt, dann MUSS in der QES–Anwendung ein DF–spezifisches symmetrischer Authentisierungsobjekt (siehe Tabelle 60) vorhanden sein.

(N20) Die gegenseitige Authentisierung und die Aushandlung von Sessionkeys MUSS gemäß [gemSpec_eGK_P1] Kapitel 16.4.1 „Symmetrische Aushandlung von Sessionkeys“ erfolgen.

7.3.2 Trusted Channel mittels asymmetrischer Schlüssel

Je nach Speicherort des verwendeten Schlüsselmaterials wird hier zwischen verschiedenen Verfahren unterschieden.

(N21) Die gegenseitige Authentisierung und die Aushandlung von Sessionkeys MUSS gemäß [gemSpec_eGK_P1] Kapitel 16.4.2 „RSA Schlüssel“ erfolgen. Als *algorithmIdentifier* wird dabei stets rsaSessionkey4SM verwendet.

7.3.2.1 Privater Schlüssel global, öffentlicher Schlüssel global

In der Variante TC.asym.PrkMF.PukMF basiert die gegenseitige Authentisierung auf einem

- privaten Schlüsselobjekt PrK.eGK.AUT_CVC (siehe Tabelle 14) zusammen mit dem ihm zugeordneten CV Zertifikat in Kapitel 6.2.3 und einem
- öffentlichen Schlüsselobjekt PuK.RCA.CS (siehe Tabelle 15), welches für den Import von Zertifikatsketten (siehe [gemSpec_eGK_P1] Kapitel 15.8.6) verwendet wird.

7.3.2.1 Privater Schlüssel global, öffentlicher Schlüssel DF–spezifisch

In der Variante TC.asym.PrkMF.PukDF basiert die gegenseitige Authentisierung auf einem

- privaten Schlüsselobjekt PrK.eGK.AUT_CVC (siehe Tabelle 14) zusammen mit dem ihm zugeordneten CV Zertifikat in Kapitel 6.2.3 und
- öffentlichen Schlüsselobjekt PuK.RCA–ZDA.CS (siehe Tabelle 59), welches für den Import von Zertifikatsketten (siehe [gemSpec_eGK_P1] Kapitel 15.8.6) verwendet wird.

7.3.2.1 Privater Schlüssel DF–spezifisch, öffentlicher Schlüssel DF–spezifisch

In der Variante TC.asym.PrkDF.PukDF basiert die gegenseitige Authentisierung auf einem

- privaten Schlüsselobjekt PrK.eGK.ZDA_AUT (siehe Tabelle 58) zusammen mit dem ihm zugeordneten CV Zertifikat in Kapitel 7.7.5 und
- öffentlichen Schlüsselobjekt PuK.RCA–ZDA.CS (siehe Tabelle 59), welches für den Import von Zertifikatsketten (siehe [gemSpec_eGK_P1] Kapitel 15.8.6) verwendet wird.

7.4 Existenz des Signaturschlüsselpaares

Dieses Unterkapitel behandelt die zur Wahl stehenden Möglichkeiten für das Schlüsselmaterial des Signaturschlüssels. Grundsätzlich ist dabei zu unterscheiden zwischen den Fällen, dass das Schlüsselmaterial zu Beginn der Komplettierung noch fehlt (siehe Kapitel 7.4.1) oder bereits vorhanden ist (siehe Kapitel 7.4.2).

7.4.1 Signaturschlüsselpaar nicht vorhanden

Zu Beginn der Komplettierung ist noch kein Schlüsselmaterial für PrK.CH.QES (keyAvailable = False, siehe Tabelle 49) vorhanden.

(N22) Das Schlüsselmaterial MUSS gemäß [gemSpec_eGK_P1] Kapitel 15.9.2.3 „Use Case Schlüsselgenerierung mit Ausgabe“ erzeugt werden. Dabei enthalten die Antwortdaten den Signaturprüfschlüssel.

Hinweis (75): Der ZDA–NL ist anschließend in der Lage ein Zertifikat für diesen Signaturprüfschlüssel zu erstellen und dieses in EF.C.CH.QES (siehe Tabelle 47) einzutragen.

7.4.2 Signaturschlüsselpaar vorhanden

Hier werden die Fälle betrachtet, dass zu Beginn der Komplettierung im Schlüsselobjekt PrK.CH.QES bereits Schlüsselmaterial vorhanden ist. Der ZDA–NL die im Folgenden beschriebenen Möglichkeiten, den Signaturprüfschlüssel auszulesen.

7.4.2.1 Signaturprüfschlüssel auslesbar

Zu Beginn der Komplettierung ist Schlüsselmaterial für PrK.CH.QES (keyAvailable = True, siehe Tabelle 49) vorhanden.

(N23) Der Signaturprüfschlüssel zu PrK.CH.QES MUSS gemäß [gemSpec_eGK_P1] Kapitel 15.9.2.2 „Use Case Auslesen eines zuvor erzeugten öffentlichen Schlüssels“ ausgelesen werden. Dabei enthalten die Antwortdaten den Signaturprüfschlüssel.

Hinweis (76): Der ZDA–NL ist anschließend in der Lage ein Zertifikat für diesen Signaturprüfschlüssel zu erstellen und dieses in EF.C.CH.QES (siehe Tabelle 47) einzutragen.

7.4.2.1 Signaturprüfschlüssel im Gütesiegel

Zu Beginn der Komplettierung ist Schlüsselmaterial für PrK.CH.QES (keyAvailable = True, siehe Tabelle 49) vorhanden.

(N24) Der Signaturprüfschlüssel zu PrK.CH.QES MUSS gemäß [gemSpec_eGK_P1] Kapitel 15.3.2 „READ BINARY“ aus der Datei EF.C.CH.QES (siehe Tabelle 47) ausgelesen werden. Dabei enthalten die Antwortdaten ein Gütesiegel (siehe Kapitel 7.9) mit dem Signaturprüfschlüssel.

Hinweis (77): Der ZDA–NL ist anschließend in der Lage ein Zertifikat für diesen Signaturprüfschlüssel zu erstellen und dieses in EF.C.CH.QES (siehe Tabelle 47) einzutragen.

7.5 Wert der Transport–-PIN für PIN.QES

7.5.1 Zufallszahl als Transport–-PIN

In diesem Dokument wird vorgeschlagen, den Wert einer zufälligen Transport–-PIN in einer Datei zu speichern (siehe Kapitel 7.7.2). Derzeit ist nicht geklärt, ob diese Vorgehensweise bestätigungsfähig ist. Falls nicht, dann ist auf andere Weise festzulegen, wie der ZDA–NL Kenntnis von der zufälligen Transport–-PIN erhält.

7.5.2 Transport–-PIN abgeleitet

In diesem Fall wird die Transport–-PIN aus einem Geheimnis und einem kartenindividuellen Merkmal CID1 abgeleitet. Dabei gilt mit den Definitionen aus Anhang C:

TransportPIN = BVD($Secret_{PIN}$, *CID1*, 5).

Durch dieses Dokument wird weder der Wert von $Secret_{PIN}$ festgelegt, noch wie dieser Wert vom ZDA–VP zum ZDA–NL transferiert wird.

7.6 Wert der PUK zu PIN.QES

7.6.1 Zufallszahl als PUK

In diesem Dokument wird vorgeschlagen, den Wert einer zufälligen PUK in einer Datei zu speichern (siehe Kapitel 7.7.2). Derzeit ist nicht geklärt, ob diese Vorgehensweise bestätigungsfähig ist. Falls nicht, dann ist auf andere Weise festzulegen, wie der ZDA–NL Kenntnis von der zufälligen PUK erhält.

7.6.2 PUK abgeleitet

In diesem Fall wird die PUK aus einem Geheimnis und einem kartenindividuellen Merkmal CID2 abgeleitet. Dabei gilt mit den Definitionen aus Anhang C:

PUK = BVD($Secret_{PUK1}$, *CID2*, 4) || BVD($Secret_{PUK2}$, *CID2*, 4).

Durch dieses Dokument werden weder der Wert von $Secret_{PUK1}$ noch von $Secret_{PUK2}$ festgelegt, noch wie diese Werte vom ZDA–VP zum ZDA–NL transferiert werden.

7.7 QES–Anwendung angelegt, aber noch nicht nutzbar

Dieses Unterkapitel enthält die Objekte, die eine (noch) nicht verwendungsfähige QES–Anwendung beschreiben. Dies ist gleichzeitig die Sicht eines ZDA–NL, der diese Anwendung nutzbar machen will. Falls bei der Auslieferung die QES–Anwendung komplett ist, dann ist Kapitel 7.1 relevant.

Tabelle 50: Attribute / MF / DF.QES

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
AID	´D276000066 01´	siehe Hinweis (79):
FID	–	
lifeCycleStatus	„Operational state (deactivated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
ACTIVATE	AUT(SK.Admin)	siehe Kapitel 7.3.1
	AUT(CHA.ZDA–NL)	siehe Kapitel 7.3.2
	AUT(SK.Admin) OR AUT(CHA.ZDA–NL)	Karte erlaubt sowohl 7.3.1 als auch 7.3.2
SELECT	ALWAYS	
andere	NEVER	

Hinweis (78): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, LOAD APPLICATION, SELECT

Hinweis (79): Der Wert des Attributes applicationIdentifier ist in [DIN 66291–4] festgelegt.

Hinweis (80): Der Wert von CHA.ZDL–NL ist ´4353 5051 4553 01´ = „CSPQES“ || ´01´.

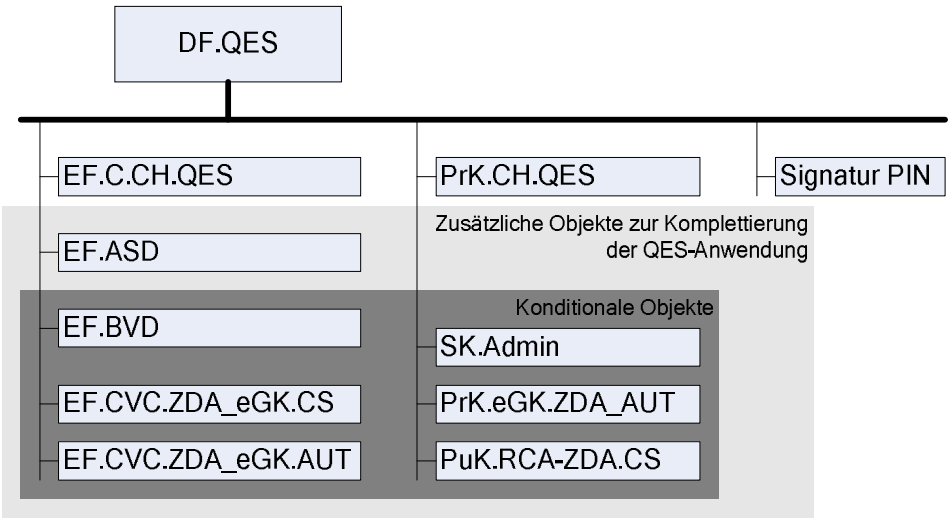

Abbildung 6: Objektstruktur der Signaturanwendung vor Komplettierung

7.7.1 / MF / DF.QES / EF.ASD

Diese Datei enthält anwendungsspezifische Informationen für den Komplettierungsprozess.

(N25) Diese Datei MUSS dann vorhanden sein, wenn die QES–Anwendung noch nicht komplettiert ist.

Tabelle 51: Attribute / MF / DF.QES / EF.ASD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 0A´	
shortFileIdentifier	´0A´= 10	
numberOfBytes	´0015´ Oktett = 21 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, siehe unten	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWASY	
SELECT	ALWAYS	
andere	NEVER	

Hinweis (81): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

(N26) Das Attribut body MUSS eine DER TLV kodierte Struktur enthalten.

(N27) Das erste Oktett von body MUSS den Wert ´6E´ besitzen. Dieses Tag zeigt an, dass anwendungsspezifische Informationen vorhanden sind.

(N28) Das zweite Oktett MUSS den Wert ´13´ = 19 besitzen und zeigt die Länge des Wertfeldes an.

(N29) Das erste Datenobjekt des Wertfeldes MUSS ein Tag = ´C1´ besitzen. Das Wertfeld dieses Datenobjektes enthält die Kennung des ZDA–VP. Werte sind der Tabelle 52 zu entnehmen.

(N30) Das zweite Datenobjekt des Wertfeldes MUSS ein Tag = ´C2´ besitzen. Das Wertfeld dieses Datenobjektes MUSS aus einem Oktett bestehen und enthält Informationen zum Aufbau eines geschützten Kommunikationskanals (siehe Kapitel 7.3). Das Wertfeld MUSS wie folgt kodiert werden (Bit b1 ist das „least significant bit“, Bit b8 das „most significant bit“:

a. Ein gesetztes Bit zeigt an, dass ein Verfahren unterstützt wird.
   Ein gelöschtes Bit zeigt an, dass ein Verfahren nicht unterstützt wird.
b. Bit b1 ist dem Verfahren TC.sym.DF aus Kapitel 7.3.1 zugeordnet.
c. Bit b2 ist dem Verfahren TC.asym.PrkDF.PukDF aus Kapitel 7.3.2.1 zugeordnet.
d. Bit b3 ist dem Verfahren TC.asym.PrkMF.PukDF aus Kapitel 7.3.2.1 zugeordnet.
e. Bit b4 ist dem Verfahren TC.asym.PrkMF.PukMF aus Kapitel 7.3.2.1 zugeordnet.
f. Die übrigen Bits sind für zukünftige Verfahren reserviert und MÜSSEN auf null gesetzt werden.

(N31) Das dritte Datenobjekt des Wertfeldes MUSS ein Tag = ´C3´ besitzen. Das Wertfeld dieses Datenobjektes MUSS aus einem Oktett bestehen und enthält Informationen zur Existenz des Signaturschlüsselpaares (siehe Kapitel 7.4). Das Wertfeld MUSS wie folgt kodiert werden (Bit b1 ist das „least significant bit“, Bit b8 das „most significant bit“:

a. Ein gesetztes Bit zeigt an, dass ein Verfahren unterstützt wird.
   Ein gelöschtes Bit zeigt an, dass ein Verfahren nicht unterstützt wird.
b. Bit b1 ist dem Verfahren qesKeyNotAvailable aus Kapitel 7.4.1 zugeordnet. Konsequenterweise sind dann die Bits b2 und b3 auf null zu setzen.
c. Bit b2 ist dem Verfahren qesPukReadable aus Kapitel 7.4.2.1 zugeordnet.
d. Bit b3 ist dem Verfahren qesPukCertificate aus Kapitel 7.4.2.1 zugeordnet.
e. Die übrigen Bits sind für zukünftige Verfahren reserviert und MÜSSEN auf null gesetzt werden.

(N32) Das vierte Datenobjekt des Wertfeldes MUSS ein Tag = ´C4´ besitzen. Das Wertfeld dieses Datenobjektes MUSS aus einem Oktett bestehen und enthält Informationen zum Wert der Transport–PIN (siehe Kapitel 7.5). Das Wertfeld MUSS gemäß [gemSpec_eGK_P1] Tabelle 9 „Transportschutzkodierung“ kodiert werden. Falls dabei der Wert „Transport–PIN_Zufallszahl“ angezeigt wird, so SOLL der Wert der Datei EF.BVD (siehe Kapitel 7.7.2) entnommen werden.

(N33) Das fünfte Datenobjekt des Wertfeldes MUSS ein Tag = ´C5´ besitzen. Das Wertfeld dieses Datenobjektes MUSS aus einem Oktett bestehen und enthält Informationen zum Wert der PUK (siehe Kapitel 7.6). Das Wertfeld MUSS wie folgt kodiert werden:

a. Der Wert ´00´ zeigt an, dass es keine PUK gibt.

b. Der Wert ´01´ zeigt an, dass eine achtstellige Zufallszahl als PUK verwendet wird. Der Wert SOLL der Datei EF.BVD (siehe Kapitel 7.7.2) entnommen werden.

c. Der Wert ´02´ zeigt an, dass eine achtstellige abgeleitete PUK verwendet wird. Der Wert ergibt sich gemäß Kapitel 7.6.2.

Tabelle 52: ZDA–VP Kennung in der Datei EF.ASD

ZDA–VP	ZDA Kennung	ASCII Wert
DGN Service GmbH	DEDGN	´4445 4447 4E´
Deutsche Post Com GmbH (Signtrust)	DEDPS	´4445 4450 53´
Deutscher Sparkassenverlag	DEDSV	´4445 4453 56´
D–Trust	DEDTR	´4445 4454 52´
TC–TrustCenter	DETCT	´4445 5443 54´
T–Systems Enterprise Services GmbH	DETSC	´4445 5453 43´
ROOT_ZDA	DEZDA	´4445 5A44 41´

Hinweis (82): Diese Tabelle enthält die derzeit gültigen Werte für ZDA Kennungen.

Hinweis (83): ZDA Kennungen werden für Deutschland zentral registriert, siehe http://sit.sit.fraunhofer.de/_karten_ident/SIT/rid_sde/ZDA.php

Hinweis (84): Beispielkodierung für den Inhalt von EF.ASD:

6E 13
| C1 05 4445445452 à ZDA–VP = D–Trust
| C2 01 05 à Verfahren aus den Kapiteln 7.3.1 und 7.3.2.1
| C3 01 06 à Auslesen PuK möglich per Gütesiegel oder GenAsymKeyPair
| C4 01 01 à Transport–PIN_Zufallszahl
| C5 01 00 à keine PUK

7.7.2 / MF / DF.QES / EF.BVD

Diese Datei enthält Benutzerverifikationsdaten.

(N34) Diese Datei MUSS genau dann vorhanden sein, wenn der Wert einer Transport–PIN oder der Wert einer PUK über diese Datei zum ZDA–NL transportiert wird (siehe Kapitel 7.5.1 und 7.6.1).

Tabelle 53: Attribute / MF / DF.QES / EF.BVD

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´D0 0B´	
shortFileIdentifier	´0B´= 11	
numberOfBytes	´000D´ Oktett = 13 Oktett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, siehe unten	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	AUT(SK.Admin)	siehe Kapitel 7.3.1
	AUT(CHA.ZDA–NL)	siehe Kapitel 7.3.2
	AUT(SK.Admin) OR AUT(CHA.ZDA–NL)	Karte erlaubt sowohl 7.3.1 als auch 7.3.2
SELECT	ALWAYS	
andere	NEVER	

Hinweis (85): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (86): Der Wert von CHA.ZDL–NL ist ´4353 5051 4553 01´ = „CSPQES“ || ´01´.

Das Attribut body enthält in den ersten acht Oktetten
– den ASCII kodierten Wert der PUK, oder
– achtmal den Wert ´00´, wenn hier keine PUK gespeichert wird.

Das Attribut body enthält ab dem neunten Oktett
– den ASCII kodierten Wert der Transport–PIN, oder
– fünfmal den Wert ´00´, wenn hier keine Transport–PIN gespeichert wird.

Hinweis (87): Beispiele für den Inhalt von EF.BVD:
*PUK = 12345678 Transport–PIN = 90123 **à** body = ´3132333435363738 3930313233,´*
*PUK fehlt Transport–PIN = 01234 **à** body = ´0000000000000000 3031323334´,*
*PUK = 02468135 Transport–PIN fehlt **à** body = ´3032343638313335 0000000000´,*
*PUK fehlt Transport–PIN fehlt **à** body = ´0000000000000000 0000000000´.*

7.7.3 / MF / DF.QES / EF.C.CH.QES

Diese Datei enthält nach der Komplettierung ein Zertifikat mit dem öffentlichen Schlüssel zu PrK.CH.QES. Vor der Komplettierung ist diese Datei entweder leer, oder sie enthält ein Gütesiegel.

(N35) Diese Datei MUSS vor der Komplettierung ein Gütesiegel (siehe Kapitel 7.9) enthalten, wenn der Signaturprüfschlüssel auf diese Art und Weise transportiert wird (siehe Kapitel 7.4.2.1).

(N36) Ein vorhandenes Gütesiegel MUSS im Rahmen der Komplettierung durch ein Zertifikat für Signaturschlüssel ersetzt werden.

Tabelle 54: Attribute / MF / DF.QES / EF.C.CH.QES

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´C0 00´	siehe Hinweis (89):
shortFileIdentifier	´01´= 1	
numberOfBytes	KANN passend zum Dateiinhalt gewählt werden	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´, Gütesiegelzertifikat für PrK.CH.QES	siehe 7.4.2.1
	´00…00´, falls kein Gütesiegel vorhanden ist	siehe 7.4.1, 7.4.2.1
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
UPDATE BINARY	AUT(SK.Admin)	siehe Kapitel 7.3.1
	AUT(CHA.ZDA–NL)	siehe Kapitel 7.3.2
	AUT(SK.Admin) OR AUT(CHA.ZDA–NL)	Karte erlaubt sowohl 7.3.1 als auch 7.3.2
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
UPDATE BINARY	AUT(SK.Admin)	siehe Kapitel 7.3.1
	AUT(CHA.ZDA–NL)	siehe Kapitel 7.3.2
	AUT(SK.Admin) OR AUT(CHA.ZDA–NL)	Karte erlaubt sowohl 7.3.1 als auch 7.3.2
alle	herstellerspezifisch	

Hinweis (88): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

Hinweis (89): Der Wert des Attributes fileIdentifier ist in [DIN 66291–4] festgelegt.

Hinweis (90): Der Wert von CHA.ZDL–NL ist ´4353 5051 4553 01´ = „CSPQES“ || ´01´.

7.7.4 / MF / DF.QES / EF.CVC.ZDA_eGK.CS

Diese Datei enthält ein CV–Zertifikat gemäß [gemSpec_eGK_P1], welches den öffentlichen Schlüssel einer CA enthält.

(N37) Diese Datei MUSS genau dann vorhanden sein, wenn der Aufbau eines geschützten Kommunikationskanals mittels asymmetrischer Verfahren stattfindet und ein DF–spezifisches privates Schlüsselobjekt verwendet wird (siehe Kapitel 7.3.2.1).

Tabelle 55: Attribute / MF / DF.QES / EF.CVC.ZDA_eGK.CS

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´CC 02´	
shortFileIdentifier	´04´= 4	
numberOfBytes	´0146´ Oktett = 326 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	

Hinweis (91): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

7.7.5 / MF / DF.QES / EF.CVC.ZDA_eGK.AUT

Diese Datei enthält ein CV–Zertifikat gemäß [gemSpec_eGK_P1], welches den öffentlichen Schlüssel zu PrK.eGK.ZDA_AUT (siehe Tabelle 58) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.CVC.ZDA_eGK.CS (siehe Tabelle 56) prüfen.

(N38) Diese Datei MUSS genau dann vorhanden sein, wenn der Aufbau eines geschützten Kommunikationskanals mittels asymmetrischer Verfahren stattfindet und ein DF–spezifisches privates Schlüsselobjekt verwendet wird (siehe Kapitel 7.3.2.1).

(N39) Für die CHR in diesem Zertifikat MUSS gelten CHR = ´0088´ || ICCSN wobei die ICCSN denselben Wert besitzen MUSS wie das Wertfeld aus (N17)b.

Tabelle 56: Attribute / MF / DF.QES / EF.CVC.ZDA_eGK.AUT

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	´CC 01´	
shortFileIdentifier	´03´= 3	
numberOfBytes	´0150´ Oktett = 336 Oktett	
flagTransactionMode	False	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
body	´XX…YY´	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”, alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
SELECT	ALWAYS	
andere	NEVER	

Hinweis (92): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem transparenten EF arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, UPDATE BINARY

7.7.6 / MF / DF.QES / PIN.QES

(N40) Dieses Objekt MUSS im Kontext der Komplettierung der QES–Anwendung exakt dieselben Eigenschaften haben, wie in Kapitel 7.1.2 beschrieben.

7.7.7 / MF / DF.QES / PrK.CH.QES

Tabelle 57: Attribute / MF / DF.QES / PrK.CH.QES

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Signierobjekt	
keyIdentifier	´04´ = 4	siehe Hinweis (94):
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True, falls qesPukCertificate oder qesPukReadable False, falls qesKeyNotAvailable	siehe Kapitel 7.4
algorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_eGK_P1] {sign9796_2_DS2, signPKCS1_V1_5, signPSS}	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Comp Dig Sig	PWD(PIN.QES)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
falls qesPukCertificate GEN. ASYM KEY P.	NEVER	siehe Kapitel 7.4.2.1
falls qesPukReadable, qesKeyNotAvailable GEN. ASYM KEY P.	AUT(SK.Admin)	siehe Kapitel 7.3.1
	AUT(CHA.ZDA–NL)	siehe Kapitel 7.3.2
	AUT(SK.Admin) OR AUT(CHA.ZDA–NL)	Karte erlaubt sowohl 7.3.1 als auch 7.3.2
andere	NEVER	

Hinweis (93): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Signierobjekt arbeiten, sind:
GENERATE ASYMMETRIC KEY PAIR, PSO Compute Digital Signature

Hinweis (94): Der Wert des Attributes keyIdentifier ist in [DIN 66291–4] festgelegt.

Hinweis (95): Der Wert von CHA.ZDL–NL ist ´4353 5051 4553 01´ = „CSPQES" || ´01´.

7.7.8 / MF / DF.QES / PrK.eGK.ZDA_AUT

(N41) Dieses Schlüsselobjekt MUSS genau dann vorhanden sein, wenn der Aufbau eines geschützten Kommunikationskanals mittels asymmetrischer Verfahren stattfindet und ein DF–spezifisches privates Schlüsselobjekt verwendet wird (siehe Kapitel 7.3.2.1).

Tabelle 58: Attribute / MF / DF.QES / PrK.eGK.ZDA_AUT

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Authentisierungsobjekt	
keyIdentifier	´08´ = 8	
privateKey	…, Moduluslänge 2048 Bit	wird personalisiert
algorithmIdentifier	rsaSessionkey4SM, siehe [gemSpec_eGK_P1]	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
INTERNAL AUTH.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
EXTERNAL AUTH.	ALWAYS	
INTERNAL AUTH.	ALWAYS	
andere	NEVER	

Hinweis (96): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem privaten Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE

7.7.9 / MF / DF.QES / PuK.RCA–ZDA.CS

(N42) Dieses Schlüsselobjekt MUSS genau dann vorhanden sein, wenn der Aufbau eines geschützten Kommunikationskanals mittels asymmetrischer Verfahren stattfindet und der Sicherheitsanker für den Zertifikatsimport DF–spezifisch ist (siehe Kapitel 7.3.2.1 und 7.3.2.1).

Tabelle 59: Attribute / MF / DF.QES / PuK.RCA–ZDA.CS

Attribute	Wert	Bemerkung
Objekttyp	öffentliches RSA Signaturprüfobjekt	
keyIdentifier	´XX…YY´, acht Oktette	wird personalisiert
publicKey	…, Moduluslänge 2048 Bit	wird personalisiert
oid	´2B24 0304 0202 03´ = {1 3 36 3 4 2 2 3}	
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Verify Cert.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Verify Cert.	ALWAYS	
andere	NEVER	

Hinweis (97): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind:
PSO Verify Certificate

7.7.10 / MF / DF.QES / SK.Admin

(N43) Dieses Schlüsselobjekt MUSS genau dann vorhanden sein, wenn der Aufbau eines geschützten Kommunikationskanals mittels symmetrischer Verfahren stattfindet (siehe Kapitel 7.3).

Tabelle 60: Attribute / MF / DF.QES / SK.Admin

Attribute	Wert	Bemerkung
Objekttyp	3TDES Authentisierungsobjekt	
keyIdentifier	´09´ = 9	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
algorithmIdentifier	desSessionkey4SM, siehe [gemSpec_eGK_P1]	für alle SE
Zugriffsregel für logischen LCS „Operational state (activated)", alle SE		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTAUL AUTH.	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTAUL AUTH.	ALWAYS	
andere	NEVER	

Hinweis (98): Kommandos, die gemäß [gemSpec_eGK_P1] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
EXTERNAL AUTHENTICATE, GET SECURITY STATUS KEY, MUTUAL AUTHENTICATE

7.8 Ablauf der Komplettierung (informativ)

Falls gemäß Kapitel 7.2 die QES–Anwendung nicht komplett ist, so ist sowohl die PIN.QES als auch der Signaturschlüssel PrK.CH.QES gesperrt. Im Zuge der Komplettierung werden diese Objekte entsperrt.

Im Folgenden wird ein beispielhafter Ablauf für die Komplettierung skizziert. Es handelt sich dabei nur um ein Beispiel, weil in gewissen Grenzen auch andere Reihenfolgen denkbar sind.

Für die Komplettierung wird vorgeschlagen, wie folgt vorzugehen:

1) *Der ZDA–NL selektiert den Ordners DF.QES*
2) *Auslesen der Datei EF.ASD, dabei werden Informationen über die weitere Vorgehensweise gewonnen.*
3) *Aufbau eines geschützten Kommunikationskanals mittels eines Verfahrens, welches in EF.ASD angezeigt wird (siehe (N30)). Dazu ist es erforderlich, kartenindividuelle Merkmale aus dem root Verzeichnis auszulesen. Zusätzlich ist es je nach Verfahren notwendig CV–Zertifikate aus dem root Verzeichnis auszulesen.*
4) *Falls in EF.ASD (siehe (N31)) angezeigt wird, dass noch kein Signaturschlüsselpaar existiert, dann wird dieses erzeugt (siehe (N22).*
   Andernfalls wird der Signaturprüfschlüssel gemäß der Anzeige in (N31) entsprechend Kapitel 7.4.2 ausgelesen.
5) *Vom ZDA–NL wird ein Zertifikat für den Signaturprüfschlüssel erzeugt und in EF.C.CH.QES (siehe Kapitel 7.7.3) eingetragen.*
6) *Falls erforderlich wird EF.BVD ausgelesen, damit ein PIN / PUK Brief erzeugbar ist.*
7) *Zwecks Aktivierung der Signaturfunktionalität wird der Ordner DF.QES aktiviert. Danach ist es möglich überflüssige Dateien (etwa EF.ASD, EF.BSD oder CV–Zertifikate in DF.QES) zu löschen. Weitere administrative Operationen sind gemäß den derzeitigen Zugriffsregeln dann NICHT mehr möglich.*

7.9 Gütesiegel

7.9.1 Zertifikatshierarchie für Gütesiegel

Zur Ausstellung von Gütesiegeln betreibt jeder ZDA eine eigene PKI mit einer eigenen Root–CA sowie optional einer oder mehreren Transport–CAs. Zur Erstellung von Gütesiegeln wird ein Transport–CA–Zertifikat eines so genannten Transport–Signers verwendet (in der eGK wird jedoch nur das Gütesiegel abgelegt). Ein Gütesiegel des ZDA_X ist so von jeder anderen für diesen Anwendungskontext zugelassenen ZDA_Y prüfbar.

Ein Transport–Signer bietet den Vorteil, dass ein einfaches Sperrmanagement von ganzen Mengen von Gütesiegeln möglich wird, indem ein solcher Signer gegebenenfalls ganz gesperrt werden kann. Es ist möglich, dass ein solcher Transport–Signer auch im Auftrag eines ZDA bei einem Kartenproduzenten steht und dann bei Missbrauch vollständig abgeschaltet wird.

Diese Struktur bietet den Vorteil, dass die gegenseitige Anerkennung verschiedener ZDAs flexibel gehandhabt werden kann. So ist es etwa möglich, dass ein ZDA anhand der Root eines anderen ZDAs die gesamte Transport–PKI–Hierarchie dieses ZDAs in sein Sicherheitskonzept integriert, während ein weiterer ZDA gegebenenfalls nur einen bestimmten Transport–Signer integriert.

Auf eine gemeinsame Root wird aus praktischen Gründen verzichtet. Jeder ZDA–NL integriert im Rahmen der Bestätigung seines Sicherheitskonzeptes die Roots der darin aufgenommenen ZDA–VPs. Die Bekanntgabe wird im Rahmen des für die Integration ins Sicherheitskonzept notwendigen Vertrages zwischen ZDA–VP und ZDA–NL geregelt.

7.9.2 Zertifikatsprofile

Für Root– und Signer–Zertifikate werden übliche Zertifikatsprofile zu [X.509v3] ohne besondere Anforderungen verwendet. Signer–Zertifikate ersetzen in diesem Zusammenhang die sonst üblichen CA–Zertifikate. Zur Kennzeichnung, dass es sich um eine PKI zur Ausgabe von X509–Gütesiegeln handelt, müssen die "CommonNames" (CN) folgendem Schema folgen:

- Root-CA-Zertifikate: CN = [ZDA] Transport Root [Jahr],
  Beispiel: "XY-ZDA Transport Root 05"
- CA-Zertifikate: CN = [ZDA] Transport Signer [Jahr],
  Beispiel: "XY-ZDA Transport Signer 05"

Für die Gütesiegel soll ein Zertifikatsprofil zu [X.509v3] mit folgenden Merkmalen verwendet werden:

Tabelle 61: Zertifikatsprofil für X.509 Gütesiegel

Attribute	Inhalt	Kommentar
Version	2	V3
SerialNumber	<Seriennummer>	
SignatureAlgorithm Identifier	1 2 840 113549 1 1 5	sha1withRSAEncryption
Issuer		
Country	<Länderkürzel>	
Organisation	<ZDA>	
Organisational Unit	<ZDA>	Attribut für weitere Beschreibung des ZDA
Common Name	>Name d. Transport Signer>	Format: CN = [ZDA] Transport [Personalisierer xyz] [Jahr], z.B."ZDA XY Transport Signer 0"
Validity		
Not Before	<Datum Erstellung>	Die Gültigkeit wird durch den ZDA festgelegt, es werden keine Vorgaben gemacht. Eine Gültigkeitsdauer wird gesetzt, um die Verarbeitung mit Standardsoftware zu ermöglichen, sie hat aber keine Bedeutung für die tatsächliche Dauer der Verwendbarkeit des enthaltenen öffentlichen Schlüssels. Diese richtet sich z.B. nach dem Algorithmenkatalog oder anderen Anforderungen an Schlüssel für qualifizierte Zertifikate
Not After	<Datum Erstellung + Gültigkeitsdauer>	
Subject		
Country	<Länderkürzel>	
Organisation Name	<ZDA>	
Organisational Unit	<ZDA>	
Common Name	ICSN	Chip-Seriennummer
SubjectPublicKeyInfo	1 2 840 113549 1 1 1	rsaEncryption
	<Public key des Signaturschlüssels>	Da es sich bei einem GS um ein Zertifikat über den Public Key des später zu erzeugenden qualifizierten Zertifikats handelt, steht hier der öffentliche Schlüssel des Signatur-Schlüsselpaares
CertificatePolicies	<Policy-OID>	Es wird eine für alle ZDAs einheitliche OIDgesetzt, welche als Kennzeichnung, dass es sich um ein GS handelt, wie folgt definiert Die OID beschreibt, dass das Schlüsselpaar geeignet ist, d.h. dass es aus einem evaluierten und nach SigG bestätigten Schlüsselgenerator stammt. Die OID beschreibt, dass es sich bei Karte um eine evaluierte und nach bestätigte Signaturkarte handelt.
AuthorityKeyID	<ID>	
SubjectKeyIdentifier	<ID>	

Anhang A (informativ)

A1 – Abkürzungen

Kürzel	Erläuterung
AID	Application Identifier
BCD	Binary Coded Decimal
CAMS	Card Application Management System, System zur Administration von Karten und Applikationen
CHA	Certificate Holder Authorization, Rechte, die ein Zertifikatsinhaber besitzt
CIA	Cryptographic Information Application, Anwendung mit Informationen zu kryptographischen Diensten
CIO	Cryptographic Information Object, Objekt mit Informationen zu einem kryptographischen Dienst
CVC	Card Verifiable Certifcate, kartenverifizierbares Zertifikat
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
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
VSD	Versichertenstammdaten
ZDA	Zertifizierungsdiensteanbieter
ZDA–VP	ZDA Vorpersonalisierung; ein ZDA, der die eGK mit einer QES–Anwendung ausstattet, die (noch) nicht nutzbar ist
ZDA–NL	ZDA Nachladen; ein ZDA, der eine QES–Anwendung nutzbar macht

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[3166]	ISO/IEC 3166: Codes for the representations of names of countries
[7816–4]	ISO/IEC 7816–4: 2005 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[7816–15]	ISO/IEC 7816–15: 2004 Identification cards - Integrated circuit cards - Part 15: Cryptographic information application
[8825–1]	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
[DIN 66291–4]	Chipcards with digital signature application/function according to SigG and SigV Part 4: Basic Security Services, September 14th 2001
[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
[gemCMS_PINPUK]	gematik (25.03.2008): Einführung der Gesundheitskarte – Beschreibung der zulässigen PIN- und PUK–Verfahren für die eGK Version 1.2.0
[gemeGK_Fach]	gematik (18.03.2008): Einführung der eGK – Speicherstrukturen der eGK für Gesundheitsanwendungen Version 1.6.0
[gemPKI_Reg]	gematik (18.03.2008): Einführung der Gesundheitskarte – Registrierung einer CVC-CA der zweiten Ebene Version 1.5.0
[gemSiKo]	gematik (10.03.2008): Einführung der Gesundheitskarte -

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.2.0
[gemSpec_eGK_P1]	gematik (20.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte Teil 1: Spezifikation der elektrischen Schnittstelle Version 2.2.0
[gemX.509_eGK]	gematik (26.11.2007): Einführung der Gesundheitskarte – Festlegungen zu den X.509-Zertifikaten der Versicherten Version 1.4.0
[prEN 14890–1]	EUROPEAN STANDARD, DRAFT, prEN 14890-1, February 2007 Application Interface for smart cards 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
[X.509v3]	ITU-T X.509: Information Technology – Open Systems Interconnection – The Direc-tory: Authentication Framework, 1997

A6 – Klärungsbedarf

Kap.	Offener Punkt	Zuständig
7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9	Der Abschnitt über das Komplettieren einer QES Anwendung befindet sich derzeit in der Abstimmung mit der T7 Gruppe	gematik, AFI
Anhang C	Funktion zur Ableitung von Benutzerverifikationsdaten: Muss dies in diesem Dokument festgelegt werden? Welche Ableitungsfunktion?	gematik, AFI

Anhang B: Zuordnung Rollen zu Berufsgruppen (informativ)

Tabelle 62 listet die derzeit verwendeten CHA Werte auf, die auf der eGK im Rahmen der PKI verwendet werden, bei welcher PuK.RCA.CS (siehe Kapitel 6.2.10) an der Wurzel steht. Dazu steht in Spalte eins der Tabelle der symbolische und in Spalte zwei der numerische Wert. Die gezeigten Werte sind dem normativen Anhang A.3.1 von [gemPKI_Reg] entnommen worden und werden hier lediglich wiederholt.

Tabelle 63 zeigt den aktuellen Stand für die Zuordnung der symbolischen Werte zu Kartenart und Akteur, wie sie in den entsprechenden Fachkonzepten und Facharchitekturen beschrieben ist.

Die Information der Tabelle richtet sich an

- die Gruppe derjenigen, welche prüft, ob die fachlichen Vorgaben über Zugriffsrechte korrekt abgebildet sind und
- an die Trustcenter, welche entsprechende Karten mit den zugehörigen Rollen ausstatten.

Tabelle 62: Zuordnung Symbol zu CHA–Wert gemäß [gemPKI_Reg]

Symbol	CHA Wert
CHA.0	'D276 0000 4000 00'
CHA.1	'D276 0000 4000 01'
CHA.2	'D276 0000 4000 02'
CHA.3	'D276 0000 4000 03'
CHA.4	'D276 0000 4000 04'
CHA.5	'D276 0000 4000 05'
CHA.6	'D276 0000 4000 06'
CHA.7	'D276 0000 4000 07'
CHA.8	'D276 0000 4000 08'
CHA.9	'D276 0000 4000 09'

Tabelle 63: Zuordnung Rollen zu Kartenart und Berufsgruppen (informativ)

Profil	Fachlicher Akteur	Erläuterungen	Träger des CV–Zertifikates
CHA.0		Dieses Profil hat keine Rechte gegenüber der eGK	SMC–B (siehe unten)
CHA.1	Versicherter	Das Profil wird zur Freischaltung der eGK am eKiosk verwendet. Da die Nutzung durch den Versicherten erfolgt, ist der fachliche Akteur der Versicherte.	SM eKiosk (in Abstimmung)
CHA.2	Arzt		HBA
	Mitarbeiter medizinische Institution	Neben der Verwendung der CV Zertifikate für die Freischaltung der eGK aus einer fachlichen Sicht werden technisch X.509–Zertifikate der SMC–B für die Authen-	SMC–A und SMC–B

		tifizierung der Organisation (Arztpraxis/Zahnarztpraxis) für den Zugang zur TI und die Aktivierung des Konnektors benötigt.	
CHA.3	Apotheker		HBA
	Mitarbeiter Apotheke	Neben der Verwendung der CV Zertifikate für die Freischaltung der eGK aus einer fachlichen Sicht werden technisch X.509–Zertifikate der SMC-B für die Authentifizierung der Organisation (Apotheke/ Krankenhausapotheke) für den Zugang zur TI und die Aktivierung des Konnektors benötigt	SMC–A und SMC–B
CHA.4	Psychotherapeut		HBA
CHA.0	Der Mitarbeiter in der psychotherapeutischen Praxis ist nicht definiert.	Die SMC–B wird für die Authentifizierung der Organisation (Psychotherapeutische Praxis) für den Zugang zur TI und die Aktivierung des Konnektors benötigt. Die Ausgabe einer SMC–B ohne CV- Zertifikate ist nicht zulässig. Da es keine fachliche Motivation für die Zugriffe von Mitarbeitern in der psychotherapeutischen Praxis auf die eGK gibt, darf diese keine Rechte gegenüber der eGK haben, daher bekommt die SMC–B das Profil 0 im CV–Zertifikat."	SMC–B
CHA.5	Heilmittelerbringer mit (H)BA (noch nicht definiert) Hilfsmittelerbringer mit (H)BA (noch nicht definiert)	Es ist noch nicht endgültig festgelegt, welche Art von Ausweis hier ausgegeben wird.	(H)BA sonstige Leistungserbringer
CHA.0	Der Mitarbeiter in der Institution eines Heilmittelerbringers/Hilfsmittelerbringers (noch nicht definiert)	Die SMC–B wird für die Authentifizierung der Organisation (Institution eines Heilmittelerbringers/ Hilfsmittelerbringers) für den Zugang zur TI und die Aktivierung des Konnektors benötigt. Die Rechte gegenüber der eGK sind noch zu definieren. Vorläufig bekommt die SMC–B das Profil 0 im CV–Zertifikat und erhält somit keine Rechte gegenüber der eGK. Die finale Festlegung muss vor der Ausgabe der SMCs an die entsprechenden Organisationen erfolgen. Eine Anpassung der eGK zu diesem Zeitpunkt ist nicht mehr notwenig.	(SMC–A und) SMC–B
CHA.6	kein fachlicher Akteur	Dieses Profil wird vorgehalten, um für mögliche spätere Anwendungen, die einen Online-Zugriff auf die eGK benötigen, immer einen Trusted Channel zur eGK zu erzwingen. Es sind bislang keine Anwendungsfälle für die Nutzung definiert, allerdings würde die nachträgliche Einführung einen Austausch der eGK verursachen, so dass dies bereits vorab vorgesehen wird.	SMC–B
CHA.7	Mitarbeiter Rettungswesen	Es ist noch nicht endgültig festgelegt, welche Art von Ausweis hier ausgegeben wird	(H)BA
CHA.8	Verwaltungsmitarbeiter Instituti	Der Verwaltungsmitarbeiter Institution erhält durch das BMG definierte Rechte gegenüber der eGK. Die Zu	SMC–A und SMC–B

	on	weisung, welche Institutionen eine Karte mit diesem Profil erhalten dürfen, ist bislang noch nicht definiert.	
CHA.9	Mitarbeiter medizinische Institution zur eGK_Anwenderunterstützung (eGK_AWU)	Der Mitarbeiter medizinische Institution zur eGK_Anwenderunterstützung erhält vordefinierte Rechte für den Zugriff auf der eGK. Die Zuweisung, welche Institutionen eine Karte mit diesem Profil erhalten dürfen, ist bislang noch nicht definiert.	SMC–A und SMC–B

Anhang C: Ableitung Benutzerverifikationsdaten (informativ)

Dieser Abschnitt beschreibt die Ableitung von Benutzerverifikationsdaten (PIN oder PUK) aus einem Geheimnis:

Input:	*S*	Oktettstring, Geheimnis
	CID	Oktettstring, Card Individual Data
	n	positive Zahl, Anzahl der Stellen in *out*
Output:	*out*	Oktettstring der Länge *n* Oktett, welche ASCII kodiert die Benutzerverifikationsdaten enthalten
Notation:		*out* = BVD(*S*, *CID*, *n*)

Hinweis (99): Derzeit wird in diesem Dokument nicht festgelegt, wie die Benutzerverifikationsdaten aus dem Geheimnis berechnet werden. Das in der Vorgängerversion beschriebene Verfahren verwendete dabei einen 2TDES Algorithmus.

Anhang D: Übersicht Zugriffsrechte (informativ)

Tabelle 64: Abkürzungen für die Matrix der Zugriffsrechte in DF.HCA und DF.ESIGN

ALW	Aktion kann jederzeit von jedermann ausgeführt werden
home	Aktion kann nach Eingabe von PIN.home ausgeführt werden
1	Aktion kann nach Rollenauthentisierung im Profil 1 ausgeführt werden
3 + CH	Aktion kann nach Rollenauthentisierung im Profil 3 UND Eingabe von PIN.CH ausgeführt werden
CMS	Rolle des CMS repräsentiert durch den Schlüssel SK.CMS oder SK.VSDDCMS
VSDD	Rolle des VSDD repräsentiert durch den Schlüssel SK.VSDD oder SK.VSDDCMS
C, Create	Recht neue Dateien, PINs oder Schlüssel anzulegen
E, Erase	Recht, Inhalte einer Datei zu „nullen“, das heißt zu löschen (siehe Hinweis (101):)
L, Löschen	Recht das entsprechende File zu löschen (Abkürzung D wird schon verwendet)
R, Read	Recht zu lesen und in strukturierten Dateien zu suchen (SEARCH RECORD)
U, Update	Recht zu Schreiben und zu Überschreiben (siehe Hinweis (101):)
A, Activate	Recht ein File zu aktivieren, dabei werden auch alle Rekords sichtbar
D, Deactivate	Recht in einer Datei enthaltene Rekords zu deaktivieren (verbergen)
a, Append	Anhängen eines Rekords in einer strukturierten Datei.
I, Inter. Auth.	INTERNAL AUTHENTICTAE, Recht von der eGK eine Authentisierung zu fordern
S, PSO CDS	PSO Compute Digital Signature, Recht eine elektronische Signatur zu erzeugen
V, PSO DEC	PSO Decipher, PSO Transcipher Recht von der eGK Daten entschlüsseln zu lassen

Hinweis (100): Diese Tabelle listet Abkürzungen aus Tabelle 65.

Hinweis (101): Derzeit wird in [gemSiKo] festgelegt, dass das Löschen von Informationen durch Überschreiben realisiert wird. Technisch wird derzeit innerhalb der TI in beiden Fällen ein UPDATE Kommando verwendet. In Zukunft ist es denkbar, dass für Schreiboperationen ein UPDATE und für das Löschen von Information ein ERASE Kommando verwendet wird.

Tabelle 65: Matrix der Zugriffsrechte in DF.HCA und DF.ESIGN

Object	ALW	home	1	1+CH	8	8+CH	2	2+CH	9	9+CH	3	3+CH	4	4+CH	5	5+CH	6	6+CH	7	7+CH	CMS	VSDD
DF.HCA																					CAD	
EF.PD EF.VD EF.StatusVD	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	RCL	RU
EF.GVD		R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	CL	RU
EF.Einwilligung		RAD		RAD				RUAD				RUAD		RUAD				R				
EF.Verweis		RUAD		RUAD				RUAD		RU		RUAD		RUAD				R				
EF.eVerordnungs-Tickets		READ		READ			RUE	RUE		RE	RUE	RUE			RUE	RUE	RUE	RUE				
EF.eVerordnungs-Container		R		R			RU	RU		R	RU	RU			RU	RU	RU	RU			CL	
EF.StatusVerord-nungen		RU		RU			RU	RU		RU	RU	RU			RU	RU	RU	RU			U	
EF.Notfalldaten und EF.StatusNotfalldaten		AD		AD			R	RUE				RE		RE					R	R		
EF.Logging		R		Ra	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a		
EF.TTN		R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	RUCL	RU
DF.ESIGN																						
EF.C.CH.AUT EF.C.CH.ENC	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	RU	R
PrK.CH.AUT		IS		IS				IS		IS		IS		IS		IS		IS				
PrK.CH.ENC		V		V				V				V		V		V		V				
EF.C.CH.AUTN		R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R			RU	
EF.C.CH.ENCV		R		R			R	R		R	R	R			R	R	R	R			RU	
PrK.CH.AUTN		IS		IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS				
PrK.CH.ENCV		V		V			V	V		V	V	V			V	V	V	V				

*Hinweis (102): Die obige Tabelle stellt die Zugriffsrechte vereinfacht dar. Tabellen in den Kapiteln 6.3 und 6.4 zeigen die Zugriffsrechte detailliert aus **technischer** Sicht.*