gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Die Spezifikation der elektronischen Gesundheitskarte

Teil 2: Anwendungen und anwendungsspezifische Strukturen

Version:	1.5.1
Stand:	27.08.07
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

In die vorliegende Version wurden folgende, bisher auf der Internetseite der gematik veröffentlichte SRQs zur Version 1.2.1 eingearbeitet:

1. Enthält EF.CVC.CA_eGK.CS das Zertifikat der CVC-Root?
   Kapitel 3.2.5 und Tabelle B.1 letzte Zeile korrigiert
2. Kodierung in ARR#1
   Tabelle B.6 Record 1 korrigiert
3. Kodierung in ARR#9
   Tabelle B.6 Record 9 korrigiert
4. Flagliste für StatusPIN
   Tabelle H.4 angepasst
5. inkonsistente Datumsformate
   Tabelle H.1 geändert

Im Weiteren wurde der Abschnitt zur Versionierung (Kap. 3.2 und Anhang B.2ff) an die aktuellen Festlegungen in [gemSpec_Vers] angepasst.

Schließlich wurden die Zugriffsregeln geändert und die entsprechenden Abschnitte in Anhang B.3.2 und B.4.2 vollständig überarbeitet.

Der Anhang G.3 (Einlösen von eRezepten bei einer Apotheke mit Online-Einlösung) wurde gestrichen.

Inhaltliche Änderungen gegenüber der Vorversion sind gelb markiert. Sofern ganze Kapitel eingefügt wurden, wurde zur besseren Lesbarkeit lediglich die Überschrift durch gelbe Markierung hervorgehoben.

Referenzierung

Das Dokument wird von anderen gematik-Dokumenten referenziert als:

[gemSpec_eGK_P2]	gematik (27.08.07): Die Spezifikation der elektronischen Gesundheitskarte – Teil 2: Anwendungen und anwendungsspezifische Strukturen Version 1.5.1

Dokumentenhistorie

Version	Stand	Kap. Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
V0.7	06.11.04		1. Version zur Kommentierung	gematik
V0.8	07.01.05		2. Version zur Kommentierung	gematik
V0.9	20.02.05		3. Version zur Kommentierung	gematik
V1.0	10.03.05		CeBIT-Version	gematik

Version	Stand	Kap. Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
V1.1 (Draft)	05.04.05		Pre-Final Version - Ergänzung von DF.QES zum Nachladen einer qualifiz. Signaturfunktion - Modifikation DF.ESIGN - Ergänzung Display Message - Überarbeitung Versichertendaten (zu schützende Dos, EHIC-Kompat.)	gematik
Übernahme durch ***gematik***, Versionierung neu begonnen				

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 Überarbeitung auf Konsistenz Einarbeitung Nachladen qualifizierter elektronischer Signatur Einarbeiten der Verfahren zur Nutzung des Schlüssels PrK.CH.ENC	gematik, AG3
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	gematik, AG3

Version	Stand	Kap. Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Erweiterung Versichertendaten Aktualisierung QES-Nachladeverfahren	
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
1.3.1	17.07.07		Einarbeitung Kommentare	gematik, AG7
1.4.0	01.08.07		freigegeben	gematik
1.4.1	15.08.07	Kapitel 1.2 und 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

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: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform

  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 Dateistrukturen der Pflichtanwendungen und der zugehörigen Datenelemente, die bei der Initialisierung und Personalisierung in die eGK geladen werden.

  Insbesondere sind hierin die Dateistrukturen der Anwendungen „Versichertenmanagement“, „elektronisches Rezept“, „qualifizierte Signatur“ und „eSign Anwendung“ spezifiziert. Dazu gehören entsprechende statische Daten sowie die Strukturen und Datencontainer für Zertifikate und Schlüsselelemente.

- **Die Spezifikation der elektronischen Gesundheitskarte**
  Teil 3: Äußere Gestaltung

  Der Teil 3 beschreibt die äußere Gestaltung der eGK. Hier werden die Bereiche auf der eGK festgelegt, in denen das Lichtbild des Versicherten sowie seine Unterschrift vorgesehen sind. Die Kartenrückseite wird entsprechend den Vorgaben für die europäische Krankenversicherungskarte definiert.

1.2 Ergänzende Dokumente zur eGK

- **Speicherstrukturen der eGK für Gesundheitsanwendungen**

  Das Dokument fasst die Daten und Datenstrukturen zusammen, die für die Realisierung der Anwendungen für 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.

  - **XSD-Schema**

    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.

- **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 [gemX.509_eGK] trifft die erforderlichen Festlegungen zur Versichertenidentität, zur Pseudonymisierung von AUTN und ENCV, zur Schlüsselverwendung und zur Zertifikatsvalidierung.

- **Aktivierung der Signaturzertifikate in der eGK für qualifizierte elektronische Signaturen**

  Beschreibung der erforderlichen technischen Festlegungen zum nachträglichen Laden von qualifizierten Signaturzertifikaten auf die eGK unter Berücksichtigung der gesetzlichen Vorgaben.

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

  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.

1.3 Das Schalenmodell der Dokumentenstruktur

Die Dokumente der technischen Spezifikation zur elektronischen Gesundheitskarte eGK werden nach einem Schalenmodell gegliedert. Dieses Modell ist modular aufgebaut und strukturiert die Dokumente und Prozesse, die sowohl für die Herstellung der Karte als auch für die nachfolgende Initialisierung und Personalisierung relevant sind.

Der innere Bereich (Teil1) beinhaltet die Spezifikation, die aufgrund ihres Reifegrades als Basis für die Ausschreibung von Betriebssystem, Mikroprozessorchip und Kartenkörper geeignet ist. Es handelt sich um die Basiskommandos, Sicherheitsfunktionen und - algorithmen sowie Grundfunktionen des Betriebssystems (sog. hard facts). Diese Spezifikation ist Grundlage der Entwicklung der Kommandostrukturen und –funktionen für eGK-konforme Chipkartenbetriebsysteme. Weiterhin definiert sie die ROM-Maske für den Halbleiter (Fertigungsmuster des Halbleiters). Teil 1 beinhaltet auch die Spezifikationen für die Sicherheitsfunktionen und kryptografischen Algorithmen der eGK.

Die nächste Schale, der Teil 2, enthält die Spezifikationen für die Dateistrukturen der Anwendungen und der zugehörigen Datenelemente. Diese werden bei der Initialisierung und Personalisierung auf die eGK gebracht. In Teil 2 sind insbesondere die Dateistrukturen der Anwendungen Versichertenmanagement, elektronisches Rezept, Notfalldaten, Protokollierung, qualifizierte Signatur und eSign Anwendung enthalten. Dazu gehören entsprechende statische Daten sowie die Strukturen und Datencontainer.

In der äußeren Schale sind die Spezifikationen für die Personalisierung enthalten. Diese beschreiben die Verfahren der Personalisierung, die zu personalisierenden Daten sowie sicherheitstechnische und organisatorische Vorraussetzungen hierfür.

Die ISO-konformen Dateistrukturen der eGK Anwendungen können ggf. nach Produktion der Karte verändert werden. Spezifikationen für weitere bzw. zukünftige Anwendungen, zugehörige Datenstrukturen und Datenelemente auf Basis der eGK können nach Fertigstellung in Teil 2 bzw. die äußere Schale eingestellt werden. Es besteht die Möglichkeit, zusätzliche Schalen zur Aufnahme weiterer Spezifikationen zu definieren.

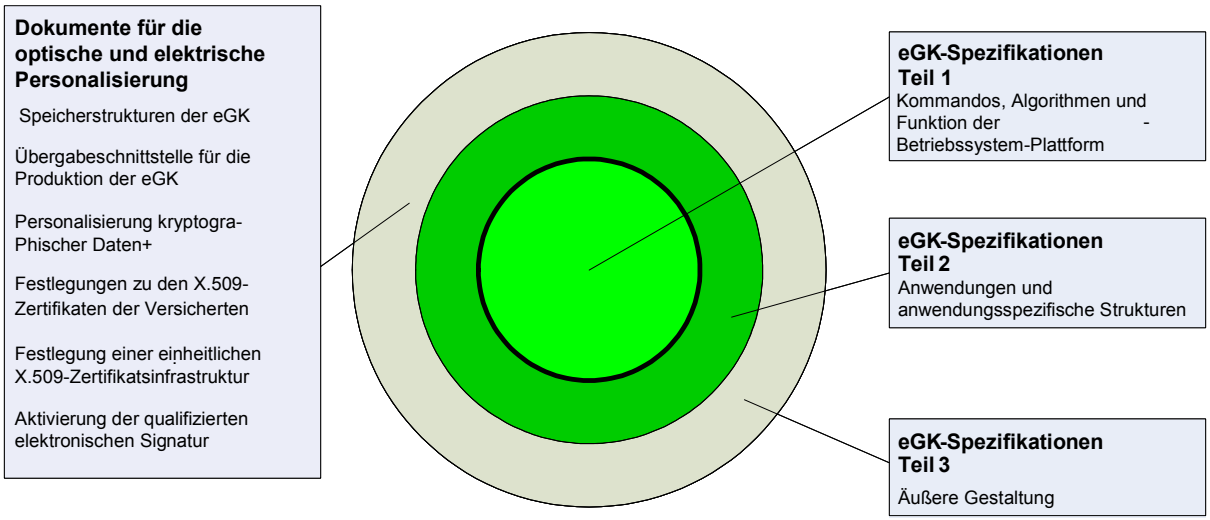

Abbildung 1 - Dokumentenstruktur

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Diese Spezifikation definiert die Anwendungen sowie die anwendungsspezifischen Strukturen und Funktionen der elektronischen Gesundheitskarte (eGK) unter folgenden Gesichtspunkten:

- technische Eigenschaften
- Vereinbarungen hinsichtlich der Datenübertragung
- Dateien und Datenstrukturen
- Sicherheitsmechanismen
- Nachlademechanismen
- Kommandos für die verschiedenen Dienste und Funktionen.

In diesem Dokument wird mit dem Wort "muss" eine unbedingt erforderliche Eigenschaft und mit dem Wort "sollte" eine empfohlene, aber nicht vorgeschriebene Eigenschaft bezeichnet. Das Wort "kann" bezeichnet dagegen eine Eigenschaft, deren Vorhandensein oder Fehlen keinen Einfluss auf die Konformität zu dieser Spezifikation hat.

2.2 Zielgruppe

Das Dokument richtet sich an Kartenhersteller.

2.3 Geltungsbereich

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

2.4 Arbeitsgrundlagen

Die Ausarbeitung steht in engem Zusammenhang mit der Spezifikation des Heilberufsausweises „German Health Professional Card and Security Module Card Specification Part 2“ [HPC].

2.5 Abgrenzung des Dokumentes

Vergleiche hierzu Kap. 1.3.

2.6 Notationen

Für Schlüssel und Zertifikate wird folgende Notation (vereinfachte Backus-Naur-Notation) verwendet:

<object descriptor> ::= <key descriptor> | <certificate descriptor>

<key descriptor>::= <key type>.<keyholder>.<usage> | <secure messaging key>

<key type>::= <private key> | <public key> | <secret key>

<private key>::= PrK (asym.)
<public key>::= PuK (asym.)
<secret key>::= SK (sym.)

<keyholder>::= <health professional> | <cardholder> | <certification authority> | <health professional card> | <electronic health card> | <security module card> | <card application management system> | <server> | <health insurance data service>

<health professional> ::= HP

<cardholder> ::= CH

<certification authority>::= CA | CA_eGK | CA_HBA | RCA | ZDA (CA_NN_XX denotes a specific CA for eGK or HBA)

<health professional card> ::= HPC (HBA)

<electronic health card> ::= eGK (elektronische Gesundheitskarte)

<security module card> ::= SMC

<card application management system> ::= CAMS

<server> ::= SVR

<health insurance data service>::= VSDD (Versichertenstammdatendienst)

<usage>::= <qualified electronic signature> | <encipherment> | <authentication> | <certsign>

<qualified electronic signature>::= QES

<encipherment>::= ENC
<authentication>::= AUT
<certsign>::= CS

<certificate descriptor>::=

<certificate>.<certificateholder>.<usage>

<certificate>::= <X.509v3 certificate> | <card verifiable certificate>

<X.509v3 certificate>::= C
<card verifiable certificate>:: CVC

<certificateholder>::=

<electronic health card> | <health professional card>|<security module card> |<certification authority>

<secure messaging key>::= <SMkey for encipherment> | <SMkey for MAC computation>
<SMkey for encipherment>::= SMK.ENC
<SMkey for MAC computation>::= SMK.MAC

Für die Darstellung von Datensequenzen wird folgende Notation verwendet:

|| = Konkatenation von Daten

Alle Kommandos werden ohne SM dargestellt, auch wenn sie im SM-Modus übertragen werden. Außerdem werden alle Kommandos zur Vereinfachung nur mit "short length" dargestellt.

Die Speicherung von Schlüsseln und Passwörtern ist COS-spezifisch. Zur besseren Lesbarkeit des Dokuments wird im Folgenden jeweils nur eine Datei pro Typ verwendet.

Die Root ist bei nativen Karten das MF, in „Global Platform-Karten“ die Default Selected Application. In diesem Dokument wird die Root als MF gekennzeichnet.

Angaben zu X.509-Zertifikaten beziehen sich immer auf die Version V3 dieser Zertifikate, siehe [X.509].

2.7 Answer-to-Reset und Historical Bytes

Für die technischen Eigenschaften und die Implementierung der Datenübertragung einer eGK muss [gemSpec_eGK_P1] beachtet werden. Die Kodierung des ATR und der Historical Bytes sind in Anhang A dargestellt.

3 Die elektronische Gesundheitskarte eGK

3.1 Allgemeiner Aufbau und Beschreibung der Kommandos

Die eGK enthält

- EFs auf Root-Ebene (MF-Level bei nativen Karten oder in einer Default Selected Application bei GP-Karten) für globale Datenobjekte und Schlüssel,
- die Gesundheitsanwendung (Health Care Application, HCA) für Daten auf der Basis des [GMG],
- die ESIGN-Anwendung gemäß [CWA14890-1] und [CWA14890-2] mit Unterstützung von X.509 PKI-Funktionen (Chiffrierung von Schlüsseln und Client/Server-Authentisierung),
- die kryptografische Informationsanwendung (CIA.ESIGN), die den Verweis auf das ESIGN-Anwendungsprofil enthält,
- die QES-Anwendung für qualifizierte elektronische Signaturen gemäß [DIN66291-4] mit nachladbaren Komponenten,

Abbildung 2: Allgemeine Dateistruktur einer eGK zeigt den allgemeinen Aufbau der Dateistruktur einer eGK.

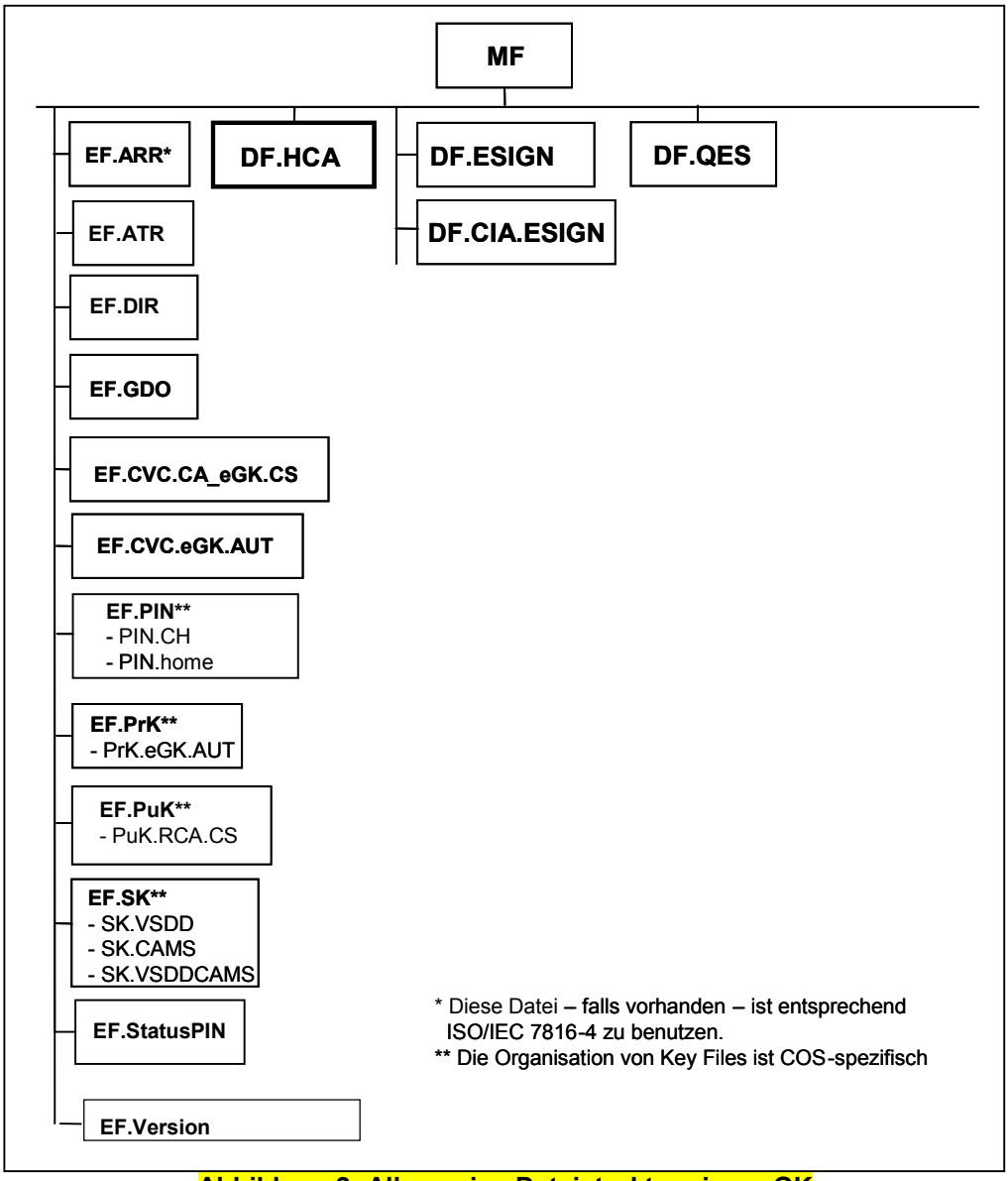

Abbildung 2: Allgemeine Dateistruktur einer eGK

3.2 Elementary Files auf MF-Ebene

3.2.1 EF.ARR

EF.ARR wird für die Speicherung von Zugriffsregeln auf MF-Ebene verwendet.

3.2.2 EF.ATR

Die transparente Datei EF.ATR enthält Datenobjekte zur Identifizierung der Karte, siehe **9.2**, und ein Datenobjekt zur Anzeige der Größe der Ein-/Ausgabe-Puffer, siehe Anhang C, Tabelle C.1.

3.2.3 EF.DIR

EF.DIR enthält die Anwendungs-Templates gemäß [ISO7816-4] für die in der eGK vorhandenen Anwendungen. Die Datei wird aktualisiert, wenn nach der Kartenausgabe weitere Anwendungen in die eGK nachgeladen werden. EF.DIR weist eine Record-Struktur auf, die in den Historical Bytes angezeigt werden muss. Der initiale Inhalt von EF.DIR ist in Tabelle C.2 dargestellt.

3.2.4 EF.GDO

In EF.GDO wird das DO ICCSN (Identifier (tag) '5A') gespeichert, das die Kennnummer der Karte enthält, siehe Abbildung 3. Die Kennnummer basiert auf dem Europäischen Beschluss 190 [Resolution190] und steht auch auf der Rückseite der eGK.

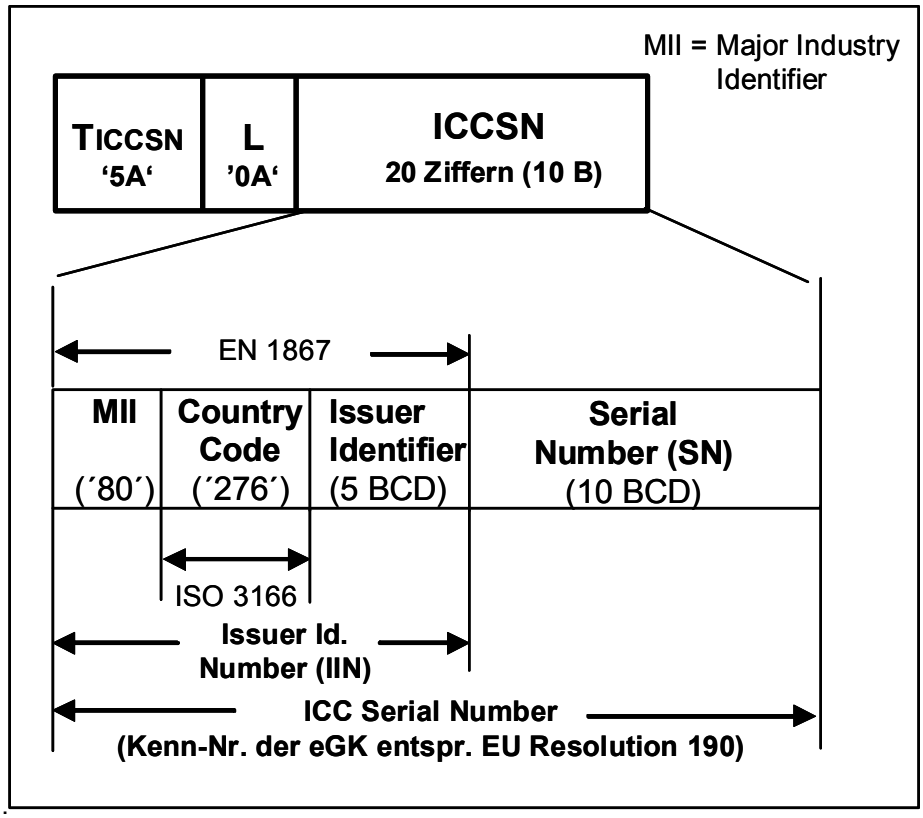

Abbildung 3 - ICCSN für Gesundheitskarten

Die Kenn-Nummer des Kartenherausgebers (issuer identification number, IIN), auch als „Kartenausgeberschlüssel" bezeichnet, ist eine weltweit eindeutige Kennung (siehe auch Anhang D).

3.2.5 EF.CVC.CA_eGK.CS

EF.CVC.CA_eGK.CS wird für die Aufnahme des CV-Zertifikats der CA, CVC.CA_eGK.CS, genutzt. Dieses Zertifikat wird von der Root–CA ausgestellt und enthält den öffentlichen Schlüssel einer CA. Struktur und Inhalt des Zertifikats sind in [gemSpec_eGK_P1] beschrieben.

3.2.6 EF.CVC.eGK.AUT

EF.CVC.eGK.AUT enthält das CV-Zertifikat der eGK, CVC.eGK.AUT. Dieses Zertifikat wird in Card-to-Card-Authentisierungsverfahren verwendet, d.h. eGK/HPC oder eGK/SMC. Struktur und Inhalt des Zertifikats sind in [gemSpec_eGK_P1] beschrieben. Die zu verwendende Certificate Holder Authorization CHA ist in Tabelle D. 2 dargestellt. Die Rollenkennung '00' in dem eGK-CV-Zertifikat bedeutet "kein Zugriffsrecht" auf Daten in anderen Karten.

3.2.7 EF.PIN

EF.PIN enthält

- die globale Persönliche Identifikations-Nummer PIN.CH (Patienten-PIN zur Nutzung gewisser Dienste innerhalb der Telematikinfrastruktur) und
- die globale Persönliche Identifikations-Nummer PIN.home (PIN zur Nutzung gewisser Dienste ausserhalb der Telematikinfrastruktur).

Welche PIN zur Freischaltung welcher Dienste notwendig ist, wird in Anhang B beschrieben.

Die PIN-Charakteristika sind in Tabelle 1 beschrieben. Das Format von PIN und Resetting Code und deren Verwendung ist in [gemSpec_eGK_P1] beschrieben.

Tabelle 1– PIN-Referenzen und Resetting Code

PIN Name	PIN Länge	PIN Referenz	Anfangswert des Retry Counters	Resetting Code	Nutzungsbegrenzung für Resetting Code
PIN.CH	6 - 8 Ziffern	'01'	3	8 Ziffern	10
PIN.home	6 - 8 Ziffern	'02'	3	8 Ziffern	10

Anmerkung: Nur die Mindestlänge wird von der eGK kontrolliert.

Wenn die eGK an den Karteninhaber ausgehändigt wird, kann z.B. ein Transport-PIN-Verfahren angewandt werden.

3.2.8 EF.StatusPIN

Die transparente Datei EF.StatusPIN ist stets vorhanden. Die Datei enthält die Information über das verwendete Verfahren zum Transportschutz von PIN.home und PIN.CH. Nach Aufheben des Transportschutzes MUSS der Inhalt von der Außenwelt angepasst werden. Der Inhalt der Datei wird in [gemeGK_Fach] spezifiziert. Die Zugriffsbedingungen sind in Anhang B dargestellt.

3.2.9 EF.Version

Das linear fixe EF.Version enthält die Versionsnummern der Spezifikation, die bei der Herstellung der Karte berücksichtigt wurden.

Der Inhalt der Datei wird in [gemeGK_Fach] spezifiziert. Die Zugriffsbedingungen sind in Anhang B dargestellt.

3.2.10 EF.PrK

Für C2C-Authentisierungsverfahren auf Basis von CV-Zertifikaten wird ein globaler privater Schlüssel PrK.eGK.AUT benötigt, der in einer Schlüssel-Datei unterhalb des MF abgelegt ist.

- PrK.eGK.AUT für die gegenseitige Authentisierung von eGK/HPC und eGK/SMC.

Für die C2C-Authentisierng bei lokalen Interaktionen zwischen eGK und HPC bzw. eGK und SMC wird ein Authentisierungsprotokoll ohne Vereinbarung von Sitzungsschlüsseln verwendet. Für die C2C-Authentisierung für remote Interaktionen zwischen eGK und SMC (nur die SMC hat die Fähigkeit, geschützte Kommandos zu produzieren und geschützte Antworten zu bearbeiten) ist ein Authentisierungsprotokoll mit Vereinbarung von Sitzungsschlüsseln zu unterstützen. Tabelle 2 zeigt die Schlüsselreferenzen und deren Verwendung in den beiden Security Environments.

Tabelle 2 – Schlüsselreferenzen von PrK.eGK.AUT und SE-Zuordnung

Name des Schlüssels	Key-ID	SE #
PrK.eGK.AUT (verwendet im Authentisierungsverfahren eGK – HPC/SMC mit und ohne Aufbau einesTC)	‘10’	‘01’ und ’02’

Der zugehörige PuK.eGK.AUT befindet sich im CVC.eGK.AUT, das im EF.CVC.eGK.AUT abgelegt ist.

Als Public-Key-Algorithmus wird RSA verwendet.

3.2.11 EF.PuK

Zur Prüfung der CV-Zertifikate von HPC muss der Public Key der gemeinsamen Root in der eGK verfügbar sein:

- PuK.RCA.CS (Public Key der Root-CA für Health Cards)

Die PuK-Referenz ist in EF.CVC.CA_eGK.CS enthalten (siehe [gemSpec_eGK_P1], Anhang B, Datenfeld CAR).

3.2.12 EF.SK

Für die gegenseitige Authentisierung mit TC Etablierung im Rahmen der Interaktion zwischen eGK und zugehörigem VSDD bzw. zwischen eGK und zugehörigem CAMS (z.B. für das Nachladen von Anwendungen) werden 3DES-Schlüssel-Paare bereitgestellt, siehe Tabelle 3. Jedes dieser Paare besteht aus je einem 3DES-Schlüssel für Verschlüsselung und MAC-Berechnung.

Tabelle 3 – Referenzen auf geheime Schlüssel

Name des Schlüssels	KeyRef
SK.VSDD.ENC / SK.VSDD.MAC	‘12’
SK.CAMS.ENC / SK.CAMS.MAC	‘13’
SK.VSDDCAMS.ENC / SK.VSDDCAMS.MAC	‘14’

3.2.13 Eröffnung der eGK

Nach dem Reset und Answer-to-Reset können EFs auf MF-Ebene gelesen werden.

3.2.14 Lesen von EF.ATR, EF.DIR und EF.GDO

Zum Lesen von EF.ATR und EF.GDO wird das ISO/IEC 7816-4 Kommando READ BINARY mit Short File Identifier SFID verwendet.

Tabelle 4 - READ BINARY Kommando mit SFID

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'B0' = READ BINARY
P1	'xx' = b8-b6: 100, b5-b1: 11101 SFID von EF.ATR: 29 b5-b1: 00010 SFID von EF.GDO: 2
P2	'00' = Offset
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'00' = Lesen bis zum Dateiende

Tabelle 5 - READ BINARY Antwort

Datenfeld	Data
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Zum Lesen von EF.DIR wird das ISO/IEC 7816-4 Kommando READ RECORD mit SFID verwendet.

Tabelle 6 - READ RECORD Kommando zum Lesen eines Records

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'B2' = READ RECORD
P1	'xx' = Record-Nummer
P2	'F4' = b8-b4: 11110 SFID of EF.DIR: 30, b3-b1: 100 (in P1 bezeichneten Record lesen)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'00' = Gesamten Record lesen

Anmerkung: In direkt nachfolgenden READ RECORD Kommandos auf EF.DIR kann der Short File Identifier (SFID) in P2 auf Null gesetzt sein.

Tabelle 7 – READ RECORD Antwort

Datenfeld	Record-Daten
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.2.15 Lesen der CV-Zertifikate

Zum Lesen der CV-Zertifikate aus der eGK wird das READ BINARY Kommando mit SFID verwendet.

Tabelle 8 – READ BINARY Kommando zum Lesen eines CV-Zertifikats

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'B0' = READ BINARY
P1	'83' = b8-b6: 100 b5-b1: 00011 SFID von EF.CVC.eGK.AUT: 3 '84' = b8-b6: 100 b5-b1: 00100 SFID von EF.CVC.CA_eGK.CS: 4
P2	'00' = Offset
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'00' = Lesen bis zum Dateiende

Tabelle 9 – READ BINARY Antwort

Datenfeld	CV certificate
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.2.16 SE-Selektion

Auf MF-Ebene werden SE # 1 und SE # 2 benutzt.

3.3 PIN-Management

3.3.1 PIN-Prüfung

Für die PIN-Verifikation wird das ISO/IEC 7816-4 Kommando VERIFY verwendet. Ob eine PIN-Verifikation erfolgen muss oder nicht, hängt von den Zugriffsregeln der jeweils referenzierten Dateien und Schlüssel ab.

Tabelle 10 – VERIFY Kommando für die Authentisierung des Karteninhabers

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'20' = VERIFY
P1	'00'

P2	‘01’ = PIN.CH-Referenz oder ‘02’ = PIN.home-Referenz
Lc	‘08’ = Länge des nachfolgenden Datenfeldes
Datenfeld	PIN, Format: siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 11 – VERIFY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.3.2 PIN-Änderung

Zur PIN-Änderung kann der Karteninhaber das ISO/IEC 7816-4 Kommando CHANGE RD ohne weitere Vorbedingungen verwenden.

Tabelle 12 – CHANGE RD Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘24’ = CHANGE REFERENCE DATA
P1	‘00’ = Referenzdaten ersetzen
P2	‘01’ = PIN.CH-Referenz oder ‘02’ = PIN.home-Referenz
Lc	‘10’ = Länge des nachfolgenden Datenfeldes
Datenfeld	PIN_alt || PIN_neu, Format: siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 13 – CHANGE RD Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.3.3 Rücksetzen des Retry Counters und Setzen einer neuen PIN

Zum Rücksetzen des Retry Counters (er entspricht funktionell einem Fehlbedienungszähler, wird jedoch dekrementiert statt inkrementiert) auf seinen Anfangswert und – falls entsprechende Option

verwendet – zum Setzen einer neuen PIN, wird das Kommando RESET RETRY COUNTER, wie in [ISO7816-4] spezifiziert, verwendet.

Tabelle 14 – RESET RC Kommando zum Rücksetzen des Retry Counters und ggf. Setzen einer neuen PIN

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2C' = RESET RETRY COUNTER
P1	'00' oder '01'
P2	'01' = PIN.CH-Referenz oder '02' = PIN.home-Referenz
Lc	'10' oder '08' = Länge des nachfolgenden Datenfeldes
Datenfeld	- Wenn P1 = '00': Resetting Code (8 B) || neue PIN (8 B) - Wenn P1 = '01': Resetting Code (8 B); Format: siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 15 – RESET RC Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.3.4 PIN-Sicherheitsstatus

Die erfolgreiche Präsentation von PIN.CH führt zum Setzen eines entsprechenden Sicherheitsstatus in der eGK. In einer Arztpraxis sind nach zusätzlicher erfolgreicher C2C-Authentisierung aus Sicht der eGK dann Lese- und Schreiboperationen auf Dateien der freiwilligen Anwendungen möglich.

Die Wahrnehmung der Patientenrechte

- zur Aktivierung/Deaktivierung freiwilliger Anwendungen,
- zum Verbergen, Sichtbarmachen und ggf. Löschen von Einträgen und
- zum Lesen der Logging-Daten

bleibt unter Kontrolle des Karteninhabers. Passive Patientenrechte (Lesen der geschützten Versichertendaten, der Logging-Daten, der eRezepte und der Notfalldaten) können nach erfolgreicher Präsentation von PIN.home an einem PC wahrgenommen werden.

Aktive Patientenrechte, die Schreiboperationen in der eGK erfordern (z.B. Verbergen eines Eintrags) können an einem eKiosk ausgeführt werden.

3.4 Card-2-Card-Authentisierung mit CVC-Verfahren

3.4.1 Verwendung

Für Interaktionen zwischen eGK und

- einem Heilberufsausweis HPC oder
- einer Sicherheitsmodulkarte SMC

sind zwei Maßnahmen erforderlich:

1. die eGK muss ihre Echtheit nachweisen
2. die eGK muss die zugreifende Instanz (z.B. einen Heilberufler) authentisieren, d.h. die zugreifende Instanz muss nachweisen, dass die präsentierte Certificate Holder Authorization (CHA) authentisch ist und zur entsprechenden Instanz gehört.

Die CHA wird in Sicherheitsbedingungen der EFs verwendet. Z.B. wird ein lesender Zugriff auf geschützte Versichertendaten nur dann gewährt, wenn die entsprechende CHA mit ihrer Profilkennung erfolgreich präsentiert wurde.

Wenn die Zugriffsberechtigung eines Heilberuflers gegenüber einer eGK nachzuweisen ist, muss ein auf CV-Zertifikate basierendes Authentisierungsverfahren durchgeführt werden, so dass in der eGK der zugehörige Sicherheitsstatus gesetzt werden kann, d.h. "CHA y (siehe Anhang D) wurde erfolgreich präsentiert".

Während des Authentisierungsverfahrens zwischen eGK und HPC werden keine SM-Schlüssel gebildet, weil in der anschließenden Kommunikation mit der eGK (Lesen/Schreiben von Daten) die HPC nicht einbezogen ist. Dies gilt auch für die lokale Interaktion zwischen eGK und SMC. Bei einer Remote-Nutzung der eGK wird ein C2C-Authentisierungsverfahren mit TC-Etablierung verwendet.

Vor der Durchführung des Authentisierungsverfahrens muss der eGK das Zertifikat CVC.HPC.AUT bzw. CVC.SMC.AUT präsentiert werden. Damit dieses prüfbar ist, muss zuvor über ein Root-Zertifikat der Public Key der CA-Instanz der betreffenden HPC importiert werden.

3.4.2 CV-Zertifikatsprüfung

Zur CVC-Prüfung sind die entsprechenden Schlüsselreferenzen der Public Keys zu setzen, siehe Abbildung 4.

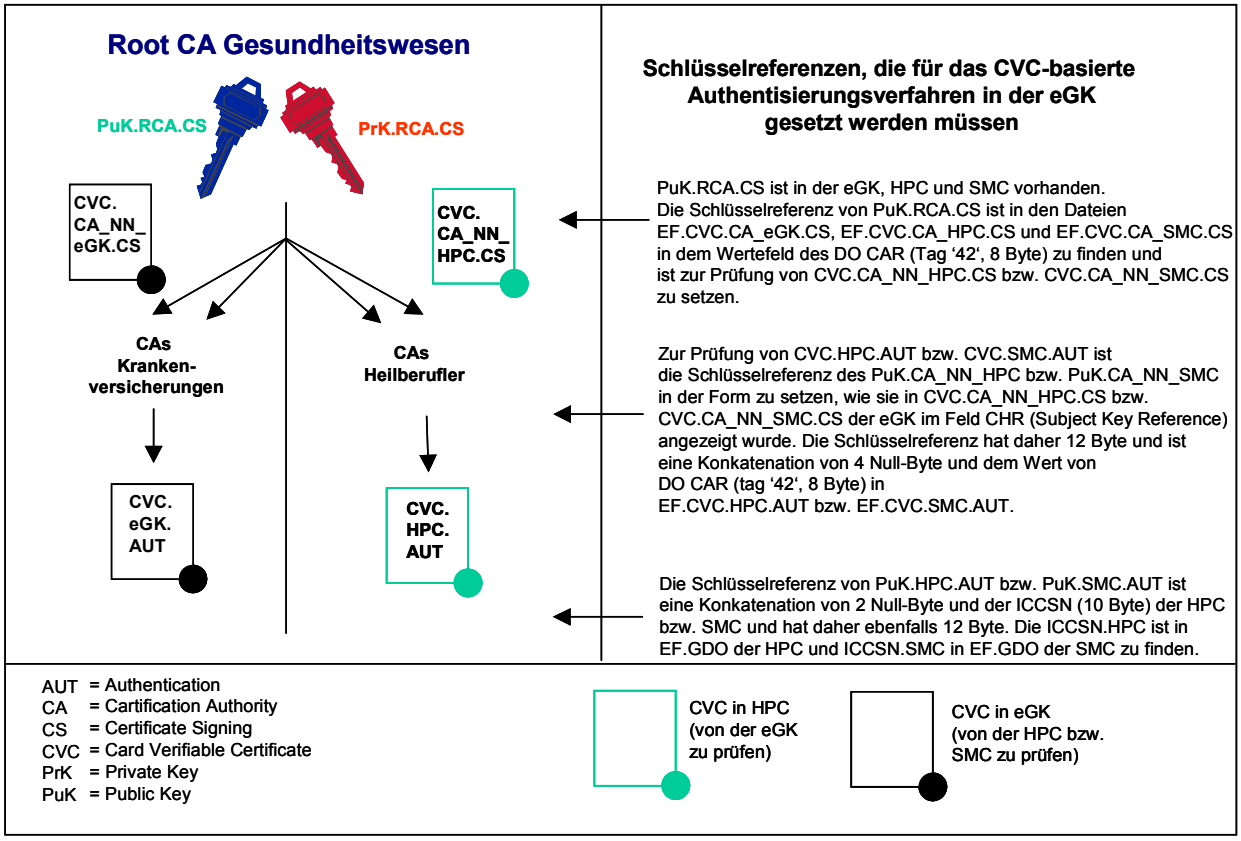

Abbildung 4 – Prüfung von CV-Zertifikaten

Für den Fall eines Root-Schlüssel-Wechsels oder zum Import des Public Keys einer parallelen RCA ist die Prüfung eines Cross-Zertifikats nötig (ein Cross-Zertifikat dient dem Import eines weiteren nicht persistent zu speichernden Root-Schlüssels). Da ein Cross-Zertifikat von der für das deutsche Gesundheitswesen zuständigen RCA signiert ist, ist der Einstieg in die Prüfung der Zertifikatskette gleich.

3.5 C2C-Authentisierung ohne Trusted Channel-Etablierung

3.5.1 SE- und Anwendungsselektion

Für das C2C-Authentisierungsverfahren ohne TC-Etablierung wird auf MF- und DF-Ebene SE # ' 01' (Default SE) benutzt. Es kann vor oder nach der Anwendungsselektion ausgeführt werden, da nach erfolgreicher Authentisierung ein globaler Sicherheitsstatus gesetzt wird, der auch nach Anwendungsselektion noch Geltung hat.

3.5.2 Prüfung von CVC.CA_NN_HPC.CS bzw. CVC.CA_NN_SMC.CS

Für die CV-Zertifikatsprüfung müssen die folgenden Befehle ausgeführt werden:

- MANAGE SECURITY ENVIRONMENT zum Setzen des öffentlichen Schlüssels der Root-CA (PuK.RCA.CS)
- VERIFY CERTIFICATE zum Prüfen des Zertifikats, das die Root-CA für die jeweilige CA_NN_HPC bzw. CA_NN_SMC ausgestellt hat.

Tabelle 16 - MSE Kommando zur Selektion des Root-CA Public Keys

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET für Verifikation
P2	'B6' = DST
Lc	'0A' = Länge des nachfolgenden Datenfeldes
Datenfeld	'83 08 ...' = DO für KeyRef von PuK.RCA.CS (Retrieval der Schlüsselreferenz: siehe Abbildung 4)
Le	Nicht vorhanden

Anmerkung: Der PuK der Root wird mit CAR referenziert (8 byte).

Tabelle 17 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nachdem der PuK.RCA.CS gesetzt wurde, wird das PSO: VERIFY CERTIFICATE Kommando zur eGK gesendet. Das Datenfeld enthält die Signatur (den ersten Teil des Root-Zertifikats abdeckend, welcher nach der Verarbeitung der Signatur anfällt) und den PK-Remainder (der restliche Teil des CV-Zertifikats, siehe [gemSpec_eGK_P1], Tabelle B.10.).

Tabelle 18 - PSO: VERIFY CERTIFICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2A' = PERFORM SECURITY OPERATION: VERIFY CERTIFICATE
P1	'00'
P2	'AE' = Zertifikat im Datenfeld, signierter Signatur-Input besteht aus Nicht-BER-TLV-kodierten Daten, d.h. der Zertifikatsinhalt ist eine Konkatenation von DEs
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	'5F37' || Länge (SIG.RCA) || SIG.RCA || '5F38' || Länge (PK-Remainder) || PK-Remainder (DOs aus EF.CVC.CA_HPC.CS bzw. EF.CVC.CA_SMC.CS aus HPC bzw. SMC)
Le	Nicht vorhanden

Tabelle 19 - PSO: VERIFY CERTIFICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.5.3 Prüfung von CVC.HPC.AUT bzw. CVC.SMC.AUT

Im ersten Schritt muss der öffentliche Schlüssel für die CV-Zertifikatsprüfung gesetzt werden.

Tabelle 20 - MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET für Verifikation
P2	'B6' = DST
Lc	'0E' = Länge des nachfolgenden Datenfeldes
Datenfeld	'83 0C ...' = DO für KeyRef von PuK.CA_NN_HPC.CS bzw. PuK.CA_NN_SMC.CS (Retrieval der Schlüsselreferenz: siehe Abbildung 4)
Le	Nicht vorhanden

Tabelle 21 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Der nächste Schritt ist die Prüfung des CV-Zertifikats der HPC bzw. der SMC.

Tabelle 22 - PSO: VERIFY CERTIFICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2A' = PERFORM SECURITY OPERATION: VERIFY CERTIFICATE
P1	'00'
P2	'AE' = Zertifikat im Datenfeld, signierter Signatur-Input besteht aus Nicht-BER-TLV-kodierten Daten, d.h. der Zertifikatsinhalt ist eine Konkatenation von DEs
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	'5F37'-L-SIG.CA_NN_HPC || '5F38'-L-PK-Remainder bzw. '5F37'-L-SIG.CA_NN_SMC || '5F38'-L-PK-Remainder (DOs aus EF.CVC.HPC.AUT bzw. EF.CVC.SMC.AUT)
Le	Nicht vorhanden

Tabelle 23 - PSO: VERIFY CERTIFICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

3.5.4 Abwicklung des Authentisierungsverfahrens

Vor Abwicklung des eigentlichen Authentisierungsverfahrens müssen jetzt zunächst mit dem MSE-Kommando die Schlüssel gesetzt werden.

Tabelle 24 - MSE Kommando zur Selektion des privaten Schlüssels

CLA	Wie in ISO/IEC 7816-4 definiert
INS	’22’ = MANAGE SECURITY ENVIRONMENT
P1	'C1'
P2	’A4’ = Authentisierung
Lc	'14' Länge des nachfolgenden Datenfeldes
Datenfeld	'84 01 10' || '83 0C XX...XX' || '80 01 1E' = DO für KeyRef von PrK.eGK.AUT || DO für KeyRef von PuK.HPC.AUT oder PuK.SMC.AUT || DO mit Algorithmus Identifier gemäß [gemSpec_eGK_P1] Anhang E.2 (Retrieval der PuK-Schlüsselreferenz siehe Abbildung 4)
Le	Nicht vorhanden

Tabelle 25 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anschließend wird die Echtheit der eGK nachgewiesen, indem das Verfahren der internen Authentisierung ausgeführt wird.

Tabelle 26 - INT. AUTHENTICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘88’ = INTERNAL AUTHENTICATE
P1	‘00’
P2	‘00’
Lc	‘10’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.2
Le	‘00’ oder ‘80’ = Länge der erwarteten Signatur

Tabelle 27 - INT. AUTHENTICATE Antwort

Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.2

SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nach der Authentisierung der eGK durch eine HPC bzw. SMC prüft die eGK die zugreifende Instanz.

Tabelle 28 - GET CHALLENGE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘84’ = GET CHALLENGE
P1, P2	‘0000’
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	‘08’

Tabelle 29 - GET CHALLENGE Antwort

Datenfeld	RND.eHC (8 Bytes)
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Unmittelbar nach dem GET CHALLENGE Kommando muss mit dem Kommando EXTERNAL AUTHENTICATE die digitale Signatur der HPC bzw. SMC an die eGK übergeben werden.

Tabelle 30 - EXT. AUTHENTICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘82’ = EXTERNAL AUTHENTICATE
P1	‘00’
P2	‘00’
Lc	‘xx’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.2
Le	Nicht vorhanden

Tabelle 31 - EXT. AUTHENTICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nach erfolgreicher Ausführung des Authentisierungsverfahrens setzt die eGK einen internen Sicherheitsstatus “Authentisierung mit Rollenkennung CHA.i erfolgreich ausgeführt” und erlaubt den Zugriff auf Objekte gemäß den in Anhang B definierten Zugriffsregeln.

3.6 C2C-Authentisierung mit Trusted Channel-Etablierung

3.6.1 SE- und Anwendungs-Selektion

Vor Benutzung der C2C-Authentisierung mit Trusted Channel-Etablierung ist auf MF-Ebene das SE # '02' mit dem MSE-Kommando zu selektieren.

Tabelle 32 - MSE Kommando zum Setzen des SEs

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘F3’ = RESTORE
P2	‘02’ = SE #
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	Nicht vorhanden

Tabelle 33 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anschließend erfolgt die Selektion der Anwendung, in dem der TC benötigt wird, siehe z.B. Kapitel 4.2

Nach Anwendungsselektion ist SE # '02' auf DF-Ebene mit demselben MSE-Kommando wie oben zu setzen. Dann folgt die Prüfung der CV-Zertifikate und das C2C-Authentisierung mit Trusted Channel-Etablierung.

3.6.2 Prüfung der CV-Zertifikate

Es ist dieselbe Kommandosequenz wie bei dem C2C-Authentisierungsverfahren ohne TC-Etablierung zu senden, siehe 3.5.2 und 3.5.4.

3.6.3 Abwicklung des Authentisierungsverfahrens

Vor Abwicklung des Authentisierungsverfahrens sind die Schlüsselreferenzen zu setzen.

Tabelle 34 - MSE Kommando zur Selektion des privaten Schlüssels

CLA	Wie in ISO/IEC 7816-4 definiert
INS	’22’ = MANAGE SECURITY ENVIRONMENT
P1	’C1’

P2	’A4’ = Authentisierung
Lc	’14’ Länge des nachfolgenden Datenfeldes
Datenfeld	'84 01 10' || '83 0C XX...XX' || '80 01 1F' = DO für KeyRef von PrK.eGK.AUT || DO für KeyRef von PuK.HPC.AUT oder PuK.SMC.AUT || DO mit Algorithmus Identifier gemäß [gemSpec_eGK_P1] Anhang E.3 (Retrieval der PuK-Schlüsselreferenz siehe Abbildung 4)
Le	Nicht vorhanden

Tabelle 35 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anschließend wird die Echtheit der eGK nachgewiesen, indem das Verfahren der internen Authentisierung ausgeführt wird.

Tabelle 36 - INT. AUTHENTICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘88’ = INTERNAL AUTHENTICATE
P1	‘00’
P2	‘00’
Lc	‘10’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.3
Le	‘00’ oder ‘xx’ = Länge der erwarteten Signatur

Tabelle 37 - INT. AUTHENTICATE Antwort

Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.3
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nach der Authentisierung der eGK durch eine SMC prüft die eGK die zugreifende Instanz.

Tabelle 38 - GET CHALLENGE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'08'

Tabelle 39 - GET CHALLENGE Antwort

Datenfeld	RND.eGK (8 Bytes)
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Unmittelbar nach dem GET CHALLENGE Kommando muss mit dem Kommando EXTERNAL AUTHENTICATE die mit dem PuK.eGK.AUT verschlüsselte digitale Signatur der SMC an die eGK übergeben werden.

Tabelle 40 - EXT. AUTHENTICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.3
Le	Nicht vorhanden

Tabelle 41 - EXT. AUTHENTICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nach erfolgreicher Beendigung des Kommandos stehen die SM-Schlüssel (ENC- und MAC-Schlüssel) zur Verfügung, die implizit selektiert sind.

Außerdem setzt die eGK einen internen Sicherheitsstatus "Authentisierung mit Profilkennung CHA.i erfolgreich ausgeführt".

3.7 C2S-Authentisierung mit symmetrischen Authentisierungsverfahren

3.7.1 SE-Selektion

Für das symmetrische C2C-Authentisierungsverfahren wird das SE # ' 01' (Default SE) benutzt.

3.7.2 Abwicklung des Authentisierungsverfahrens

Bei der Card-to-Server-Authentisierung (eGK mit VSDD bzw. eGK und CAMS) wird das in [gemSpec_eGK_P1] Anhang E.4 spezifizierte symmetrische Authentisierungsverfahren mit SM-Key-Vereinbarung verwendet.

- **Schritt 1: Der individuelle Schlüssel der eGK muss gesetzt werden.**

Tabelle 42 - MSE Kommando zur Selektion des symmetrischen Schlüssels

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘C1’ = SET für int./ext. Authentisierung
P2	‘A4’ = AT
Lc	‘03’ = Länge des nachfolgenden Datenfeldes
Datenfeld	- ‘83 0112’ = DO KeyRef für SK.VSDD oder - ‘83 0113’ = DO KeyRef für SK.CAMS oder - ‘83 0114’ = DO KeyRef für SK.VSDDCAMS siehe Tabelle 3
Le	Nicht vorhanden

Tabelle 43 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

- **Schritt 2: Von der eGK wird eine Zufallszahl angefordert.**

Tabelle 44 - GET CHALLENGE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘84’ = GET CHALLENGE
P1, P2	‘0000’
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	‘08’

Tabelle 45 - GET CHALLENGE Antwort

Datenfeld	RND.eGK (8 B)
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

- **Schritt 3: Ausführung des Kommandos MUTUAL AUTHENTICATE.**

Tabelle 46 - MUTUAL AUTHENTICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘82’ = MUTUAL AUTHENTICATE
P1	‘00’
P2	‘00’
Lc	‘xx’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.4
Le	‘00’

Tabelle 47 - MUTUAL AUTHENTICATE Antwort

Datenfeld	Authentisierungsdaten, siehe [gemSpec_eGK_P1], Anhang E.4
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Die Bildung der SM-Schlüssel und die Berechnung des Send Sequence Counter sind in [gemSpec_eGK_P1] beschrieben.

4 Gesundheitsanwendung HCA

4.1 Dateistruktur und Dateiverwendung

Die Dateien in einer eGK müssen gemäß [ISO7816-4] organisiert sein. Die folgende Abbildung zeigt die Dateistruktur von DF.HCA (Health Care Application).

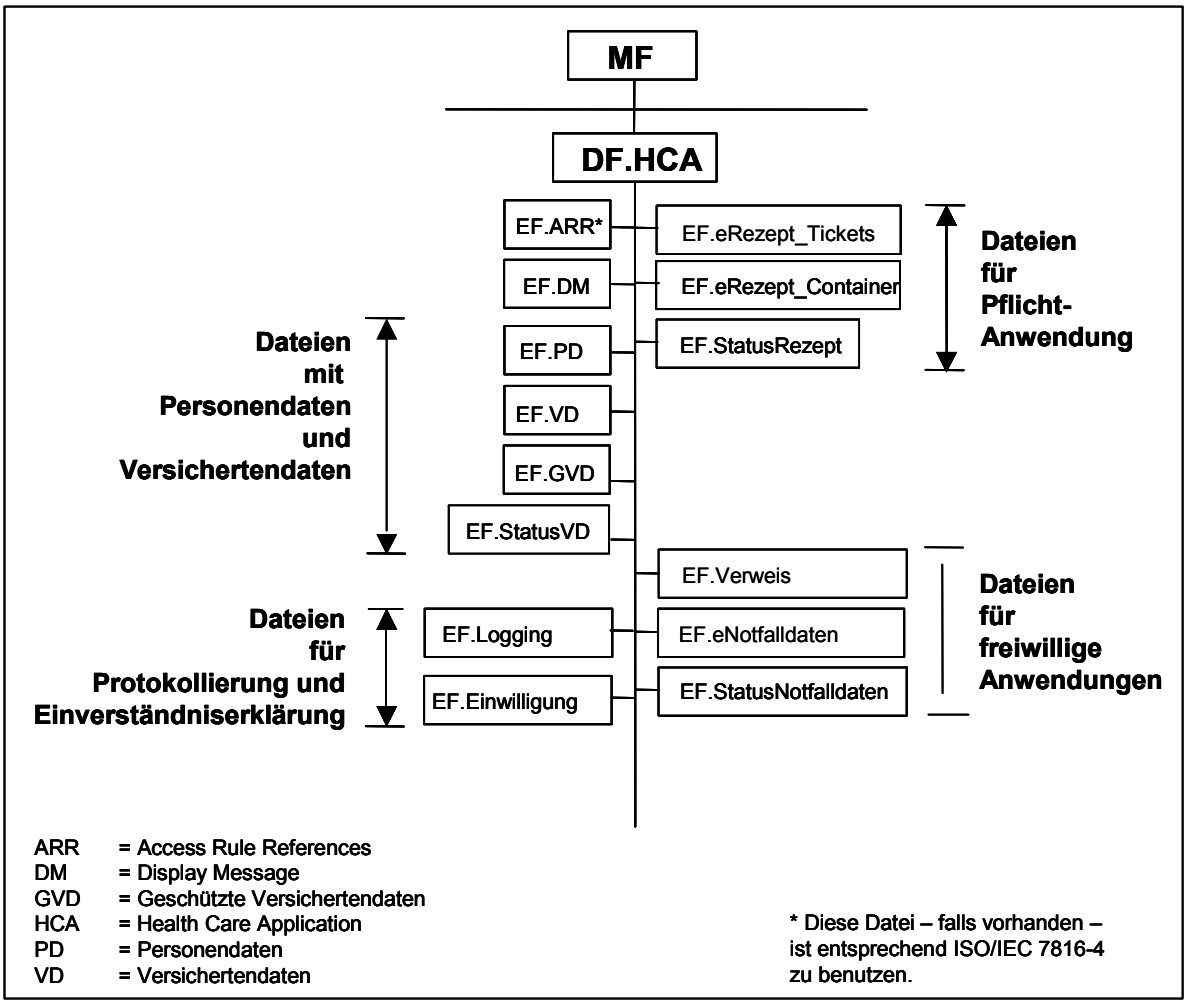

Abbildung 5 - Dateistruktur der Gesundheitsanwendung DF.HCA

Die Dateikenndaten und die Zugriffsregeln der EFs sind in Anhang B dargestellt.

4.1.1 EF.ARR

EF.ARR wird für die Speicherung von Zugriffsregeln in DF.HCA verwendet.

4.1.2 EF.DM

Die transparente Datei enthält eine Display Message (8 Byte, ASCII-Codierung). Die Daten können nur mit SM ausgelesen werden, d.h. die Anzeige gilt als Hinweis, dass auch tatsächlich ein Trusted Channel etabliert wurde. Eine Änderung der Display Message durch den Karteninhaber ist möglich. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.3 EF.PersonenDaten (EF.PD)

Die transparente Datei EF.PD enthält die Personenstammdaten. Der Inhalt der Datei wird in einem gesonderten Dokument [gemFA_VSDM] spezifiziert. Die Zugriffsbedingungen sind in Anhang B detailliert beschrieben

4.1.4 EF. VersichertenDaten (EF.VD)

Die transparente Datei EF.VD enthält Versichertendaten. Der Inhalt der Datei wird in einem gesonderten Dokument [gemFA_VSDM] spezifiziert. Die Zugriffsbedingungen sind in Anhang B detailliert beschrieben.

4.1.5 EF. Geschützte_ VersichertenDaten (EF.GVD)

Die transparente Datei EF.GVD wird zum Speichern schutzbedürftiger Versicherungsdaten verwendet. Der Inhalt der Datei wird in einem gesonderten Dokument [gemFA_VSDM] spezifiziert. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.6 EF.StatusVD

Die transparente Datei EF.StatusVD enthält Statusinformationen für EF.PD, EF.VD und EF.GVD. Der Inhalt der Datei wird in einem gesonderten Dokument [gemFA_VSDM] spezifiziert. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.7 EF.Logging

EF.Logging ist ein zyklisches EF mit fester Record-Länge und enthält Protokollierungsinformation über die letzten 50 Zugriffe auf die eGK durch Instanzen des Gesundheitswesens. Die Struktur eines Protokollierungs-Records wird in einem gesonderten Dokument spezifiziert [gemeGK_Fach]. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.8 EF.Einwilligung

In der transparenten Datei EF.Einwilligung werden Informationen zur Einverständniserklärung des Karteninhabers zur Nutzung der freiwilligen Anwendungen hinterlegt. Die genaue Datenstruktur wird in [gemeGK_Fach] spezifiziert. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.9 EF.eRezept_Tickets

EF.eRezept_Tickets enthält Records fester Länge für die Aufnahme von eRezept-Tickets, siehe Abb. G.1. Die Records haben einen Record Life Cycle Status. Die Zugriffsbedingungen sind in Anhang B dargestellt. Das eRezept-Ticket-Handling ist in Anhang G beschrieben.

4.1.10 EF.eRezept_Container

Die transparente Datei EF.eRezept_Container ist für die Aufnahme von eRezepten bestimmt. Die Datei muss Informationen enthalten, die die Zuordnung eines eTickets zu einem eRezept in dem EF.eRezept_Container ermöglichen. Die eRezepte werden komprimiert und anschließend mit einem Session Key verschlüsselt, so dass zum Löschen eines eRezepts nur das Löschen des zugehörigen eTickets notwendig ist.

Der Inhalt der Datei wird in einem gesonderten Dokument spezifiziert [gemFA_VODM]. Da die eRezepte chiffriert abgelegt werden, kann die Datei immer gelesen werden. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.11 EF.StatusRezept

Die transparente Datei EF.StatusRezept enthält Statusinformationen für EF.eRezept. Der Inhalt der Datei wird in einem gesonderten Dokument spezifiziert [gemFA_VODM]. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.12 EF.Verweis

Die Datei EF.Verweis enthält 10 Records fixer Länge für die Aufnahme von Dienst-IDs für den Zugriff auf freiwillige Anwendungen. Der Inhalt der Records wird in einem gesonderten Dokument spezifiziert [gemFA_VfA].Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.13 EF.eNotfalldaten

Die transparente Datei EF.eNotfalldaten ist für die Aufnahme bestimmter medizinischer Informationen vorgesehen. Der Inhalt der Datei wird in einem gesonderten Dokument spezifiziert [gemFA_NFDM]. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.1.14 EF.StatusNotfalldaten

Die transparente Datei EF.StatusNotfalldaten enthält Statusinformationen für EF.Notfalldaten. Der Inhalt der Datei wird in einem gesonderten Dokument [gemFA_NFDM] spezifiziert. Die Zugriffsbedingungen sind in Anhang B dargestellt.

4.2 HCA-Anwendungsselektion

Die folgenden zwei Tabellen zeigen das ISO/IEC 7816-4 Kommando für die ‘Direkte Anwendungsselektion’.

Tabelle 48 – SELECT Kommando für DF.HCA-Selektion mit AID

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘A4’ = SELECT
P1	‘04’ = DF-Selektion mit AID
P2	‘0C’ = keine FCI zurückgeben

Lc	‘06’ = Länge des nachfolgenden Datenfeldes
Datenfeld	‘D276 00000102’ = AID von DF.HCA
Le	Nicht vorhanden

Tabelle 49 – SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anmerkung: Falls die Anwendung deaktiviert ist, wird eine Warnung (Statusbytes ‘62 83’) zurückgegeben.

4.3 Lesen und Aktualisieren der Personen- und Versichertendaten

Zum Lesen von transparenten EFs, wird das Kommando READ BINARY mit Selektion des EF über die Short EFID verwendet.

Tabelle 50 – READ BINARY Kommando mit SFID

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘B0’ = READ BINARY
P1	‘81’ = b8-b6: 100, b5-b1: 00001 SFID von EF.PD: 1 ‘82’ = b8-b6: 100, b5-b1: 00010 SFID von EF.VD: 2 ‘83’ = b8-b6: 100, b5-b1: 00011 SFID von EF.GVD: 3
P2	‘00’ = Offset
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	- ‘xx’ = Länge der erwarteten Daten, siehe [gemSpec_eGK_P1]

Wenn der Offset größer als 255 ist, dann müssen weitere Daten (ohne Nutzung der SFID) mit fortgeschaltetem Offset in P1-P2 gelesen werden.

Tabelle 51 – READ BINARY Antwort

Datenfeld	Daten
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Zum Aktualisieren von transparenten EFs wird das Kommando UPDATE BINARY verwendet.

Tabelle 52 – UPDATE BINARY Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'D6' = UPDATE BINARY
P1	'81' = b8-b6: 100, b5-b1: 00001 SFID von EF.PD: 1 '82' = b8-b6: 100, b5-b1: 00010 SFID von EF.VD: 2 '83' = b8-b6: 100, b5-b1: 00011 SFID von EF.GVD: 3
P2	'00' = Offset
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	Daten
Le	Nicht vorhanden

Wenn der Offset größer als 255 ist, dann müssen P1-P2 für den Offset verwendet werden. Dies kann zuvor ein SELECT Kommando (siehe [gemSpec_eGK_P1]) erfordern, wenn die entsprechende Datei nicht das aktuelle EF ist.

Tabelle 53 – UPDATE BINARY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anmerkung: Die eGK kann ggf. auch Extended Length unterstützen (Anzeige im ATR, siehe Anhang A).

4.4 Prüfung der Echtheit einer eGK

Die Echtheit einer eGK wird bei jeder eGK/HPC- bzw. eGK/SMC-Interaktion im Rahmen des betreffenden C2C-Authentisierungsverfahrens verifiziert. Zeitpunkt und Häufigkeit der Prüfung der Aktualität der Daten in den Dateien EF.PD, EF.VD und EF.GVD ist nicht Gegenstand dieser Spezifikation.

4.5 eRezept-Handling

Das eRezept-Handling ist im Anhang G beschrieben. In diesem Kapitel werden im Wesentlichen nur die Kommandos an der eGK-Schnittstelle für das eRezept-Handling dargestellt.

4.5.1 eRezept-Transportverfahren nur über VODD

Bei diesem Verfahren ist die eGK bei der eigentlichen eRezept-Ausstellung nicht involviert. Beim Einlösen wird die eGK für die Dechiffrierung des Session Keys benötigt, mit dem das eRezept verschlüsselt wurde. Die betreffenden Kommandos sind in Kapitel 5.7 beschrieben.

4.5.2 eRezept-Transportverfahren nur über eGK

4.5.2.1 Setzen des Sicherheits-Status für Lese- und Schreiboperationen

Für das eRezept-Handling über die eGK ist eine C2C-Authentisierung erforderlich, wie in Kapitel 3.4 beschrieben. Welche Profile welche Berechtigung haben, ergibt sich aus den Zugriffsregeln in Anhang B. Die Zuordnung von Berufsgruppen zu Profilen ist nicht Gegenstand dieser Spezifikation.

4.5.2.2 Suchen eines freien Records zum Speichern eines eTickets

Für das Suchen eines freien Records zum Speichern eines eTickets werden die Records sequentiell mit dem READ RECORD-Kommando gelesen, bis der erste freie Record gefunden wird. Wie ein freier Rekord erkennbar ist, wird anhand der Definition eines eTickets in [gemeGK_Fach] deutlich.

Tabelle 54 - READ RECORD Kommando zum Lesen eines Records

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘B2’ = READ RECORD
P1	‘xx’ = Record-Nummer
P2	'3C' = b8-b4: 00111 SFID of EF.eRezept_Tickets: 7, b3-b1: 100 (in P1 bezeichneten Record lesen)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	‘XX’

Tabelle 55 – READ RECORD Antwort

Datenfeld	Record-Daten
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Zum Suchen kann auch das SEARCH RECORD-Kommando verwendet werden (gleiche Zugriffsregel wie READ RECORD).

4.5.2.3 Schreiben eines eRezept-Tickets

Zum Schreiben eines eRezept-Tickets wird das UPDATE RECORD-Kommando verwendet.

Tabelle 56 – UPDATE RECORD Kommando zum Eintragen eines eTickets

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'DC' = UPDATE RECORD
P1	'xx' = Record-Nummer
P2	'3C' = b8-b4: 00111 SFID of EF.eRezept_Tickets: 7, b3-b1: 100 (in P1 bezeichneten Record schreiben)
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	eRezept-Ticket
Le	Nicht vorhanden

Tabelle 57 – UPDATE RECORD Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anmerkung: Für die eGK ist nicht sichtbar, ob in einer Arzneimittelverordnung ein oder mehrere Medikamente verschrieben sind.

4.5.2.4 Schreiben eines eRezepts

Nach Ermittlung eines freien Bereichs in EF.eRezept_Container (siehe Anhang G) wird das komprimierte und verschlüsselte eRezept mit dem UPDATE BINARY-Kommando eingetragen. Dabei wird davon ausgegangen, dass das EF bereits durch die vorausgehende Suche selektiert ist. Aufgrund der großen Offsets ist eine implizite Selektion mittels SFID im Normalfall nicht möglich.

Tabelle 58 – UPDATE BINARY Kommando zum Eintragen eines eRezeptes

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'D6' = UPDATE BINARY
P1-P2	- P1:'88' = b8-b6: 100, b5-b1: 01000 SFID von EF.eRezept_Container: 8 - P2: 'xx' Offset oder - P1-P2: 'Offset' (bit b8 von P1 = 0)
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	eRezept-Daten
Le	Nicht vorhanden

Tabelle 59 – UPDATE BINARY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

4.5.2.5 Lesen eines eRezepts bei eRezept-Einlösung

Nach Selektion von DF.HCA im Präsenzprozess und gegenseitiger Authentisierung (eGK-HPC bzw. eGK-SMC) oder Selektion von DF.HCA mit anschließender gegenseitiger Authentisierung mit TC-Etablierung können eRezept-Tickets, die in Records mit Zustand "activated" abgelegt sind, gelesen werden. Das READ RECORD-Kommando zum Lesen ist in Kapitel 4.5.2.2 beschrieben.

Wurde ein eRezept-Ticket gefunden, dann kann das eRezept nun aus EF.eRezept_Container entsprechend den zu dem eTicket gehörenden Offset-Daten (Speicheradressen) gelesen werden. Das READ BINARY-Kommando muss mit fortgeschaltetem Offset in P1-P2 wiederholt werden, bis das eRezept komplett gelesen ist.

Tabelle 60 – READ BINARY Kommando mit SFID zum Lesen von eRezept-Daten

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘B0’ = READ BINARY
P1-P2	- P1 = ‘88’ = b8-b6: 100, b5-b1: 01000 SFID von EF.eRezept_Container: 8 - P2 = ‘00’ = Offset oder - P1-P2 = 'xxxx' Offset (bit b8 von P1 = 0)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'xx'

Tabelle 61 – READ BINARY Antwort

Datenfeld	Daten
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

4.5.2.6 Löschen eines eRezepts

Das Löschen eines eRezepts wird durch Überschreiben des Records mit einem mit ’73 00 ….. 00’ gefüllten Record erreicht. Hierfür wird das UPDATE RECORD-Kommando verwendet, siehe Kapitel 4.5.2.3.

Ist das eRezept nicht dispensierbar, wird das eRezept-Ticket so belassen, wie es vor dem Einlöse-Vorgang war.

4.5.2.7 Verbergen und Wiedersichtbarmachen von eRezepten

Der Karteninhaber hat die Möglichkeit, nach erfolgreicher PIN-Präsentation an einem eKiosk eRezepte zu verbergen und wieder sichtbar zu machen (Zugriffsregel siehe Anhang B). Nach dem Verbergen können die eRezepte nicht mehr gelesen werden. Zum Verbergen wird das DEACTIVATE RECORD-Kommando verwendet.

Tabelle 62 – DEACTIVATE RECORD Kommando zum Verbergen eines eRezept-Tickets

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘06’ = DEACTIVATE RECORD
P1	‘xx’ = Record Nummer des zu deaktivierenden Records
P2	'3C' = b8-b4: 00111 SFID von EF.eRezept_Tickets: 7 b3-b1= 100: deaktiviere Record P1
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	Nicht vorhanden

Tabelle 63 - DEACTIVATE RECORD Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Records mit verborgenen eRezept-Tickets können mit dem ACTIVATE FILE-Kommando wieder in den Zustand "activated" versetzt werden.

Tabelle 64 – ACTIVATE FILE Kommando zum Setzen aller Records von EF.eRezept_Ticket in den Zustand "Activated"

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘44’ = ACTIVATE FILE
P1	‘02’ = FID
P2	‘00’
Lc	‘02’ = Länge des nachfolgenden Datenfeldes
Datenfeld	'D007' = FID von EF.eRezept_Ticket
Le	Nicht vorhanden

Tabelle 65 - ACTIVATE FILE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

4.6 EF.Verweis

In EF.Verweis werden Records mit Service-IDs für den Zugriff auf freiwillige Anwendungen.gespeichert.

4.6.1 Verzeichniseintrag-Handling für Arzneimitteldokumentation

Die Anwendung "elektronische Arzneimittel-Dokumentation" gehört zu den freiwilligen Anwendungen. Für die Arzneimitteldokumentation ist auf der eGK die Speicherung einer Service-ID für das Finden des zugehörenden Dienstes vorgesehen. Der Inhalt der linearen Datei wird in einem gesonderten Dokument spezifiziert [gemFA_AMTS].

4.6.2 Verzeichniseintrag-Handling für elektronische Patienten-Akten

Die Anwendung "elektronische Patienten-Akte" gehört zu den freiwilligen Anwendungen. Für die elektronische Patienten-Akte ist auf der eGK die Speicherung einer Service-ID für das Finden des zugehörenden Dienstes vorgesehen. Der Inhalt der linearen Datei wird in einem gesonderten Dokument [gemFA_ePA] spezifiziert.

4.7 Lesen und Schreiben von eNotfalldaten

Die Nutzung von eNotfalldaten gehört zu den freiwilligen Anwendungen. Für die Lese- und Schreiboperationen sind die Kommandos READ BINARY und UPDATE BINARY zu verwenden.

4.8 Erstellen und Lesen von Protokollierungs-Records

Um einen Record hinzuzufügen, d.h. einen neuen Protokollierungseintrag zu schreiben, muss das ISO/IEC 7816-4 Kommando APPEND RECORD verwendet werden. Dieses Kommando, falls mit SFID verwendet, selektiert zudem EF.Logging. Der Inhalt der Records wird in einem gesonderten Dokument spezifiziert [gemeGK_Fach] beschrieben.

Tabelle 66: APPEND RECORD Kommando zum Hinzufügen eines Protokollierungs-Records

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘E2’ = APPEND RECORD
P1	‘00’ = Nicht verwendet
P2	‘30’ = b8-b4: 00110 SFID von EF.Logging: 6, b3-b1: 000
Lc	‘xx’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Protokollierungsdaten
Le	Nicht vorhanden

Tabelle 67 – APPEND RECORD Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Wird beim Hinzufügen von Protokollierungs-Records die Grenze von 50 Einträgen erreicht, wird der jeweils älteste Record überschrieben (first-in first-out).

Logging-Daten dienen der Information, welcher Leistungserbringer lesend und/oder schreibend auf medizinische Daten (z.B. Notfalldaten, Arzneimitteldokumentation, ...) zugegriffen hat.

Zum Lesen eines Protokollierungs-Records wird das Kommando READ RECORD verwendet. Die Recordnummer 1 bezeichnet dabei den zuletzt geschriebenen Record. Die Recordnummer i bezeichnet den Record, der unmittelbar vor Record (i–1) geschrieben wurde.

Tabelle 68 – READ RECORD Kommando zum Lesen eines Records

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘B2’ = READ RECORD
P1	‘xx’ = Recordnummer
P2	‘34’ = b8-b4: 00110 SFID von EF.Logging: 6 b3-b1: 100: in P1 bezeichneten Record lesen
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	‘00’ = gesamten Record lesen

Tabelle 69 – READ RECORD Antwort

Datenfeld	Record-Daten
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Soll gezielt nach bestimmten Records gesucht werden, ist das SEARCH RECORD Kommando zu verwenden.

Tabelle 70 – SEARCH RECORD Kommando zum Suchen eines Records

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘A2’ = SEARCH RECORD
P1	‘xx’ = Recordnummer
P2	‘34’ = b8-b4: 00110 SFID von EF.Logging: 6 b3-b1: 100: Suche vorwärts von dem in P1 bezeichneten Record
Lc	‘xx’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Suchstring
Le	'00'

Tabelle 71 – SEARCH RECORD Antwort

Datenfeld	- Recordnummern - Nicht vorhanden
SW1-SW2	- Falls Record gefunden: ‘9000’ - Falls keinen Record gefunden: ’6282’ - spezifische Statusbytes, siehe [gemSpec_eGK_P1]

5 ESIGN-Anwendung

5.1 Allgemeines Konzept

Die ESIGN-Anwendung (DF.ESIGN) ist in [CWA14890-1] und [CWA14890-2] spezifiziert und wird in der eGK genutzt für

- die Client/Server-Authentisierung (Verwendung z.B. zum Signieren von Challenges und Authentisierungstoken)
- die pseudonymisierte Client/Server-Authentisierung und Nachrichtensignatur (Verwendung z.B. zum Signieren von Challenges, Nachrichten und Authentisierungstoken)
- die Schlüssel-Chiffrierungsfunktion für die kryptografische Sicherung von Daten, die unter der Datenhoheit des Karteninhabers stehen
- die Schlüssel-Chiffrierungsfunktion im Kontext elektronischer Rezepte

An der Verschlüsselung eines Dokuments ist die eGK nicht direkt beteiligt: Die Software im PC des Dokumentsenders berechnet den Dokumenten-Chiffrierschlüssel, verschlüsselt damit das Dokument und verschlüsselt schließlich den Dokumenten-Chiffrierschlüssel, indem der öffentliche Schlüssel des Empfängers auf ihn angewendet wird. Dieser öffentliche Schlüssel stammt aus dem X.509 ENC-Zertifikat des Empfängers, das von der eGK bereitgestellt wird und auch von einem Online-Verzeichnisdienst abgerufen werden kann. Es wird ein zweites Schlüsselpaar zur Verschlüsselung von eRezepten verwendet: bei diesem erfordert die Nutzung des privaten Schlüssels keine PIN-Eingabe, d.h., zur Entschlüsselung genügt der Besitz der Karte.

Folgende SEs sind für die ESIGN-Anwendung relevant:

- SE # ’01’: (Default SE): Security Environment ohne TC
- SE # '02': Security Environment mit TC (z.B. für einen Online-Zugriff auf geschützte Bereiche der eGK).

5.2 Dateistruktur und Dateiverwendung

Abbildung 6 zeigt die allgemeine Dateistruktur von DF.ESIGN, wie sie in der eGK bei eGK-Ausgabe verwendet wird.

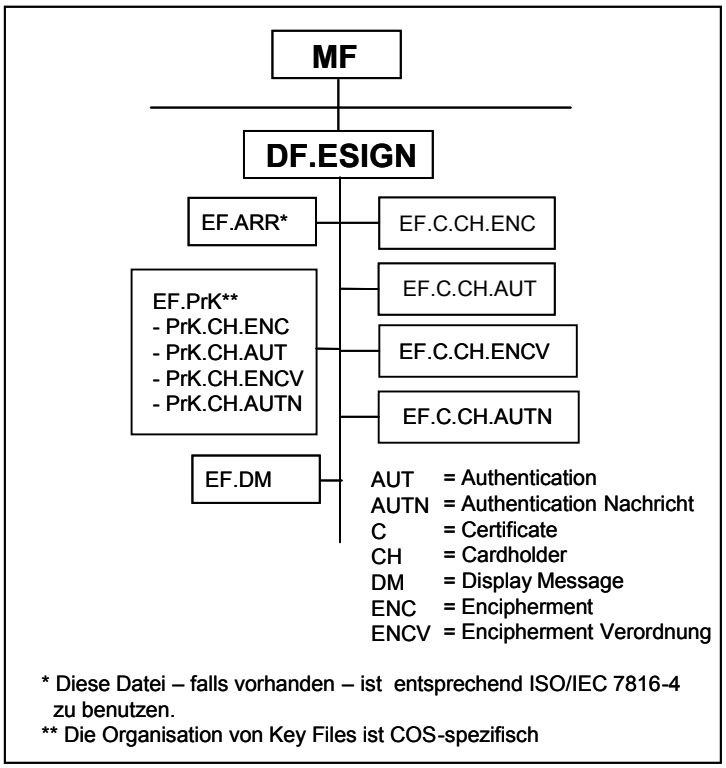

Abbildung 6 – Dateistruktur der Anwendung DF.ESIGN

5.2.1 EF.ARR

EF.ARR wird für die Speicherung von Zugriffsregeln in DF.ESIGN verwendet.

5.2.2 EF.PrK

EF.PrK enthält die privaten RSA-Schlüssel für die PKI-Funktionen. Die kryptografischen Parameter müssen dem Algorithmenkatalog für elektronische Signaturen genügen [ALGCAT]. Der Schutz der Schlüssel wird in Anhang B beschrieben.

Tabelle 72 – Schlüsselreferenzen

Name des Schlüssels	KeyRef	
PrK.CH.AUT	‘82’	
PrK.CH.ENC	‘83’	
PrK.CH.AUTN	‘86’	
PrK.CH.ENCV	‘87’	

5.2.3 EF.DM

Die transparente Datei enthält eine Display Message (8 Byte, ASCII-Codierung). Die Daten können nur mit SM ausgelesen werden, d.h. die Anzeige gilt als Hinweis, dass auch tatsächlich ein Trusted Channel etabliert wurde. Die Zugriffsbedingungen sind in Anhang B dargestellt.

5.2.4 EF.C.CH.ENC

EF.C.CH.ENC dient der Speicherung des X.509-ENC-Zertifikats des Karteninhabers.

Das Zertifikat ist bei Ausgabe der eGK vorhanden und kann mit entsprechender Berechtigung ersetzt werden. Die Zugriffsbedingungen sind in Anhang B dargestellt.

5.2.5 EF.C.CH.AUT

EF.C.CH.AUT dient der Speicherung des X.509-AUT-Zertifikats des Karteninhabers.

Das Zertifikat ist bei Ausgabe der eGK vorhanden und kann mit entsprechender Berechtigung ersetzt werden. Die Zugriffsbedingungen sind in Anhang B dargestellt.

5.2.6 EF.C.CH.ENCV

EF.C.CH.ENCV dient der Speicherung des pseudonymisierten X.509-ENCV-Zertifikats des Karteninhabers zur Verschlüsselung von eRezepten.

Das Zertifikat ist bei Ausgabe der eGK vorhanden und kann mit entsprechender Berechtigung ersetzt werden. Die Zugriffsbedingungen sind in Anhang B dargestellt.

5.2.7 EF.C.CH.AUTN

EF.C.CH.AUTN dient der Speicherung des pseudonymisierten X.509-AUTN-Zertifikats des Karteninhabers.

Das Zertifikat ist bei Ausgabe der eGK vorhanden und kann mit entsprechender Berechtigung ersetzt werden. Die Zugriffsbedingungen sind in Anhang B dargestellt.

5.3 ESIGN-Anwendungsselektion

Die folgenden zwei Tabellen zeigen das ISO/IEC 7816-4 Kommando für die ‘Direkte Anwendungsselektion’.

Tabelle 73 – SELECT Kommando für DF.ESIGN-Selektion mit AID.ESIGN

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘A4’ = SELECT
P1	‘04’ = DF-Selektion mit AID
P2	‘0C’ = Kein FCI zurückgeben
Lc	‘0A’ = Länge des nachfolgenden Datenfeldes
Datenfeld	‘A000000167 455349474E’ = AID von DF.ESIGN
Le	Nicht vorhanden

Tabelle 74 – SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

5.4 Lesen eines X.509-Zertifikats

Zum Lesen wird das ISO/IEC 7816-4 Kommando READ BINARY verwendet.

Tabelle 75 – READ BINARY Kommando zum Lesen eines X.509-Zertifikats

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'B0' = READ BINARY
P1-P2	-P1: '81' = b8-b6: 100, b5-b1: 00001 SFID von EF.C.CH.AUT '82' = b8-b6: 100, b5-b1: 00010 SFID von EF.C.CH.ENC '89' = b8-b6: 100, b5-b1: 00009 SFID von EF.C.CH.AUTN '8A' = b8-b6: 100, b5-b1: 0000A SFID von EF.C.CH.ENCV -P2: Offset oder -P1-P2: 'xxxx' = Offset (bit b8 = 0)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'xx' = Länge der erwarteten Daten

Weil X.509-Zertifikate mehr als 256 Byte haben, ist es normalerweise erforderlich, das Kommando mit fortgeschaltetem Offset zu wiederholen, falls die eGK nicht extended length unterstützt.

Tabelle 76 – READ BINARY Antwort

Datenfeld	Zertifikatsdaten
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

5.5 Client/Server-Authentisierung

5.5.1 Freischaltung der Authentisierungsschlüssel

Die Verwendung des privaten Schlüssels für “Client/Server-Authentisierung” erfordert bei PrK.CH.AUT die erfolgreiche Präsentation der PIN.home oder der PIN.CH zusammen mit einer C2C–Authentisierung. Die Verwendung des privaten Schlüssels PrK.CH.AUTN erfordert keine PIN-Eingabe, aber eine C2C-Authentisierung. Genaueres zu den Freischaltbedingungen findet sich in den Tabellen des Anhangs B.4.

5.5.2 Abwicklung der Authentisierung

Zur Überprüfung von Zugriffsrechten auf Komponenten, wie z.B. Server, oder zum Signieren eines Tokens im Rahmen einer Autorisierung muss ein PK-basiertes Authentisierungsverfahren durchgeführt werden.

Das verwendete Schlüsselpaar ist das des Karteninhabers (PrK.CH.AUT, PuK.CH.AUT bzw. PrK.CH.AUTN, PuK.CH.AUTN). Der öffentliche Schlüssel ist zusammen mit dem eindeutigen Namen des Karteninhabers/dem Pseudonym durch das X.509-Authentisierungs-Zertifikat nachweisbar beglaubigt. Welches Schlüsselpaar in einem bestimmten Kontext verwendet wird (AUT oder AUTN), entscheidet die Anwendung.

Relevante Authentisierungsprotokolle sind z.B.

- das PK-Kerberos-Protokoll (für Login-Authentisierung)
- das TLS-Protokoll (für Authentisierung auf Seiten des Clients; umfasst das SSL-Protokoll)
- das WTLS-Protokoll
- ....

Die privaten Schlüssel PrK.CH.AUT und PrK.CH.AUTN können zur Berechnung einer digitalen Signatur in einem Kommando INTERNAL AUTHENTICATE oder in einem Kommando PSO : Compute DS genutzt werden, siehe [gemSpec_eGK_P1].

Die übrigen Anteile des Verfahrens auf Seiten des Clients muss die Systemsoftware übernehmen.

Bevor das Kommando INTERNAL AUTHENTICATE bzw. das Kommando PSO : Compute DS ausgeführt werden kann, muss der zugehörige private Schlüssel (PrK.CH.AUT bzw. PrK.CH.AUTN) selektiert werden.

Tabelle 77 – MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET for internal authentication
P2	‘A4’ = AT
Lc	‘03’ = Länge des nachfolgenden Datenfeldes
Datenfeld	‘84 01 82’ = DO für KeyRef von PrK.CH.AUT

	'84 01 86' = DO für KeyRef von PrK.CH.AUTN
Le	Nicht vorhanden

Tabelle 78 – MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Tabelle 79 – INT. AUTHENTICATE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'88' = INTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	DigestInfo, verwendet für KERBEROS H_MD5 || H_SHA1, verwendet für SSL/TLS H_SHA1, verwendet für WTLS und NETSCAPE Formatierung des Digital Signature Inputs: siehe [gemSpec_eGK_P1], Anhang E.6
Le	'00' oder 'xx' = Länge der erwarteten Signatur

Tabelle 80 – INT. AUTHENTICATE Antwort

Datenfeld	Digitale Signatur
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

5.6 Entschlüsselung mit dem Dokumenten-Chiffrierungsschlüssel PrK.ENC

Die Benutzung von PrK.CH.ENC durch den Karteninhaber (z.B. für die Dechiffrierung eines Dokument-Chiffrierschlüssels) erfordert die vorherige Freischaltung von Prk.CH.ENC.

5.6.1 Freischaltung von PrK.CH.ENC mit PIN.home

Das VERIFY-Kommando ist in Kapitel 3.3 beschrieben. Die Kommando-Folge zur Dechiffrierung eines Dokument-Chiffrierungsschlüssels ist in Kapitel 5.6.2 beschrieben.

5.6.2 Schlüsselselektion und Dechiffrierung

Bevor die Schlüssel-Dechiffrierung (Entschlüsselung des Schlüssels, mit dem das Dokument verschlüsselt wurde) erfolgen kann, muss der private Schlüssel PrK.CH.ENC mittels ISO/IEC 7816-4 Kommando MSE selektiert werden.

Tabelle 81 – MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für Entschlüsselung
P2	'B8' = CT
Lc	'03' = Länge des nachfolgenden Datenfeldes
Datenfeld	'84 01 83' = DO für KeyRef von PrK.CH.ENC
Le	Nicht vorhanden

Tabelle 82 – MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nachdem der Schlüssel selektiert wurde, kann die Entschlüsselung mittels ISO/IEC 7816-8 Kommando PSO: DECIPHER ausgeführt werden.

Tabelle 83 – PSO: DECIPHER Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2A' = PERFORM SECURITY OPERATION: DECIPHER
P1	'80' = Klartext zurückgeben
P2	'86' = verschlüsselte Daten im Datenfeld
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	Padding Indicator Byte gefolgt von Kryptogramm, siehe [gemSpec_eGK_P1]
Le	'00' oder 'xx' = Länge des Dokumenten-Chiffrierschlüssels

Tabelle 84 – PSO: DECIPHER Antwort

Datenfeld	Dokumenten-Chiffrierschlüssel
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

5.7 Entschlüsselung mit dem Dokumenten-Chiffrierungsschlüssel PrK.ENCV

Die Benutzung von PrK.CH.ENCV durch den Karteninhaber (z.B. für die Dechiffrierung eines Dokument-Chiffrierschlüssels) erfordert die vorherige Freischaltung von Prk.CH.ENCV nach einem der zwei im Folgenden beschriebenen Verfahren.

5.7.1 Freischaltung von PrK.CH.ENCV durch C2C-Authentisierung ohne TC-Etablierung

Zur Einlösung von eRezepten mit rein Server-basierten eRezept-Transportverfahren wird der private Schlüssel PrK.CH.ENCV durch externe C2C-Authentisierung mit festgelegter Profilkennung (siehe Anhang B) freigeschaltet.

Nach erfolgreicher Authentisierung kann dann die Entschlüsselungs-Operation durchgeführt werden, siehe Kapitel 5.6.2.

5.7.2 Freischaltung von PrK.CH.ENCV durch C2C-Authentisierung mit TC-Etablierung

Soll der Schlüssel PrK.CH.ENCV z.B. zur Einlösung von eRezepten im Versandprozess genutzt werden, dann ist auf MF-Ebene und nach DF.ESIGN-Selektion SE # '02' mit dem MSE-Kommando zu setzen.

Tabelle 85 - MSE Kommando zum Setzen von SE # '02'

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘F3’ = RESTORE
P2	‘02’ = SE #
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	Nicht vorhanden

Tabelle 86 - MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Dann erfolgt die Abwicklung des Authentisierungsverfahrens mit TC-Etablierung, siehe Kapitel 3.4.

Im Anschluss daran soll zur Kontrolle der Etablierung des Trusted Channel durch den Karteninhaber die Display Message angezeigt werden, siehe Kapitel 5.7.4.

5.7.3 Schlüsselselektion und Dechiffrierung

Bevor die Schlüssel-Dechiffrierung (Entschlüsselung des Schlüssels, mit dem das Dokument verschlüsselt wurde) erfolgen kann, muss der private Schlüssel PrK.CH.ENCV mittels ISO/IEC 7816-4 Kommando MSE selektiert werden.

Tabelle 87 – MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET für Entschlüsselung
P2	‘B8’ = CT
Lc	‘03’ = Länge des nachfolgenden Datenfeldes
Datenfeld	’84 01 87’ = DO für KeyRef von PrK.CH.ENCV
Le	Nicht vorhanden

Tabelle 88 – MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nachdem der Schlüssel selektiert wurde, kann die Entschlüsselung mittels ISO/IEC 7816-8 Kommando PSO: DECIPHER ausgeführt werden.

Tabelle 89 – PSO: DECIPHER Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘2A’ = PERFORM SECURITY OPERATION: DECIPHER
P1	‘80’ = Klartext zurückgeben
P2	‘86’ = verschlüsselte Daten im Datenfeld
Lc	‘xx’ = Länge des nachfolgenden Datenfeldes
Datenfeld	Padding Indicator Byte gefolgt von Kryptogramm, siehe [gemSpec_eGK_P1]
Le	‘00’ oder ‘xx’ = Länge des Dokumenten-Chiffrierschlüssels

Tabelle 90 – PSO: DECIPHER Antwort

Datenfeld	Dokumenten-Chiffrierschlüssel
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

5.7.4 Lesen und Ändern der Display Message

Zum Lesen und Ändern der Display Message werden die Kommandos READ BINARY bzw. UPDATE BINARY verwendet.

6 Signaturanwendung für qualifizierte elektronische Signaturen (QES)

6.1 Allgemeines Konzept

Im Hinblick auf den Zustand der QES-Anwendung bei eGK-Ausgabe sind 5 Varianten zu unterscheiden:

1. Es gibt kein DF.QES. Damit ist das folgende Kapitel nicht relevant.
2. Die QES-Anwendung ist komplett angelegt und sofort nutzbar, d.h. QES-Schlüsselpaar und QES-Zertifikat sind vorhanden. Beschreibung im folgenden Kapitel.
3. Die QES-Anwendung ist mit ihrem DF und den benötigten Files inklusive der Zugriffsregeln angelegt. Das QES-Schlüsselpaar existiert noch nicht. Es ist ein CV-Zertifikat für die Aktivierung vorhanden. Beschreibung in Anhang E und F.
4. Die QES-Anwendung ist mit ihrem DF und den benötigten Files inklusive der Zugriffsregeln angelegt. Das QES-Schlüsselpaar existiert schon. Es ist ein CV-Zertifikat für die Aktivierung vorhanden. Beschreibung in Anhang F
5. Die QES-Anwendung ist mit ihrem DF und den benötigten Files inklusive der Zugriffsregeln angelegt. Das QES-Schlüsselpaar existiert schon. Es ist ein Gütesiegel-Zertifikat für die Aktivierung vorhanden. Beschreibung in Anhang F

6.2 Die QES-Anwendung ist komplett angelegt und sofort nutzbar

6.2.1 File-Struktur und File-Inhalt

Abbildung 7 zeigt die allgemeine Dateistruktur von DF.QES, wie sie in der eGK bei der Ausgabe angelegt wird, wenn diese Anwendung sofort nutzbar sein soll.

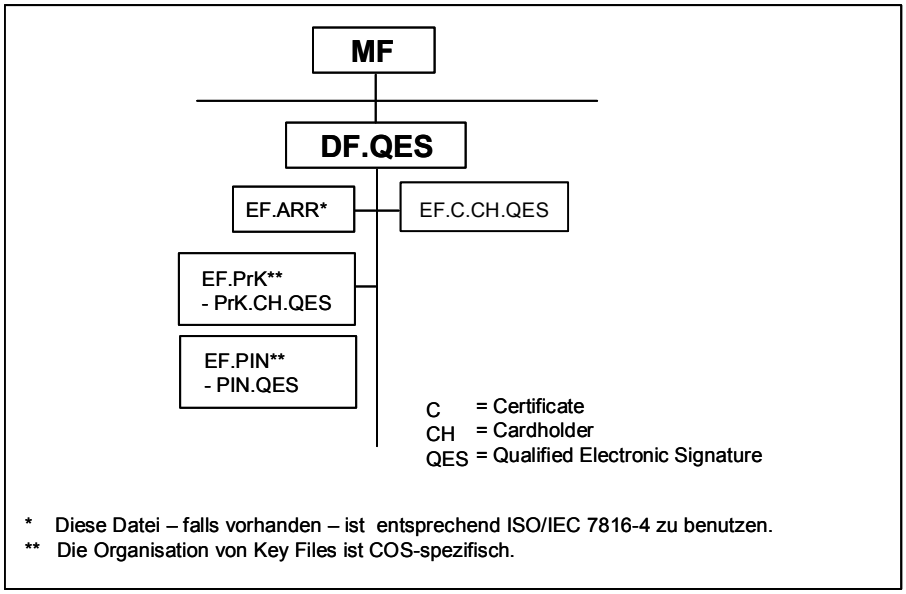

Abbildung 7 – Dateistruktur der Anwendung DF.QES

Das Vorhandensein von DF.QES wird in EF.DIR angezeigt.

Als Security Environment wird das Default SE (SE # '01') verwendet.

6.3 Dateistruktur und Dateiverwendung

6.3.1 EF.ARR

EF.ARR wird für die Speicherung der Zugriffsregeln in DF.QES verwendet.

6.3.2 EF.PrK

EF.PrK enthält den privaten QES-Schlüssel für die qualifizierte elektronische Signatur. Die kryptografischen Parameter müssen dem Algorithmenkatalog für elektronische Signaturen genügen [ALGCAT].

Als Schlüssel-Referenz ist gemäß [DIN66291-4] '84' zu verwenden.

Tabelle 91 – Schlüsselreferenz und Schutz

Name des Schlüssels	KeyRef	Schutz	Rücksetzung des Sicherheitsstatus nach n Signaturen
PrK.CH.QES	'84'	PIN.QES	n = 1

6.3.3 EF.PIN

Diese Datei ist für die Verwendung von PIN.QES vorgesehen. Die PIN-Charakteristika sind in der nachfolgenden Tabelle dargestellt.

Tabelle 92 - PIN-Charakteristika von PIN.QES

PIN-Name	PIN-Länge	PIN-Referenz	Anfangswert des Resetting Code	Resetting Code	Nutzungsbegrenzung des Resetting Code
PIN.QES	6-8 Ziffern	'81'	3	8 Ziffern	10 mal

Anmerkung: Nur die Mindestlänge wird von der eGK kontrolliert.

Wenn die eGK an den Karteninhaber ausgehändigt wird, kann z.B. ein Transport-PIN-Verfahren angewandt werden.

Die PIN ist änderbar, aber mit dem RESET RETRY COUNTER-Kommando kann kein neuer PIN-Wert eingetragen werden.

6.3.4 EF.C.CH.QES

In dieser Datei wird das X.509-QES-Zertifikat gespeichert.

6.4 QES-Anwendungsselektion

Die folgenden zwei Tabellen zeigen das ISO/IEC 7816-4 Kommando für die ‘Direkte Anwendungsselektion’.

Tabelle 93 – SELECT Kommando für die Selektion von DF.QES

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘A4’ = SELECT
P1	‘04’ = DF-Selektion mit AID
P2	'0C' = Kein FCI zurückgeben
Lc	‘06’ = Länge des nachfolgenden Datenfeldes
Datenfeld	‘D27600006601’ = AID von DF.QES
Le	Nicht vorhanden

Tabelle 94 – SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

6.5 PIN-Management

Die Verwendung des privaten Schlüssels für die qualifizierte elektronische Signatur erfordert eine erfolgreiche Präsentation der PIN.QES vor jeder Signatur-Berechnung. Folgende PIN-Management-Funktionen werden unterstützt:

Tabelle 95 – VERIFY Kommando zur Freischaltung der Benutzung des privaten QES-Schlüssels

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘20’ = VERIFY
P1	‘00’
P2	‘81’ = PIN.QES-Referenz
Lc	‘08’ = Länge des nachfolgenden Datenfeldes
Datenfeld	PIN, Format: siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 96 – VERIFY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Zur Änderung der PIN.QES ist das Kommando CHANGE REFERENCE DATA zu verwenden.

Tabelle 97 – CHANGE RD Kommando zur Änderung von PIN.QES

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘24’ = CHANGE REFERENCE DATA
P1	‘00’ = Referenzdaten ersetzen
P2	‘81’ = PIN.QES-Referenz
Lc	‘10’ = Länge des nachfolgenden Datenfeldes
Datenfeld	PIN_alt || PIN_neu, Format: siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 98 – CHANGE RD Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nach dreimaliger aufeinander folgender Falscheingabe von PIN.QES ist diese Authentisierungsmethode blockiert. Mit dem Kommando RESET RETRY COUNTER kann der Retry Counter 10 mal wieder auf seinen Anfangswert gesetzt werden.

Tabelle 99 – RESET RC Kommando zum Rücksetzen des Retry Counters

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2C' = RESET RETRY COUNTER
P1	'01' = Datenfeld enthält Resetting Code
P2	'81' = PIN.QES-Referenz
Lc	'08' = Länge des nachfolgenden Datenfeldes
Datenfeld	Resetting Code ("PUK", 8 Byte); Format: siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 100 – RESET RC Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

6.6 Erzeugen einer qualifizierten elektronischen Signatur

6.6.1 Signieren mit „Final Hashing" in der Karte

Zur Selektion des Hash-Verfahrens ist das Kommando MSE zu verwenden.

Tabelle 101 – MSE Kommando zur Selektion des Hash-Algorithmus

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für Hash-Berechnung
P2	'AA' = Hash-Template
Lc	'03' = Länge des nachfolgenden Datenfeldes
Datenfeld	80 01 xx' = DO für AlgID, siehe Tabelle 10 [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 102 – MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anschließend ist der private QES-Schlüssel zusammen mit dem Signatur-Verfahren zu selektieren.

Tabelle 103 - MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für DS-Berechnung
P2	'B6' = DST
Lc	'06' = Länge des nachfolgenden Datenfeldes
Datenfeld	'84 01 84 || 80 01 12' = DO für KeyRef von PrK.CH.QES || DO für AlgID, siehe [gemSpec_eGK_P1]
Le	nicht vorhanden

Tabelle 104 - MSE Antwort

Datenfeld	nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anschließend ist das Kommando PSO: HASH an die eGK zu senden.

Tabelle 105 – PSO: HASH Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2A' = PSO: HASH
P1	'90' = Compute hash
P2	'A0' = Input Template für Hash-Berechnung
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	'90 xx ... || 80 xx ...' = DO mit Hash-Zwischenwert (bisher berechneter Hash-wert (x Byte) || Anzahl der bereits gehashten Bits (y Byte)) || DO mit letzten Teil der zu hashenden Daten (z Byte), siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 106 – PSO: HASH Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Nachdem die eGK den „Final Hashwert" berechnet hat, kann das Kommando PSO: COMPUTE DS gesendet werden.

Tabelle 107 – PSO: COMPUTE DS Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘2A’ = PSO: COMPUTE DS
P1	‘9E’ = Compute digital signature
P2	‘9A’ = Zu signierende Daten (wurden durch PSO:HASH bereitgestellt)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	’00’

Tabelle 108 – PSO: COMPUTE DS Antwort

Datenfeld	Signatur
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

6.6.2 Signieren mit Hashen außerhalb der Karte

Zur Selektion des Signaturschlüssels und des Algorithm Identifiers ist das Kommando MSE zu verwenden.

Tabelle 109 – MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET für DS-Berechnung
P2	‘B6’ = DST
Lc	‘06’ = Länge des nachfolgenden Datenfeldes
Datenfeld	‘84 01 84 || 80 01 xx’ = DO für KeyRef von PrK.CH.QES || DO für AlgID, siehe [gemSpec_eGK_P1]
Le	Nicht vorhanden

Tabelle 110 – MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anschließend wird mit dem Kommando PSO: COMPUTE DS entweder

die Digestinfo (bei Padding-Verfahren nach [PKCS#1]) oder

der Hash-Wert (bei Padding-Verfahren nach ISO 9796 RND)

übergeben. Als Antwort wird die Signatur zurückgeliefert. Derzeit wird nur das Paddingverfahren nach [PKCS#1] verwendet.

Tabelle 111 – PSO: COMPUTE DS Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'2A' = PSO: COMPUTE DS
P1	'9E' = Berechne digitale Signatur
P2	'9A' = Zu signierende Daten
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	Digestinfo (Padding-Verfahren nach [PKCS#1])
Le	'00'

Tabelle 112 – PSO: COMPUTE DS Antwort

Datenfeld	Signatur
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

6.6.3 Lesen des X.509-QES-Zertifikats

Zum Lesen des X.509.QES-Zertifikats wird das READ BINARY-Kommando verwendet, siehe Kapitel 0 (FID/SFID: siehe Anhang B).

6.7 Kryptografische Informationsanwendung

6.8 Allgemeines Konzept und Struktur von DF.CIA.ESIGN

In [CWA14890-1] und [CWA14890-2] ist das Vorhandensein einer kryptografischen 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
- EF.OD (Object Directory)

und normalerweise weitere

- EFs, welche die FIDs, Schlüssel, PINs, Zertifikate etc. beschreiben.

Im Fall der eGK enthält das zugeordnete DF.CIA.ESIGN nur EF.CIAInfo, das den Profile Identifier bereitstellt, welcher auf [DIN 66291-4] verweist, siehe Anhang C. 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, d.h. seine Abwesenheit bedeutet, dass keine Objektverzeichnisinformation in weiteren EFs von DF.CIA.ESIGN zur Verfügung steht.

Falls jedoch weitere Schlüssel und kryptografische Protokolle verfügbar sind, dann muss dies entweder explizit nach [ISO7816-15] beschrieben oder durch einen anderen Profile Identifier angezeigt werden.

6.9 Dateistruktur und Dateiverwendung

Abbildung 8 zeigt die allgemeine Dateistruktur von DF.CIA.ESIGN wie sie in der eGK zur Anwendung kommt.

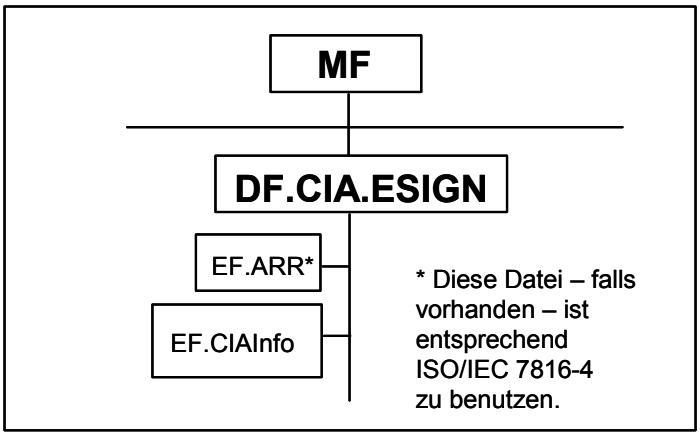

Abbildung 8 - Dateistruktur von DF.CIA.ESIGN

6.9.1 EF.ARR

EF.ARR enthält die Zugriffsregeln für EFs, die DF.CIA.ESIGN zugehören.

6.9.2 EF.CIAInfo

EF.CIAInfo enthält die CIA-Information, insbesondere den Profile Identifier, siehe Anhang C. Diese Datei ist immer lesbar und wird nicht aktualisiert.

Wenn zusätzliche Funktionen zur Verfügung stehen, z.B. Signaturfunktion auf Basis von Elliptischen Kurven, können diese ebenfalls in der CIA-Information angezeigt werden.

6.10 Anwendungsselektion

Die nachfolgenden Tabellen zeigen das ISO/IEC 7816-4 Kommando für die 'Direkte Anwendungsselektion'.

Tabelle 113 - SELECT Kommando für DF.CIA.ESIGN-Selektion mit AID

CLA	'00'
INS	'A4' = SELECT
P1	'04' = DF-Selektion mit AID
P2	'0C' = Keine FCI zurückgeben
Lc	'0F' = Länge des nachfolgenden Datenfeldes
Datenfeld	'E828BD080F A000000167 455349474E' = AID von DF.CIA.ESIGN
Le	Nicht vorhanden

Tabelle 114 – SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

6.11 Lesen der CIA-Information

Die CIA-Daten werden mit dem ISO/IEC 7816-4 Kommando READ BINARY gelesen.

Tabelle 115 – READ BINARY Kommando zum Lesen der CIA-Daten

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'B0' = READ BINARY
P1	'92' = b8-b6: 100 b5-b1: 10010 SFID von EF.CIAInfo: 18
P2	'00' = Offset
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'00' = Lesen bis Dateiende oder 'xx' = Länge der erwarteten Daten

Tabelle 116 – READ BINARY Antwort

Datenfeld	CIOs
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

7 Karten-Managementfunktionen für die Aktivierung / Deaktivierung von DF.HCA

7.1 Überblick

Der Tatbestand einer verlorenen oder gestohlenen eGK kann im Datenbestand des betreffenden Kartenherausgebers dokumentiert werden. Wenn eine solche Karte in einer Interaktion mit einem System des Kartenherausgebers wieder erkannt wird, dann kann dieser Server ein DEACTIVATE FILE Kommando zum Deaktivieren von DF.HCA senden. Die Reaktivierung von DF.HCA ist ebenso möglich.

7.1.1 Auslesen der ICCSN

Die ICCSN kann wie in Kapitel 3.2.14 beschrieben ermittelt werden, d.h. das Auslesen der ICCSN muss dem Reset folgen.

7.1.2 Ausführung des Authentisierungsverfahrens

Es wird das in Kapitel 3.7 beschriebene C2S-Authentisierungsverfahren mit einem der Schlüssel SK.VSDD, SK.CAMS oder SK.VSDDCAMS verwendet.

7.2 Deaktivierung von DF.HCA

Für die Deaktivierung von DF.HCA wird das DEACTIVATE FILE Kommando verwendet. Zuvor ist DF.HCA mit dem SELECT-Kommando zu selektieren, siehe Kapitel 4.2. Die Zugriffsbedingungen für das DEACTIVATE FILE-Kommando sind in Anhang B dargestellt.

Tabelle 117 – DEACTIVATE FILE Kommando zum Deaktivieren der HCA

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘04’ = DEACTIVATE FILE
P1	‘00’
P2	‘00’
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	Nicht vorhanden

Tabelle 118 – DEACTIVATE FILE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

7.3 Aktivierung von DF.HCA

Zum Aktivieren von DF.HCA wird das ACTIVATE FILE Kommando verwendet. Zuvor ist DF.HCA mit dem SELECT-Kommando zu selektieren, siehe Kapitel 4.2. Die Zugriffsbedingungen für das ACTIVATE FILE-Kommando sind in Anhang B dargestellt.

Tabelle 119 – ACTIVATE FILE Kommando zur Re-Aktivierung der HCA

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'44' = ACTIVATE FILE
P1	'00'
P2	'00'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	Nicht vorhanden

Tabelle 120 – ACTIVATE FILE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anmerkung: Falls das File schon aktiviert war, wird ebenfalls als Status-Code '9000' zurückgegeben.

8 Aktivierung / Deaktivierung von EF.Notfalldaten

8.1 Überblick

Im Fachkonzept des Notfalldatenmanagements wird gefordert, dass der Versicherte den Notfalldatensatz verbergen können muss.

8.2 Deaktivierung von EF.Notfalldaten

Für die Deaktivierung von EF.Notfalldaten wird das DEACTIVATE FILE Kommando verwendet. Zuvor ist DF.HCA mit dem SELECT-Kommando zu selektieren, siehe Kapitel 4.2. Die Zugriffsbedingungen für das DEACTIVATE FILE-Kommando sind in Anhang B dargestellt.

Tabelle 121 - DEACTIVATE FILE Kommando zum Deaktivieren der Notfalldaten

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'04' = DEACTIVATE FILE
P1	'02'
P2	'00'
Lc	'02' = Länge des nachfolgenden Datenfeldes
Datenfeld	File Identifier von EF.Notfalldaten
Le	Nicht vorhanden

Tabelle 122 - DEACTIVATE FILE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

8.3 Aktivierung von EF.Notfalldaten

Zum Aktivieren von EF.Notfalldaten wird das ACTIVATE FILE Kommando verwendet. Zuvor ist DF.HCA mit dem SELECT-Kommando zu selektieren, siehe Kapitel 4.2. Die Zugriffsbedingungen für das ACTIVATE FILE-Kommando sind in Anhang B dargestellt.

Tabelle 123 – ACTIVATE FILE Kommando zur Re-Aktivierung der Notfalldaten

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'44' = ACTIVATE FILE
P1	'02'
P2	'00'
Lc	'02' = Länge des nachfolgenden Datenfeldes
Datenfeld	File Identifier von EF.Notfalldaten
Le	Nicht vorhanden

Tabelle 124 - ACTIVATE FILE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anmerkung: Falls das File schon aktiviert war, wird ebenfalls als Status-Code '9000' zurückgegeben.

9 Karten-Managementfunktionen für das Erzeugen / Löschen von Dateien oder Anwendungen

9.1 Überblick

Die Unterstützung von Karten-Managementfunktionen für das Erzeugen/Löschen von Dateien oder Anwendungen ist obligatorisch.

Ein Karten-Managementverfahren kann in folgenden Schritten ablaufen:

- Reset der Karte
- Abruf des Inhalts von EF.GDO
- Abruf des Inhalts von EF.DIR
- Abruf der Karteneigenschaften (DO Kartendaten)
- Selektion des DF für die Bearbeitung
- (z.B. DF.HCA für das Hinzufügen von Dateien innerhalb der Gesundheitsanwendung oder MF für das Hinzufügen eines neuen DF)
- Im Falle des Erzeugens oder Löschens eines EF: Abruf des Inhalts des Datenobjektes mit dem Tag '6E', DO anwendungsbezogene Daten.
- Gegenseitige Authentisierung mit Vereinbarung von Sitzungsschlüsseln und Bildung eines SSC zwischen eGK und Karten-Anwendungs-Managementsystem (CAMS).
- Abfolge von Kommandos für das Karten-Management.

Die folgende Beschreibung bezieht sich auf die oben erwähnten Abfolgen von Kommandos für das Karten-Management.

9.2 Lesen von kartenbezogenen Daten

Zum Lesen der Inhalte von EF.ATR, EF.DIR und EF.GDO siehe Kapitel 3.2.14.

Das EF.ATR muss Informationen über die Karte, in einem Datenobjekt mit dem Tag '66' enthalten (Datenobjekt mit Tag '46' mit Angaben über den Betriebssystemhersteller, der Maskenversion etc., die aufgrund des begrenzten Speichers nicht im ATR übermittelt werden, siehe Tabelle 125.

Das gesamte DO Kartendaten mit Tag '66' muss an das CAMS übermittelt werden, wo die relevanten Daten abgerufen werden können.

Die hier abgerufenen karten- und anwendungsbezogenen Daten werden vom jeweiligen Terminal nicht interpretiert (auch nicht hinsichtlich eines formalen Aufbaus), sondern transparent an das CAMS weitergereicht.

In der nachfolgenden Tabelle mit der Reihenfolge von oben nach unten ist der Inhalt des Datenobjektes mit dem Tag ‘46’ (DO ’Pre-issuing data’) dargestellt.

Tabelle 125 – Inhalt des DO Pre-Issuing Data (Tag ’46’)

Länge	Beschreibung
1 Byte	Chip-Hersteller-ID ICM (siehe www.sc17.com)
5 Byte	Kartenhersteller-ID (siehe DIN-RA www.sit.fraunhofer.de)
x Byte	IC-ID (herstellerspezifisch)
x Byte	COS-Version (herstellerspezifisch)
x Byte	ROM-Maskenversion (herstellerspezifisch)

9.3 Aufbau eines sicheren Kanals zwischen eGK und CAMS

Für die Erzeugung oder Löschung von DF oder EF müssen die entsprechenden Kommandos durch die Verwendung von Secure Messaging geschützt werden. Deshalb muss ein gesicherter Kanal zwischen der eGK und dem Karten-Managementsystem aufgebaut werden, siehe Kapitel 3.7.

Alle im Folgenden beschriebenen Kommandos müssen mit Secure Messaging – zumindest mit MAC geschützt – ausgeführt werden, das gilt für Daten des Kommandos und der Antwort. Falls vertrauliche Information wie Schlüssel oder Passwörter übermittelt werden, müssen die relevanten Befehlsdaten verschlüsselt sein.

Anmerkung: Wenn eine Karte in den verschiedenen Befehlen einer Befehlskette den Wechsel von verschlüsselten und unverschlüsselten Befehlsdaten nicht unterstützt, kann es notwendig sein, alle Befehlsdaten der Kette zu verschlüsseln.

9.4 Erzeugen und Löschen von Anwendungen und Dateien

Die Befehle zum Erzeugen von Anwendungen und Dateien sind in [gemSpec_eGK_P1] beschrieben. Die erforderlichen Kommandosequenzen sind herstellerspezifisch. Es sind jedoch entsprechende Zugriffsregeln vorzusehen, siehe Anhang B. Löschen von EFs oder einer Anwendung ist nicht erlaubt, falls keine explizite Zugriffsregel dies erlaubt.

Anhang A
(normativ)
ATR

A.1 ATR-Kodierung

Tabelle A.1 zeigt die Kodierung des ATR für die eGK (T = 1 Karten).

Tabelle A. 1 – ATR-Kodierung (Sequenz von oben nach unten)

Zeichen	Wert	Bedeutung
TS	‘3B’	Initial Character (direct convention)
T0	‘9x’	Format Character (TA1/TD1 indication, x = no. of HB)
TA1	‘xx’	Interface Character (FI/DI, erlaubte Werte: siehe [gemSpec_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)

Für die Kodierung der Historical Bytes gelten die folgenden Konventionen in Übereinstimmung mit ISO/IEC 7816-4:

CI	‘00’ gemäß ISO/IEC 7816-4
TPI	‘6x’ gemäß ISO/IEC 7816-4 (x kodiert die Länge des DO)
ICM	IC Herstellerkennung
ICT	Kodierung herstellerspezifisch
OSV	Kodierung herstellerspezifisch
DD	Kodierung herstellerspezifisch (normalerweise nicht verwendet)

TCS	'31' gemäß ISO/IEC 7816-4
CS	Card Service Data Byte gemäß ISO/IEC 7816-4
TCC	'73' gemäß ISO/IEC 7816-4
CCB	Card Capabilities Data Bytes gemäß ISO/IEC 7816-4 (Anzeige von unterstützten logischen Kanälen, Extended Le-Feld, …)
CLS	Card Life Cycle (Default-Wert '00')
SW1-SW2	'9000'

Aus Performancegründen ist es erlaubt, ein TC1 mit dem Wert 'FF' im ATR anzuzeigen.

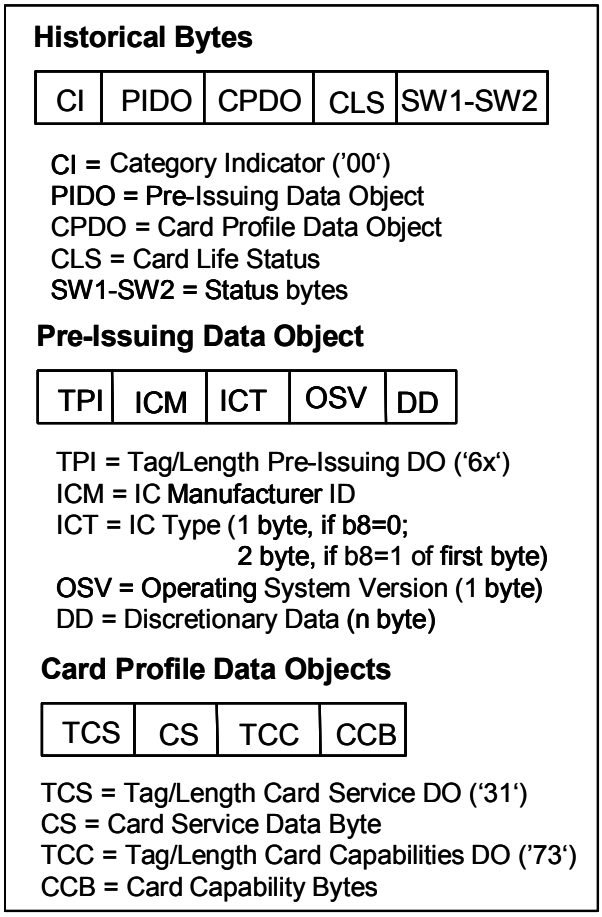

Abbildung 9 - Struktur der Historical Bytes

Die aktuellen Werte für die Chip-Hersteller-Kennung (IC Manufacturer ICM) können unter www.sc17.com abgerufen werden.

Anhang B
(normativ)
Dateiattribute, Zugriffsbedingungen und Sicherheitsumgebungen

B.1 eGK Dateieigenschaften und Zugriffsregeln

Nur solche EFs sind beschrieben, auf die mit Read/Update/Append-Kommandos nach der Personalisierung der eGK zugegriffen werden kann.

Die in den Tabellen dargestellten Zugriffsregeln sind konform zu [ISO7816-4]. Die Kodierung kann für eine spezielle COS-Plattform davon abweichen (z.B. durch eine abweichende Strategie, mit CHAs umzugehen). Trotzdem muss die Funktionalität identisch sein.

Eine COS-spezifische SM-Schlüsselreferenz muss in CCT und CT vorhanden sein, wenn der Sicherheits-Status in Bezug auf die Authentisierung bei Auftreten eines SM-Fehlers nicht zurückgesetzt wird.

Alle definierten EFs sind bei eGK-Ausgabe im Zustand "activated". Falls ein Dual-Interface-Chip mit RF-Interface verwendet wird, dann ist über eine entsprechende Zugriffsregel sicherzustellen, dass die beschriebenen Anwendungen nur über das kontakt-basierte Interface genutzt werden können.

Hinweis: Die Zugriffsregeln SOLLEN in einem EF.ARR gespeichert werden. EF.ARR KANN auch durch andere Verfahren ersetzt werden, wenn dieselbe Funktionalität garantiert wird.

Hinweis:
In dieser Version werden die Zugriffsregeln nicht mehr als Rekord in einem EF.ARR spezifiziert, dessen Inhalt hexadezimal angegeben wird. Vielmehr werden die Zugriffsregeln tabellarisch für jedes File, jeden Schlüssel und jede PIN explizit angegeben. Die erste Spalte der Tabelle enthält das Objekt, die zweite die Zugriffsarten und die dritte die jeweiligen Zugriffsbedingungen. Die Darstellung ist äquivalent zur hexadezimalen Darstellung aus der Vorgängerversion, aber leichter verständlich und leichter zu pflegen.
Zugriffsbedingungen werde in Form eines boolschen Ausdrucks angegeben, der aus folgenden Elementen bestehen kann:

1. Always: Die Zugriffsart ist stets erlaubt, unabhängig vom Sicherheitszustand, mit und ohne Secure Messaging
2. Never: Die Zugriffsart ist niemals erlaubt.
3. PIN.x: Das boolsche Element liefert TRUE genau dann, wenn der Sicherheitszustand von PIN.x gesetzt ist.
4. CHA.x: Das boolsche Element liefert TRUE genau dann, wenn die Rolle CHA.x authentisiert wurde.
5. TC_ENC_MAC(x): Das boolsche Element liefert TRUE genau dann, wenn der Schlüssel bzw. die Rolle x authentisiert wurde UND die Kommando APDU MAC gesichert ist UND optional vorhandene Kommandodaten verschlüsselt (Tag ´87´) übertragen wurden. Die Antwort APDU MUSS MAC gesichert werden und vorhandene Antwortdaten MÜSSEN verschlüsselt werden.
6. TC_ENC_MAC(*): Das boolsche Element wird genauso behandlet wie TC_ENC_MAC(x), aber das Wildcardsymbol '*' zeigt an, dass jeder Schlüssel für den Aufbau des Trusted Channels akzeptiert wird.

7. Die boolschen Elemente PIN.x, CHA.x und TC_ENC_MAC(…) können mittels „AND“ und „OR“ zu einem boolschen Ausdruck verknüpft werden. Der Zugriff ist erlaubt, wenn der boolsche Ausdruck als Wert TRUE liefert.

Hinweis: In den Tabellen mit Zugriffsbedingungen ist das Kommando SEARCH BINARY nicht vorhanden, weil dieses Kommando in [gemSpec_eGK_P1] nicht obligatorisch ist. Falls das COS das Kommando SEARCH BINARY unterstützt, dann MUSS die Zugriffsbedingung eines EFs für dieses Kommando entweder „Never“ sein, oder identisch zur Zugriffsbedingung des Kommandos READ BINARY gewählt werden. Insofern fällt dieses Kommando dann nicht in die Kategorie „Andere Kommandos“, die in den Tabellen enthalten ist.

B.2 MF-Ebene

B.2.1 EFs

Tabelle B. 1 – EFs auf MF-Ebene und ihre Eigenschaften

Datei	FID / SFID	Dateistruktur	Dateigröße (Datenlänge)
EF.ATR (ATR Extension Data)	‘2F01’ / 29	transparent	herstellerspezifisch, siehe Kapitel C.1.1
EF.DIR (Application Directory)	‘2F00’ / 30	linear variabel	10 Records mit max. 19 Byte/Record
EF.GDO (Global Data Objects)	‘2F02’ / 2	transparent	12 Byte
EF.StatusPIN	‘2F05’ / 5	transparent	10 Byte
EF.CVC.eGK.AUT (CVC der eGK für AUT)	‘2F03’ / 3	transparent	209 Byte
EF.CVC.CA_eGK.CS (CVC der CA)	‘2F04’ / 4	transparent	210 Byte
EF.Version	‘2F10’ / 16	Linear fix	4 Record a 5 Byte

Anmerkung:
FID/SFID von EF.DIR sind in [ISO-7816-4] festgelegt. Ebenso ist die FID von EF.ATR in [ISO-7816-4] spezifiziert.

B.2.2 Zugriffsregeln auf MF-Ebene

Wenn keine Einschränkung bzgl. SE # angegeben ist, dann gilt die Zugriffsregel für alle SEs auf MF-Ebene. Die Zugriffsregeln DÜRFEN NICHT veränderbar sein.

Tabelle B. 2 – Zugriffsregeln auf MF–Ebene

Objekt	Zugriffsart	Zugriffsbedingung
MF	LOAD APPLICATION	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	CREATE DF	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	CREATE EF	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.ATR und EF.GDO und EF.CVC.CA_eGK.CS und EF.CVC.eGK.AUT	READ BINARY	Always
	UPDATE BINARY	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.DIR	APPEND RECORD	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	READ RECORD SEARCH RECORD	Always
	UPDATE RECORD	Never
	ACTIVATE FILE	Never
	DEACTIVATE RECORD	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.StatusPIN	READ BINARY	Always
	UPDATE BINARY	CHA.1 OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.7 OR CHA.8 OR CHA.9 OR CHA.10
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Version	APPEND RECORD	Never
	READ RECORD SEARCH RECORD	Always
	UPDATE RECORD	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	Never
	DEACTIVATE RECORD	Never

Objekt	Zugriffsart	Zugriffsbedingung
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
PIN.home	CHANGE REFERENCE DATA und P1=´00´	Always
	RESET RETRY COUNTER und P1 aus der Menge {´00´, ´01}	Always
	VERIFY	Always
	Andere Kommandos	Never
PIN.CH in SE #01	CHANGE REFERENCE DATA und P1=´00´	Always
	RESET RETRY COUNTER und P1 aus der Menge {´00´, ´01}	Always
	VERIFY	Always
	Andere Kommandos	Never
PIN.CH in SE #02	CHANGE REFERENCE DATA	Never
	RESET RETRY COUNTER	Never
	VERIFY	Always
	Andere Kommandos	Never
SK.CAMS und SK.VSDD und SK.VSDDCAMS	MUTUAL AUT.	Always
	Andere Kommandos	Never
PrK.eGK.AUT in SE #01	GENERATE ASYMMETRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Always
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	Never
	PSO Decipher	Never
	Andere Kommandos	Never
PrK.eGK.AUT in SE #02	GENERATE ASYMMETRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Always
	EXTERNAL AUTH.	Always
	PSO Compute Digital Signature	Never
	PSO Decipher	Never
	Andere Kommandos	Never

B.3 DF.HCA

B.3.1 EFs unter DF.HCA

Tabelle B. 3 – HCA-Dateien und ihre Eigenschaften

Datei	FID/ SFID	Datei-struktur	Dateigröße (Datenlänge)
EF.PD (Personen-Daten)	'D001' / 1	transparent	850 Byte
EF.VD (Versicherten-Daten)	'D002' / 2	transparent	1250 Byte *
EF.GVD (Geschützte Vers.-Daten)	'D003' / 3	transparent	450 Byte
EF.StatusVD	'D00C' / 12	transparent	25 Byte
EF.DM (Display Message)	'D004' / 4	transparent	8 Byte
EF.Einwilligung	'D005' / 5	transparent	55 Byte
EF.Logging	'D006' / 6	zyklisch	50 Records mit 46 Byte/Record
EF.eRezept_Tickets	'D007' / 7	linear fix	8 Records mit 165 Byte/Rec.
EF.StatusRezept	'D00D' / 13	transparent	25 Byte
EF.eRezept_Container	'D008' / 8	transparent	30.000 Byte
EF.Verweis	'D009' / 9	linear fix	10 Records mit 20 Byte/Record
EF.eNotfalldaten	'D00B' / 11	transparent	5600 Byte
EF.Status.Notfalldaten	'D00E' / 14	transparent	25 Byte

* Anmerkung:

In der Startphase werden die Daten von EF.GVD mit in EF.VD gespeichert. Später werden die Daten dann wieder in EF.GVD untergebracht. In diesem Fall reduziert sich der Speicherplatzbedarf für EF.VD von 1250 Byte auf 800 Byte.

B.3.2 Zugriffsregeln in DF.HCA

Die Zugriffsregeln für DF.HCA sind noch nicht endgültig festgelegt und werden noch zwischen dem BMG, der gematik und den Leistungserbringer-Organisationen abgestimmt.

Hinweise:

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
6	Damit Rolle CHA.6 im DF.HCA Aktionen ausführen kann ist es notwendig einen Trusted Channel aufzubauen. Dies ist in der folgenden Tabelle nicht extra ausgewiesen
CAMS	Rolle des CAMS repräsentiert durch den Schlüssel SK.CAMS

VSCA	Rolle des VSDD/CAMS repräsentiert durch den Schlüssel SK.VSDDCAMS
VSDD	Rolle des VSDD repräsentiert durch den Schlüssel SK.VSDD
C, Create	Recht neue Dateien, PINs oder Schlüssel anzulegen
R, Read	Recht zu lesen und in strukturierten Dateien zu suchen (SEARCH RECORD)
U, Update	Recht zu Schreiben und zu Überschreiben (= Löschen von Information)
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.

Tabelle B. 4 Zugriffsrechtematrix

Object	ALW	home	1	1+CH	2	2+CH	8	8+CH	3	3+CH	9	9+CH	6	6+CH	4	4+CH	10	10+CH	5	5+CH	7	7+CH	CAMS	VSCA	VSDD
DF.HCA																							CAD	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	R	R	R	RU	RU
EF.GVD		R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R				RU	RU
EF.Einwilligung		R		R		RU		R		RU		R		R		RU									
EF.Verweis		RAD		RAD		RUAD		R		RUAD		R		R		RUAD									
EF.eRezept_Tickets		RAD		RUAD	RU	RU	RU	RU	RU	RU	RU	RU	RU	RU					RU	RU					
EF.StatusRezept EF.eRezept_Container				R	RU	RU	RU	RU	RU	RU	RU	RU	RU	RU					RU	RU					
EF.Notfalldaten EF.StatusNotfalldaten		AD		AD	R	RU	R	RU	R	RU	R	RU			R	RU					R	R			
EF.Logging		R		Ra	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a			
EF.DM		U											R	R									R	R	R

Die obige Tabelle stellt die Zugriffsrechte übersichtlich, einfach und kompakt dar. Die folgende Tabellezeigt die Zugriffsrechte detailliert aus **technischer** Sicht. Die Zugriffsregeln DÜRFEN NICHT veränderbar sein.

Wenn keine Einschränkung bzgl. SE # angegeben ist, dann gilt die Zugriffsregel für alle SEs in DF.HCA.

Tabelle B. 5 – Zugriffsregeln in DF.HCA

Objekt	Zugriffsart	Zugriffsbedingung
DF.HCA	CREATE EF	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	DEACTIVATE FILE	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	DELETE FILE	Never
	Andere Kommandos	Never
EF.PD und EF.VD und EF.StatusVD	READ BINARY	Always
	UPDATE BINARY	TC_ENC_MAC(SK.VSDD) OR TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.GVD in SE #01	READ BINARY	PIN.home OR (CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.8 OR CHA.9 OR CHA.10 OR TC_ENC_MAC(SK.VSDD) OR TC_ENC_MAC(SK.VSDDCAMS)
	UPDATE BINARY	TC_ENC_MAC(SK.VSDD) OR TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.GVD in SE #02	READ BINARY	TC_ENC_MAC(CHA.6)
	UPDATE BINARY	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.DM	READ BINARY	TC_ENC_MAC(CHA.6) OR TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDD) OR TC_ENC_MAC(SK.VSDDCAMS)
	UPDATE BINARY	PIN.home
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Einwilligung in SE #01	READ BINARY	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH) OR (CHA.8 AND PIN.CH) OR (CHA.9 AND PIN.CH)

Objekt	Zugriffsart	Zugriffsbedingung
	UPDATE BINARY	(CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Einwilligung in SE #02	READ BINARY	PIN.CH AND TC_ENC_MAC(CHA.6)
	UPDATE BINARY	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Logging in SE #01	APPEND RECORD	(CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.7 OR CHA.8 OR CHA.9 OR CHA.10
	READ RECORD SEARCH RECORD	PIN.home OR (CHA.1 AND PIN.CH)
	UPDATE RECORD	Never
	ACTIVATE FILE	Never
	DEACTIVATE RECORD	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Logging in SE #02	APPEND RECORD	TC_ENC_MAC(CHA.6)
	READ RECORD SEARCH RECORD	Never
	UPDATE RECORD	Never
	ACTIVATE FILE	Never
	DEACTIVATE RECORD	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.eRezept_Tickets in SE #01	APPEND RECORD	Never
	READ RECORD SEARCH RECORD	PIN.home OR (CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.5 OR CHA.8 OR CHA.9
	UPDATE RECORD	(CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.5 OR CHA.8 OR CHA.9
	ACTIVATE FILE	PIN.home OR (CHA.1 AND PIN.CH)

Objekt	Zugriffsart	Zugriffsbedingung
	DEACTIVATE RECORD	PIN.home OR (CHA.1 AND PIN.CH)
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.eRezept_Tickets in SE #02	APPEND RECORD	Never
	READ RECORD SEARCH RECORD	TC_ENC_MAC(CHA.6)
	UPDATE RECORD	TC_ENC_MAC(CHA.6)
	ACTIVATE FILE	Never
	DEACTIVATE RECORD	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.StatusRezept und EF.eRezept_Container in SE #01	READ BINARY	(CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.5 OR CHA.8 OR CHA.9
	UPDATE BINARY	CHA.2 OR CHA.3 OR CHA.8 OR CHA.9
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.StatusRezept und EF.eRezept_Container in SE #02	READ BINARY	TC_ENC_MAC(CHA.6)
	UPDATE BINARY	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Verweis in SE #01	APPEND RECORD	Never
	READ RECORD SEARCH RECORD	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH) OR (CHA.8 AND PIN.CH) OR (CHA.9 AND PIN.CH)
	UPDATE RECORD	(CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH)
	ACTIVATE FILE	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH)
	DEACTIVATE RECORD	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH)

Objekt	Zugriffsart	Zugriffsbedingung
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Verweis in SE #02	APPEND RECORD	Never
	READ RECORD SEARCH RECORD	PIN.CH AND TC_ENC_MAC(CHA.6)
	UPDATE RECORD	Never
	ACTIVATE FILE	Never
	DEACTIVATE RECORD	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.Notfalldaten und EF.StatusNotfalldaten	READ BINARY	CHA.2 OR CHA.3 OR CHA.4 OR CHA.7 OR CHA.8 OR CHA.9
	UPDATE BINARY	(CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH) OR (CHA.8 AND PIN.CH) OR (CHA.9 AND PIN.CH)
	ACTIVATE FILE	PIN.home OR CHA.1 AND PIN.CH
	DEACTIVATE FILE	PIN.home OR CHA.1 AND PIN.CH
	DELETE FILE	Never
	Andere Kommandos	Never

Tabelle B. 6 – Authentisierungs-Templates für HPC- und SMC-Authentisierung gegenüber eGK

Profil-Nr. I	Profilkennung	CHA Wert
1	CHA.1	'D276000040001A'
2	CHA.2	'D276000040002A'
3	CHA.3	'D276000040003A'
4	CHA.4	'D276000040004A'
5	CHA.5	'D276000040005A'
6	CHA.6	'D276000040006A'
7	CHA.7	'D276000040007A'
8	CHA.8	'D276000040008A'
9	CHA.9	'D276000040009A'
10	CHA.10	'D27600004000AA'

B.4 DF. ESIGN

B.4.1 EFs unter DF. ESIGN

Tabelle B. 7 – DF.ESIGN-Dateien und ihre Eigenschaften

Datei	FID / SFID	Dateistruktur	Dateigröße (Dateilänge)

Datei	FID / SFID	Dateistruktur	Dateigröße (Dateilänge)
EF.C.CH.AUT (X.509-AUT-Zertifikat)	'C500' /1	transparent	1536 Byte oder Länge des Zertifikats
EF.C.CH.AUTN (X.509-AUT-Pseudonym-Zertifikat)	'C509' /9	transparent	1536 Byte oder Länge des Zertifikats
EF.C.CH.ENC (X.509-ENC-Zertifikat)	'C200' /2	transparent	1536 Byte oder Länge des Zertifikats
EF.C.CH.ENCV (X.509-ENC-Pseudonym-Zertifikat für eRezepte)	'C50A' /10	transparent	1536 Byte oder Länge des Zertifikats
EF.DM (Display Message)	'D004' /4	transparent	8 Byte

B.4.2 Zugriffsregeln in DF.ESIGN

Hinweise:

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
6	Damit Rolle CHA.6 im DF.HCA Aktionen ausführen kann ist es notwendig einen Trusted Channel aufzubauen. Dies ist in der folgenden Tabelle nicht extra ausgewiesen
CAMS	Rolle des CAMS repräsentiert durch den Schlüssel SK.CAMS
VSCA	Rolle des VSDD/CAMS repräsentiert durch den Schlüssel SK.VSDDCAMS
VSDD	Rolle des VSDD repräsentiert durch den Schlüssel SK.VSDD
R, Read	Recht zu lesen und in strukturierten Dateien zu suchen (SEARCH RECORD)
U, Update	Recht zu Schreiben und zu Überschreiben (= Löschen von Information)
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
E, PSO DEC	PSO Decipher, Recht von der eGK Daten entschlüsseln zu lassen

Tabelle B. 8 Zugriffsrechtematrix

Object	ALW	home	1	1+CH	2	2+CH	8	8+CH	3	3+CH	9	9+CH	6	6+CH	4	4+CH	10	10+CH	5	5+CH	7	7+CH	CAMS	VSCA	VSDD
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	R	R	RU	RU	R
PrK.CH.AUT		IS		IS		IS		IS		IS		IS		IS		IS		IS		IS					
PrK.CH.ENC		E		E		E		E		E		E		E		E		E		E					
EF.C.CH.AUTN EF.C.CH.ENCV		R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R			RU	RU	
PrK.CH.AUTN		IS		IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS	IS					
PrK.CH.ENCV		E		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E					
EF.DM		U											R	R									R	R	R

Die obige Tabelle stellt die Zugriffsrechte übersichtlich, einfach und kompakt dar. Die folgende Tabelle zeigt die Zugriffsrechte detailliert aus **technischer** Sicht. Die Zugriffsregeln DÜRFEN NICHT veränderbar sein.

Tabelle B. 9 – Zugriffsregeln in DF.ESIGN

Objekt	Zugriffsart	Zugriffsbedingung
DF.ESIGN	CREATE EF	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.C.CH.AUT und EF.C.CH.ENC	READ BINARY	Always
	UPDATE BINARY	TC_ENC_MAC(SK.CAMS) AND TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
PrK.CH.AUT in SE #01	GENERATE ASYM-METRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH) OR (CHA.5 AND PIN.CH) OR (CHA.8 AND PIN.CH) OR (CHA.9 AND PIN.CH) OR (CHA.10 AND PIN.CH)
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH) OR (CHA.5 AND PIN.CH) OR (CHA.8 AND PIN.CH) OR (CHA.9 AND PIN.CH) OR (CHA.10 AND PIN.CH)
	PSO Decipher	Never
	Andere Kommandos	Never
PrK.CH.AUT in SE #02	GENERATE ASYM-METRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	PIN.CH AND TC_ENC_MAC(CHA.6)
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	PIN.CH AND TC_ENC_MAC(CHA.6)
	PSO Decipher	Never
	Andere Kommandos	Never
PrK.CH.ENC in SE #01	GENERATE ASYM-METRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Never
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	Never

	PSO Decipher	PIN.home OR (CHA.1 AND PIN.CH) OR (CHA.2 AND PIN.CH) OR (CHA.3 AND PIN.CH) OR (CHA.4 AND PIN.CH) OR (CHA.5 AND PIN.CH) OR (CHA.8 AND PIN.CH) OR (CHA.9 AND PIN.CH) OR (CHA.10 AND PIN.CH)
	Andere Kommandos	Never
PrK.CH.ENC in SE #02	GENERATE ASYM-METRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Never
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	Never
	PSO Decipher	PIN.CH AND TC_ENC_MAC(CHA.6)
	Andere Kommandos	Never
EF.C.CH.AUTN und EF.C.CH.ENCV in SE #01	READ BINARY	PIN.home OR (CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.8 OR CHA.9 OR CHA.10 OR TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	UPDATE BINARY	TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDDCAMS)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
EF.C.CH.AUTN und EF.C.CH.ENCV in SE #02	READ BINARY	TC_ENC_MAC(CHA.6)
	UPDATE BINARY	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never
PrK.CH.AUTN in SE #01	GENERATE ASYM-METRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	PIN.home OR (CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.8 OR CHA.9 OR CHA.10
	EXTERNAL AUTH.	Never

	PSO Compute Digital Signature	PIN.home OR (CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.8 OR CHA.9 OR CHA.10
	PSO Decipher	Never
	Andere Kommandos	Never
PrK.CH.AUTN in SE #02	GENERATE ASYMMETRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	TC_ENC_MAC(CHA.6)
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	TC_ENC_MAC(CHA.6)
	PSO Decipher	Never
	Andere Kommandos	Never
PrK.CH.ENCV in SE #01	GENERATE ASYMMETRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Never
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	Never
	PSO Decipher	PIN.home OR (CHA.1 AND PIN.CH) OR CHA.2 OR CHA.3 OR CHA.4 OR CHA.5 OR CHA.8 OR CHA.9 OR CHA.10
	Andere Kommandos	Never
PrK.CH.ENCV in SE #02	GENERATE ASYMMETRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Never
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	Never
	PSO Decipher	TC_ENC_MAC(CHA.6)
	Andere Kommandos	Never
EF.DM	READ BINARY	TC_ENC_MAC(CHA.6) OR TC_ENC_MAC(SK.CAMS) OR TC_ENC_MAC(SK.VSDD) OR TC_ENC_MAC(SK.VSDDCAMS)
	UPDATE BINARY	PIN.home
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never

B.5 DF.CIA. ESIGN

B.5.1 EFs unter DF.CIA. ESIGN

Tabelle B. 10 – CIA. ESIGN-Dateien und ihre Eigenschaften

Datei	FID / SFID	Datei-struktur	Dateigröße (Datenlänge)
EF.CIAInfo (CIA Information)	'5032' /18	transparent	64 Byte

Anmerkung: FID / SFID entsprechen [ISO7816-15].

B.5.2 Zugriffsregeln in DF.CIA. ESIGN

Tabelle B. 11 – Zugriffsregeln in DF.CIA.ESIGN

Objekt	Zugriffsart	Zugriffsbedingung
EF.CIAInfo	READ BINARY	Always
	UPDATE BINARY	Never
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	DELETE FILE	Never
	Andere Kommandos	Never

B.6 DF.QES

B.6.1 EFs unter DF. QES

Tabelle B. 12 – DF.QES-Dateien und ihre Eigenschaften

Datei	FID / SFID	Datei-struktur	Dateigröße (Dateilänge)
EF.C.CH.QES (X.509-QES-Zertifikat)	'C000' /1	transpa-rent	1536 B oder Länge des Zertifikats

Als FID von EF.C.CH.QES ist gemäß [DIN66291-4] 'C000' zu verwenden.

B.6.2 Zugriffsregeln für DF.QES

Tabelle B. 13 – Zugriffsregeln in DF.QES

Objekt	Zugriffsart	Zugriffsbedingung
EF.C.CH.QES	READ BINARY	Always
	UPDATE BINARY	TC_ENC_MAC(SK.ZDA)
	ACTIVATE FILE	Never
	DEACTIVATE FILE	Never
	Andere Kommandos	Never
PrK.CH.QES	GENERATE ASYM-METRIC KEY PAIR	Nicht Gegenstand dieses Dokumentes
	INTERNAL AUTH.	Never
	EXTERNAL AUTH.	Never
	PSO Compute Digital Signature	PIN.QES_mit_SSEC=1
	PSO Decipher	Never
	Andere Kommandos	Never
PIN.QES	CHANGE REFERENCE DATA und P1='00'	Always
	RESET RETRY COUNTER und P1='01'	Always
	VERIFY	Always
	Andere Kommandos	Never

Die Zugriffsregeln DÜRFEN NICHT veränderbar sein.

Anhang C
(normativ)
Datei-Inhalte
(bei der Initialisierung/Personalisierung zu laden)

C.1 EFs auf MF-Ebene

C.1.1 EF.ATR

Tabelle C. 1 – DOs in EF.ATR

Tag	Länge	Wert	Bemerkung
'E0'	'xx'	'02'-L-'xxxx' || '02'-L-'xxxx' || '02'-L-'xxxx' || '02' -L-'xxxx'	Puffer-Größen, siehe [gemSpec_eGK_P1]
'66'	'xx'	'46 xx …'	DO Card Data (DO Pre-issuing data, siehe Tabelle 125)

C.1.2 EF.DIR (Directory File)

Tabelle C. 2 – Anwendungs-Templates in EF.DIR

Rec -Nr.	Tag	L	Anwendungs-Templates	Bemerkung
1	'61'	'08'	'4F 06 D276000001 02'	HCA - siehe Anmerkungen 1 und 2
2	'61'	'0C'	'4F 0A A000000167 455349474E'	ESIGN - siehe Anmerkung 3
3	'61'	'11'	'4F 0F E828BD080F A000000167 455349474E'	CIA.ESIGN - siehe Anmerkung 4
4	'61'	'08'	'4F 06 D276000066 01'	QES - siehe Anmerkung 5

Anmerkungen:

1. Der RID 'D276000001' wurde für das deutsche Gesundheitswesen zur Verwendung in Versichertenkarten festgelegt.
2. Zukünftig könnte DF.HCA einen zweiten AID bekommen, welcher sich auf die europäische Krankenversichertenkarte (EHIC) bezieht.
3. Die ESIGN-Anwendung hat einen internationalen AID, der in [CWA14890-1] definiert ist.
4. DF.CIA hat einen RID gemäß [ISO7816-15]. An den RID schließt sich der erste Teil des AIDs derjenigen Anwendung an, zu welcher die CIOs gehören.
5. Die AID für QES (DINSIG) ist in [DIN66291-4] spezifiziert.

C.1.3 EF.GDO (Datei für globale Datenobjekte)

Tabelle C. 3 – DO ICCSN

Tag	Länge	Wert	Bemerkung
'5A'	'0A'	'80276xx….'	Der Sinngehalt der Struktur ist in Abbildung 3 dargestellt. Die Kennnummer des Kartenherausgebers (IIN) und die serielle Kartennummer (SN) müssen während der Personalisierung eingetragen werden.

C.1.4 EF.CVC.CA_eGK.AUT und EF.CVC.eGK.AUT (Dateien für CV-Zertifikate)

Der Inhalt dieser Dateien ist in [gemSpec_eGK_P1] beschrieben.

C.2 EFs unter DF.HCA

C.2.1 EF.DM

In diese Datei wird ein Random 8 Byte-String (8 alphanumerische ASCII-Zeichen) eingetragen.

C.2.2 EF.PD, EF.VD und EF.GVD

Der Inhalt dieser EFs wird in einem gesonderten Dokument beschrieben.

C.2.3 EF.eRezept_Tickets und EF.Verweis

Alle Records sind anzulegen und mit dem in [gemeGK_Fach] beschriebenen Initialwert vorzubelegen (= leere Records).

C.2.4 EF.Logging

Alle Records sind anzulegen und mit dem in [gemeGK_Fach] beschriebenen Initialwert vorzubelegen (= leere Records).

C.2.5 EF.StatusVD

In diese Datei wird ein Start-Datenstring eingetragen, der die Statusdaten für den bei Ausgabe der eGK geschriebenen Datensatz enthält. Der Inhalt dieses Start-Datenstrings wird in einem gesonderten Dokument [gemFA_VSDM] beschrieben.

C.2.6 EF.Status.Rezept, EF.Status.Notfalldaten

In diese Dateien wird ein Start-Datenstring eingetragen. Der Inhalt der Start-Datenstrings besteht aus Null-Bytes.

C. 2.7 EF.Notfalldaten

In diese Datei wird ein mit Platzhaltern vorstrukturierter Datensatz eingetragen. Der Inhalt dieses Datensatzes wird in einem gesonderten Dokument [gemFA_NFDM] beschrieben.

C.2.8 EF.eRezept

In diese Datei wird ein Start-Datenstring eingetragen. Der Inhalt des Start-Datenstrings besteht aus Null-Bytes.

C.3 EFs unter DF.ESIGN

C.3.1 EF.C.CH.ENC, EF.C.ENCV, EF.C.AUT und EF.C.CH.AUTN

In diese Dateien sind die X.509-Zertifikate abzulegen (Kodierung nicht Bestandteil dieser Spezifikation, siehe [gemX.509_eGK]).

C.3.2 EF.DM

In diese Datei wird ein Random 8 Byte-String eingetragen (derselbe Inhalt wie in EF.DM unter DF.HCA).

C.3.3 EFs unter DF.QES

Die Inhalte der Dateien sind mit den ZDAs abzustimmen.

C.4 EFs unter DF. CIA.ESIGN

C.4.1 EF.CIAInfo

Tabelle C. 4 – Inhalt von EF.CIAInfo

Tag	Länge	Wert	Bemerkung
‘30’	‘15’	‘02 0101 03 0100 A60D 0C 0B 44 49 4E 20 56 20 36 36 32 39 31’	Die CIA-Information enthält die Versionsangabe der CIO-Beschreibung und die Kennung des referenzierten Profils / Signaturkartenstandards DIN V 66291. "cardflags" bleibt frei (erforderlich).

ASN.1 Werte-Notation

```
1       ciaInfoExample CardInfo ::= {
2               version v2,
3               cardflags {     },
4               profileIndication {
5                       "DIN V 66291"
                        }
        }
```

ASN.1 Beschreibung, Tags, Längen und Werte

```
1    CiaInfo SEQUENCE: tag = [UNIVERSAL 48] constructed; length = 21
2      version INTEGER: tag = [UNIVERSAL 2] primitive; length = 1
         1
3      cardflags CardFlags BIT STRING: tag = [UNIVERSAL 3] primitive; length
= 1
         0x00
4      profileIndication SEQUENCE OF : tag = [UNIVERSAL 166] constructed;
length = 13
5        profileName UTF8String : tag = [UNIVERSAL 12] primitive; length =
11
           0x44494E2056203636323931
```

Hexadezimale DER-Kodierung

```
1    30 15
2          02 01
                 01
3          03 01
                 00
4          A6 0D
5                0C 0B
                       44 49 4E 20 56 20 36 36 32 39 31
```

Anhang D
(normativ)
Kennungen der Kartenherausgeber, CAs und CHA-Werte

D.1 Kennungen der Kartenherausgeber

Die Kennung eines Kartenherausgebers (issuer identifier) erlaubt in Verbindung mit dem Ländercode eine weltweit eindeutige Identifizierung des Kartenherausgebers. Der in BCD kodierte Ländercode hat für Deutschland den Wert '276' gemäß [ISO 3166]. Die Kennung des Kartenherausgebers ("Kartenausgeberschlüssel" entsprechend DIN EN 1867, siehe [EN 1867]) wird in Deutschland im Auftrag des DIN durch GS1 Germany GmbH, Köln (www.gs1-germany.de) vergeben. Der Kartenherausgeber ist gewöhnlich der rechtmäßige Besitzer der ausgegebenen Karte.

Die Kennung des Kartenherausgebers ist Teil der ICCSN (Integrated Circuit Card Serial Number, siehe [Resolution190]), welche die weltweit eindeutige Identifizierung der jeweiligen Karte erlaubt. Für Karten im Gesundheitswesen wird eine solche Kennung im Europäischen Standard [EN 1867] vorgeschrieben. In diesem Standard ist zudem der so genannte Major Industry Identifier (MII) für Kartenherausgeber im Gesundheitsbereich spezifiziert, welcher den Wert '80' hat.

Die ICCSN (siehe Abbildung 2) oder Teile daraus werden technisch eingesetzt, z.B. für

- Identifizierung von Karten
- karten-individuelle Schlüsselableitung
- Schlüsselidentifizierung (z.B. der öffentliche Schlüssel in einem CV-Zertifikat)
- Bildung von Authentisierungsdaten.

Die folgende Tabelle zeigt die grundsätzliche Struktur einer Issuer Identification Number IIN in einer eGK.

Tabelle D. 1 - Issuer Identification Number

MII für Gesundheitswesen	Country Code Germany	Issuer Identifier , z.B. für - eine bestimmte Krankenversicherung - einen Verband von Krankenversicherungen (VDAK, …)
'80'	'276'	... (5 BCD)

D.2 Certification Authorities

Der Name einer deutschen CA beginnt mit DE und muss registriert sein. Fraunhofer SIT fungiert als vom DIN autorisierte Registration Authority. Bisherige vergebene Kennungen und das Antragsformular sind zu finden über www.sit.fraunhofer.de.

D.3 CHA und Profilkennungen

Eine Profilkennung ist ein 1-Byte großes Feld in der Certificate Holder Authorization (CHA) eines CV-Zertifikats und wird in asymmetrischen Card-to-Card-Authentisierungsverfahren verwendet. Eine CHA spielt mit ihrer Profilkennung eine wesentliche Rolle hinsichtlich des Zugriffs auf Daten in einer elektronischen Gesundheitskarte (eGK). Eine Profilkennung mit dem Wert '00' bedeutet, dass die betreffende Instanz kein Zugriffsrecht hat.

Wenn verschiedene Berufsgruppen dieselben Zugriffsrechte gegenüber der eGK haben, dann gehören sie zum selben Profil. Dieses führt zu einer Reduzierung der verschiedenen Zugriffsbedingungen in der eGK. Die Zuordnung von Berufsgruppen zu einem bestimmten Profil ist nicht Gegenstand dieser Spezifikation.

Das Konzept der Rollen- und Profilkennungen findet auch in anderen Kontexten (Fahrtenschreiber, ID-Cards, ...) zunehmend Verwendung. Daher ist es wichtig, dass der Anwendungskontext von Profilkennungen klar unterschieden werden kann. Zu diesem Zweck ist der Profilkennung ein Präfix vorangestellt, welcher Folgendes kennzeichnet:

- den Anwendungskontext, durch einen Application Identifier (AID) oder einem Teil daraus angegeben oder
- die betreffende Instanz, welche für die Vergabe der Rollenkennungen zuständig ist.

Die. Profil-Identifier, die in Zugriffsregeln der eGK verwendet werden, sind in Tabelle B. 7 zu finden.

Die CHA für elektronische Gesundheitskarten (eGK) ist in Tabelle D.2 dargestellt.

Tabelle D. 2 - CHA für die elektronische Gesundheitskarte (eGK)

CHA-Präfix	CHA- Rollenkennung	CV-Zertifikatsinhaber
‘D27600000100’	‘00’	eGK-Inhaber

Die CHA für CVCs, die von der Root-CA für CAs der Krankenversicherungen ausgegeben werden, zeigt Tabelle D.3. Für Cross-CV-Zertifikate, die - falls nötig - von der Root-CA herausgegeben werden, gilt ebenfalls Tabelle D.3.

Tabelle D. 3 - CHA für CVC.CA_NN_eGK.CS

CHA-Präfix	CHA- Rollenkennung	CV-Zertifikatsinhaber
DEZGW (5 B) || ‘00’	‘00’	Certification Authority (CA)

Anhang E
(normativ)
Generieren des QES-Schlüsselpaares

E.1 Schlüsselgenerierung in der eGK

Wurde in den Card Capabilities angezeigt, dass die eGK das QES-Schlüsselpaar generieren kann und dieser Vorgang noch auszuführen ist (gilt nur bei CVC als Sicherheitsanker), dann wird zunächst mit dem MSE-Kommando der zu generierende Schlüssel referenziert, für den schon eine Key-Beschreibung in der eGK angelegt sein muss (u.a. Algorithmus, Schlüssellänge, Exponent entsprechend [ALGCAT]).

Tabelle E. 1: MSE Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET für Berechnung einer digitalen Signatur
P2	‘B6’ = DST
Lc	‘03’ = Länge des nachfolgenden Datenfeldes
Datenfeld	‘84 01 84' = DO für KeyRef von PrK.CH.QES, siehe Tabelle 91
Le	Nicht vorhanden

Tabelle E. 2: MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	‘9000’ oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Dann folgt das GENERATE ASYMMETRIC KEY PAIR Kommando. Der Public Key wird in der in [ISO7816-8] beschriebenen Form auf der Basis einer implizit vorhandenen Headerliste zurückgegeben.

Tabelle E. 3 -GENERATE ASYMMETRIC KEY PAIR Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	‘46’ = GENERATE ASYMMETRIC KEY PAIR
P1	‘82’ = Schlüssel generieren und Antwort entsprechend Tabelle E.4
P2	‘00’
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'00' bzw. '0000'

Tabelle E. 4: GENERATE ASYMMETRIC KEY PAIR Antwort

Datenfeld	'7F49' -L-('81'-L-'xx…xx' || '82'-L-'xx…xx') = DO Public Key Data Objects (DO Modulus || DO Public Exponent)
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Anhang F
(normativ)
Aktivieren der QES-Anwendung

F.1 Allgemeine Verfahren

Es wird hinsichtlich des „Sicherheitsankers“ unterschieden zwischen

- CVC-Verfahren und
- Gütesiegel-Verfahren.

Beide Verfahren beginnen mit folgenden Schritten:

- Auslesen der ICCSN
- Selektion der QES-Anwendung
- Lesen der anwendungspezifischen Daten für die QES-Komplettierung.

Es 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.

F.1.1 Lesen von EF.GDO

Für den Komplettierungsprozess ist die ICCSN wichtig. Daher ist EF.GDO zu lesen.

F.1.2 QES-Anwendungsselektion

Die QES-Anwendungsselektion erfolgt wie in Kapitel 6.4 beschrieben.

F.1.3 Lesen von EF.ASD

Nach der Anwendungsselektion wird zunächst das EF.ASD gelesen, das Informationen für die QES-Komplettierung bereitstellt. Zum Lesen von EF.ASD wird das READ BINARY-Kommando verwendet.

In EF.ASD wird das DO "Anwendungsspezifische Daten" (Tag '6E', siehe

Tabelle F. 1) abgelegt.

Es enthält die folgenden Informationen:

- die ZDA-Kennung der ZDA-VP
- eine Kennzeichnung für das verwendete PIN- und PuK-Verfahren
- eine ID des Kartentyps mit evaluierter und bestätigter QES-Funktion

Tabelle F. 1: Aufbau des DO "Anwendungsspezifische Daten"

Tag	Länge	Wert	Bedeutung
'6E'	'09'	siehe Tabelle F.2	Anwendungsbezogene Daten

Tabelle F. 2: Kodierung der Daten im Wertefeld von DO "Anwendungsspezifische Daten"

Byte	Länge	Wert	Bedeutung
1-5	5	…	ZDA-Kennung der ZDA-VP, siehe Tabelle F.3
6-7	2	'XX XX'	Komplettierungs-Indikator, siehe Tabelle F.4
8-9	2	'XX XX'	ID des Kartentyps mit evaluierter und bestätigter QES-Funktion (vom ZDA-VP festzulegen)

Tabelle F. 3: ZDA-Kennungen für DO "Anwendungsspezifische Daten" und CVCs (derzeitiger Stand)

ZDA	ZDA-Kennung
Root_ZDA	DEZDA (noch zu beantragen)
Deutsche Post Com (Signtrust)	DEDPS
DSV	DEDSV
D-Trust	DEDTR
T-Systems	DETSC

Anmerkung:

ZDA-Kennungen werden zentral registriert, siehe :
www.sit.fraunhofer.de/cms/de/forschungsbereiche/sde/rid_sde/RID_Ueberblick.php

Tabelle F. 4: Komplettierungs-Indikator (1. Byte)

b8 b7 b6 b5 b4 b3 b2 b1	**Bedeutung**
x x x x - - - -	SM-Verfahren
0 0 0 0	Keine Angabe
0 0 1	Sym. AUT-Verfahren mit SM-Schlüsselvereinbarung ([gemSpec_eGK_P1], E.4)
0 1 1	Asym. AUT-Verfahren ([gemSpec_eGK_P1], E.3) mit kartenglobalen CVC *
1 0 0	Asym. AUT-Verfahren ([gemSpec_eGK_P1], E.3) mit anw.spez. CVC u. globalen Keys *
1 0 1	Asym. AUT-Verfahren ([gemSpec_eGK_P1]), E.3) mit anw.spez. CVC u. anw.spez. Keys *
	Andere Kodierungen reserviert (Defaultwert 0)

b8 b7 b6 b5 b4 b3 b2 b1	**Bedeutung**
- - - x x x x	Komplettierungsverfahren
0 0	Gütesiegel
0 1	Auslesen PuK mit GENERATE ASYM. KEY PAIR
1 0	Schlüssel generieren und Auslesen PuK mit GEN. ASYM. KEY PAIR
	Andere Kodierungen reserviert (Defaultwert 0)

** Anmerkung*

In diesem Fall müssen die CV-Schlüssel und Zertifikate sowohl den Anforderungen der Bundesnetzagentur bzw. SigG/SigV für das Nachladen als auch den Anforderungen der gematik für das Gesundheitswesen genügen.

Tabelle F. 5 - Komplettierungs-Indikator (2. Byte)

b8 b7 b6 b5 b4 b3 b2 b1	Bedeutung
x x x x - - - -	PIN-Verfahren
0 0	NULL-PIN-Verfahren (PIN-Aktivierung abhängig von ZDA-Kartentyp-ID)
0 1	Transport PIN (Zufallszahl)
1 0	Transport PIN (abgeleitet)
1 1	Transport PIN (leer)
	Andere Kodierungen reserviert (Defaultwert 0)
- - - - x x x x	PUK-Verfahren
0 0	Keine PUK
0 1	8-stellige PUK (Zufallszahl)
1 0	8-stellige PUK (abgeleitet)
	Andere Kodierungen reserviert (Defaultwert 0)

Das EF.ASD darf immer gelesen werden. Es darf nicht überschrieben werden können. Die Zugriffsregeln befinden sich in Record 1 des EF.ARR im DF.QES.

F.1.4 PIN/PUK-Handhabung

F.1.4.1 NULL-PIN-Verfahren

Beim NULL-PIN-Verfahren muss das PIN-Objekt bei eGK-Auslieferung im Zustand „deactivated“ sein, d.h. ein CHANGE RD-Kommando darf nicht ausgeführt werden. Nach Eintragung des QES-X.509-Zertifikats ist durch den ZDA-NL das PIN-Objekt in den Zustand „activated“ zu versetzen, so dass erst dann ein CHANGE RD-Kommando zum Setzen der PIN.QES ausgeführt werden kann. Dieses Verfahren muss betriebssystemspezifisch umgesetzt werden.

Wurde als PUK eine 8-stellige Zufallszahl gewählt, dann muss diese in die Datei EF.BVD (EF für BenutzerVerifikationsDaten) abgelegt werden, die nur von dem ZDA-NL auslesbar ist.

Wurde die PUK kryptografisch abgeleitet (Ableitungsverfahren siehe Kapitel 9.5.5.3), dann ist eine Ablage in EF.BVD nicht erforderlich, da ihr Wert in der Komplettierungsphase erneut berechnet werden kann, um z.B. einen PUK-Brief zu versenden.

Ein hersteller-spezifisches PUK-Handling zur PUK-Initialisierung ist im Prinzip auch möglich.

Im Rahmen der Evaluierung des QES-Nachladeprozesses müssen auch die PUK-Verfahren untersucht werden. Der ZDA-VP kann zusammen mit dem Kostenträger aus den bestätigten Verfahren auswählen.

Anmerkung: Das NULL-PIN-Verfahren ist patentrechtlich geschützt.

F.1.4.2 PIN/PUK-Ableitungsverfahren

Falls die Transport-PIN bzw. die PUK abgeleitet werden, dann ist das nachstehende Ableitungsverfahren zu verwenden.

F.1.2.2.1 Überblick über das Ableitungsverfahren

Zur Berechnung wird ein geheimer 16 Byte langer Masterkey MK herangezogen. Dieser wird vom ZDA-VP allen ZDA-NL zur Verfügung gestellt. Für die Berechnung der Transport-PIN wird ein anderer Masterkey als zur Berechnung der PUK verwandt.

Das Verfahren zur Ableitung unterteilt sich in drei Schritte und unterscheidet sich geringfügig, je nachdem, ob eine Transport PIN oder eine PUK berechnet wird:

- **Transport-PIN**
  - Erzeugung eines kartenindividuellen Datenblocks DBL_1.
  - Ableitung eines Zwischenwerts ZW_1 aus dem kartenindividuellen Datenblock DBL_1 und dem Masterkey MK.
  - Ableitung der Transport-PIN aus dem Zwischenwert ZW_1.
- **PUK**
  - Erzeugung von zwei kartenindividuellen Datenblöcken DBL_1 und DBL_2.
  - Ableitung von zwei Zwischenwerten ZW_1 und ZW_2 aus den kartenindividuellen Datenblöcken DBL_1 und DBL_2 und dem Masterkey MK.

- Ableitung der PUK aus den Zwischenwerten ZW_1 und ZW_2.

F.1.4.2.2 Erzeugung der kartenindividuellen Datenblöcke

Die kartenindividuellen Datenblöcke bestehen aus 12 Byte

- ICCSN aus dem CV-Zertifikat, Gütesiegel oder EF.GDO (10 Byte)
- ID der evaluierten und bestätigten Signaturkarte aus EF.ASD (2 Byte)

und sind wie folgt aufgebaut:

- DBL_1 = ICCSN | ID
- DBL_2 = ID | ICCSN

F.1.4.2.3 Ableitung der Zwischenwerte aus einem Masterkey

Zur Ableitung eines Zwischenwerts ZW aus einem kartenindividuellen Datenblock DBL und einem Masterkey MK wird der folgende Algorithmus verwendet:

Dabei wird für die Zwischenwerte ZW_1 bzw. ZW_2 der Datenblock DBL_1 bzw. DBL_2 verwandt.

Der 16 Byte lange Zwischenwert ZW (= ZW_1 oder ZW_2) wird aus den Daten

- MK (16 Byte)
- DBL (= DBL_1 oder DBL_2), Datenblock mit '00' auf eine Länge eines Vielfachen von 8 Byte gepaddet, wobei die Mindestlänge 16 Byte ist
- der öffentliche Initialwert

  I='52 52 52 52 52 52 52 52 25 25 25 25 25 25 25 25' (16 Byte)

berechnet als

- ZW = d*MK(H(I,DBL))

Hierbei ist

- d*MK die Triple-DES Entschlüsselung mit dem Schlüssel MK, wobei die beiden 8 Byte langen Blöcke H1 und H2 von H(I,DBL) = H1 | H2 separat entschlüsselt werden (ECB-Mode)
- H die in [ISO10118-2] definierte Hash-Funktion, die Werte X mit einer Länge, die ein Vielfaches von 8 Byte ist, mittels des Startwertes I (gemäß Anhang A von [ISO10118-2]) auf einen Wert von 16 Byte Länge abbildet. Es werden die um das Parity Adjustment P erweiterten Transformationen u (Ad10) und u' (Ad 01) aus Anhang A von [ISO10118-2] verwendet. H ist rekursiv definiert:
- Sei X = x1|...|xn die Zerlegung des Wertes X in 8 Byte lange Blöcke und L0|R0 die Zerlegung des vorgegebenen Startwerts I in zwei 8 Byte Blöcke.
- eK(X) ist die DES-Verschlüsselung eines 8 Byte Wertes mit einem 8 Byte Schlüssel.
- $\oplus$ sei die bitweise Addition modulo 2 (XOR).
- Die Transformationen Ad10 und Ad01 transformieren 8 Byte Werte K wie folgt:

  Sei K = $k_1,...,k_{64}$ die Darstellung von K als Folge von 64 Bit. Dann ist

$Ad10(K) = [P](k_1,1,0,k_4,...,k_{64})$

$Ad01(K) = [P](k_1,0,1,k_4,...,k_{64})$

[P]: Das Parity Adjustment in Ad10 und Ad01 ist optional. Wenn vor der DES-Verschlüsselung eK(X) keine Paritätsprüfung des Schlüssels K erfolgt, kann P entfallen.

- Dann errechnet sich $L_i|R_i$ aus $L_{i-1}|R_{i-1}$ und x_i wie folgt:

  L_{i-1} bestehe aus den Bits $l_1,...,l_{64}$ und R_{i-1} bestehe aus den Bits $r_1,...,r_{64}$,

  Schritt 1: $L'_i := Ad10(L_{i-1}) = [P](l_1,1,0,l_4,...,l_{64})$

  $R'_i := Ad01(R_{i-1}) = [P](r_1,0,1,r_4,...,r_{64})$

  Schritt 2: $A_i = A_{i[links]}|A_{i[rechts]} = eL'_i(x_i) \oplus x_i$.

  $B_i = B_{i[links]}|B_{i[rechts]} = eR'_i(x_i) \oplus x_i$.

  Schritt 3: $L_i = A_{i[links]}|B_{i[rechts]}$

  $R_i = B_{i[links]}|A_{i[rechts]}$

- $L_n|R_n$ ist dann der Hash-Wert von X unter H:

  $H(I,X) = L_n|R_n$

F1.4.2.4 Ableitung der Transport-PIN aus dem Zwischenwert ZW_1

Zur Ableitung der 5-stelligen Transport-PIN aus dem Zwischenwert ZW_1 wird der folgende Algorithmus benutzt:

Der Zwischenwert ZW_1 besteht aus 32 Halb-Bytes, die ihrerseits jeweils eine Ziffer zwischen 0 und 15 darstellen. In diesem Sinne besteht ZW_1 aus 32 Ziffern.

1. Setze n = Anzahl der Ziffern aus ZW_1, die im Bereich '0' – '9' liegen.
2. Falls n >= 5 gehe zu Schritt 7.
3. Suche von links nach rechts die erste Ziffer im Bereich 'A' - 'F'.
4. Falls n gerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '0', 'B' durch '1', ... und 'F' durch '5'.
5. Falls n ungerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '4', 'B' durch '5', ... und 'F' durch '9'.
6. Erhöhe n um eins und gehe zu Schritt 2.
7. Die Transport-PIN besteht aus der Konkatenation der ersten 5 Ziffern von links nach rechts in dem Bereich '0' – '9' von ZW_1.

Bemerkung: In dem Fall, dass es in den 32 Halb-Bytes keine fünf Ziffern im Bereich '0 – 9' gibt, werden die Ziffern '0 – 9' der Transport-PIN nicht exakt gleichverteilt. Dieser Fall kann aber vernachlässigt werden, da er nur mit der Wahrscheinlichkeit

$$\sum_{i=0}^{4}\binom{32}{i}\left(\frac{10}{16}\right)^{i}\left(\frac{6}{16}\right)^{32-i} \approx 7\cdot 10^{-9}$$

auftritt (Bernoulli-Experiment).

F1.4.2.5 Ableitung einer PUK aus den Zwischenwerten ZW_1 und ZW_2

Für die kryptographische Ableitung der 8-stelligen PUK wird ein eigener Masterkey verwendet, der vom ZDA-VP an den ZDA-NL zu übergeben ist.

Zur Ableitung der PUK werden aus den Zwischenwerten ZW_1 und ZW_2 jeweils eine Halb-PUK HP_1 und HP_2 von je vier Ziffern berechnet. Die beiden Halb-PUKs HP_1 und HP_2 werden dann zu der PUK zusammengefügt. Jede der Halb-PUKs wird analog zu der Ableitung der Transport-PIN berechnet.

Der Zwischenwert ZW_i (i = 1, 2) besteht aus 32 Halb-Bytes, die ihrerseits jeweils eine Ziffer zwischen 0 und 15 darstellen. In diesem Sinne besteht ZW_i aus 32 Ziffern.

1. Setze n = Anzahl der Ziffern aus K, die im Bereich '0' – '9' liegen.
2. Falls n >= 4 gehe zu Schritt 7.
3. Suche von links nach rechts die erste Ziffer im Bereich 'A' - 'F'.
4. Falls n gerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '0', 'B' durch '1', ... und 'F' durch '5'.
5. Falls n ungerade ist, ersetze die in Schritt 3 gefundene Ziffer gemäß folgender Abbildung: 'A' durch '4', 'B' durch '5', ... und 'F' durch '9'.
6. Erhöhe n um eins und gehe zu Schritt 2.
7. Die Halb-PUK HP_i (i = 1, 2) besteht aus der Konkatenation der ersten 4 Ziffern von links nach rechts in dem Bereich '0' – '9' von ZW_i.

Bemerkung: In dem Fall, dass es in den 32 Halb-Bytes keine vier Ziffern im Bereich '0 – 9' gibt, werden die Ziffern '0 – 9' der Transport-PIN nicht exakt gleichverteilt. Dieser Fall kann aber vernachlässigt werden, da er nur mit der Wahrscheinlichkeit

$$\sum_{i=0}^{3}\binom{32}{i}\left(\frac{10}{16}\right)^{i}\left(\frac{6}{16}\right)^{32-i} \approx 8\cdot 10^{-10}$$

auftritt (Bernoulli-Experiment).

Die PUK ergibt sich aus den beiden Halb-PUKs: PUK = HP_1 | HP_2.

Anmerkung:
Es wird vorausgesetzt, dass das beschriebene Verfahren nicht durch Patente geschützt ist.

F.1.5 Aktivieren mit CV-Zertifikaten als Sicherheitsanker

F.1.5.1 DF.QES

Abbildung 10 zeigt die QES-Dateistruktur für den Anwendungsfall der QES-Komplettierung mit anwendungsspezifischen CVCs.

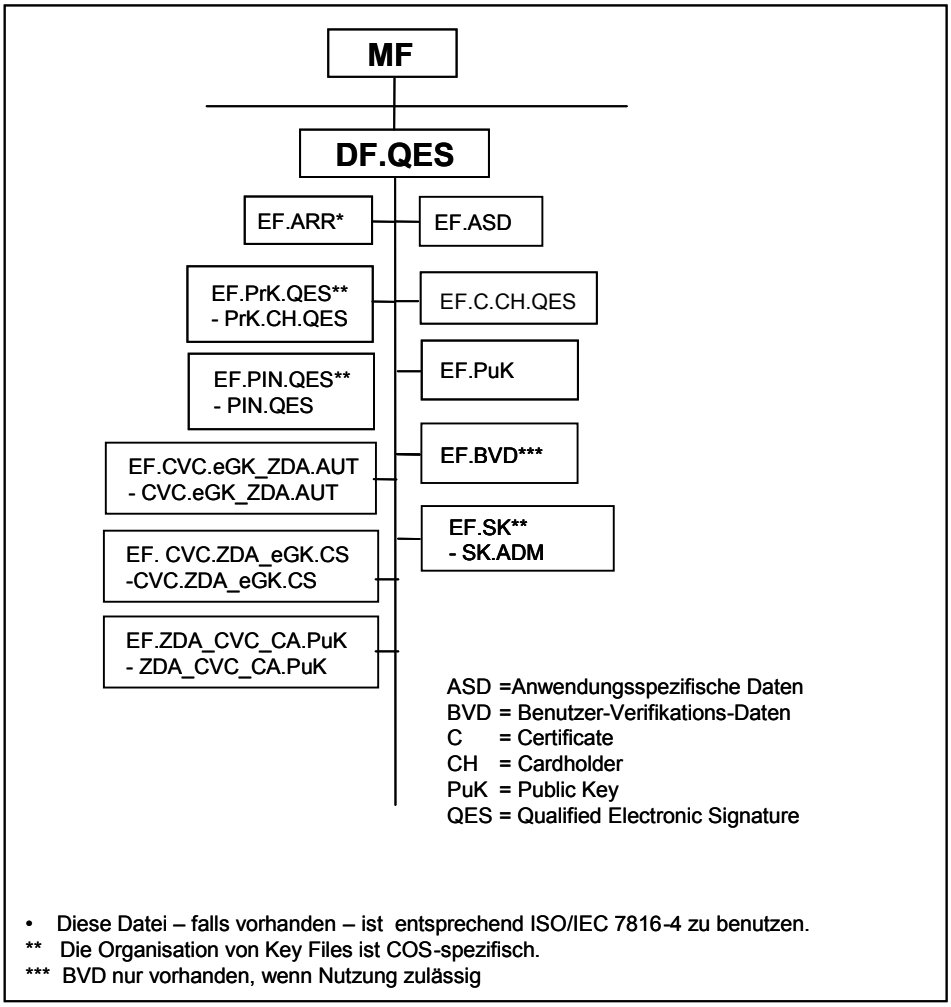

Abbildung 10 – Dateistruktur der Anwendung DF.QES bei Aktivierung mit CVC

F.1.5.1.1 EF.ARR

EF.ARR enthält die Zugriffregeln, siehe Kapitel F.1.3.5.6.

F.1.5.1.2 EF.PrK

EF.PrK ist für die Aufnahme von

- PrK.CH.QES (Konventionen: siehe Kapitel 6) und
- PrK.eGK.ZDA_AUT (falls anwendungsspezifisches Schlüsselpaar verwendet wird)

vorgesehen (Organisation von EF.PrK COS-spezifisch).

Tabelle F. 6: Schlüsselreferenzen

Name des Schlüssels	Key-ID
PrK.CH.QES	’84’
PrK.eGK.ZDA_AUT	’88’

F1.5.1.3 EF.SK

Für die gegenseitige Authentisierung mit TC Etablierung im Rahmen der Interaktion zwischen eGK und ZDA-NL wird ein 3DES-Schlüssel-Paar (3DES-Schlüssel für Verschlüsselung und MAC-Berechnung) bereitgestellt, siehe [gemSpec_eGK_P1], E.4.

Tabelle F. 7 - Referenzen auf geheime Schlüssel

Name des Schlüssels	KeyRef
SK.ADM.ENC / SK.ADM.MAC	'89'

Der Masterkey zur Ableitung des 3DES-Schlüsselpaars SK.ADM.ENC / SK.ADM.MAC muss vom ZDA-VP an die ZDA-NL übergeben werden.

F.1.5.1.3 EF.PIN, EF.C.CH.QES

Es gelten die Konventionen wie in Kapitel 6.

F.1.5.1.4 EF.CVC.ZDA_eGK.CS

In diesem EF wird das von dem Root-ZDA für einen ZDA-VP ausgestellte Zertifikat abgelegt.

F.1.5.1.5 EF.CVC.eGK.ZDA_AUT

In diesem EF wird das von dem ZDA-VP für die eGK ausgestellte CV-Zertifikat abgelegt.

F.1.5.1.6 EF.PuK

In EF.PuK wird der Public Key des Root-ZDA abgelegt. Die PuK-Referenz ist in EF.CVC.ZDA_eGK.CS angegeben (siehe [gemSpec_eGK_P1], Anhang B, Datenfeld CAR).

F.1.5.1.7 EF.BVD

Die transparente Datei EF.BVD enthält entweder

- 13 Bytes mit Wert '00', d.h. sie ist leer, oder
- 8 Ziffern (ASCII-codiert) als PUK und 5 Bytes mit Wert '00', oder
- 13 Ziffern (ASCII-codiert: PUK || 5-stellige Transport PIN).

Die Datei EF.BVD ist jedoch nur durch einen berechtigten ZDA lesbar, damit z.B. ein PIN/PUK-Brief zum Zeitpunkt der Komplettierung erstellt werden kann. Die Zugriffsbedingungen sind in Kapitel F.1.3.5.6, Record 3 dargestellt.

Anmerkung:
Die Bestätigungsfähigkeit dieses Verfahrens ist noch zu klären.

F.1.5.2 Spezifikation der CV-Zertifikate für das Nachladen

Für den in Abbildung 10 – Dateistruktur der Anwendung DF.QES bei Aktivierung mit CVC

dargestellten Anwendungsfall muss eine eigene CV-Hierarchie wie folgt aufgebaut werden.

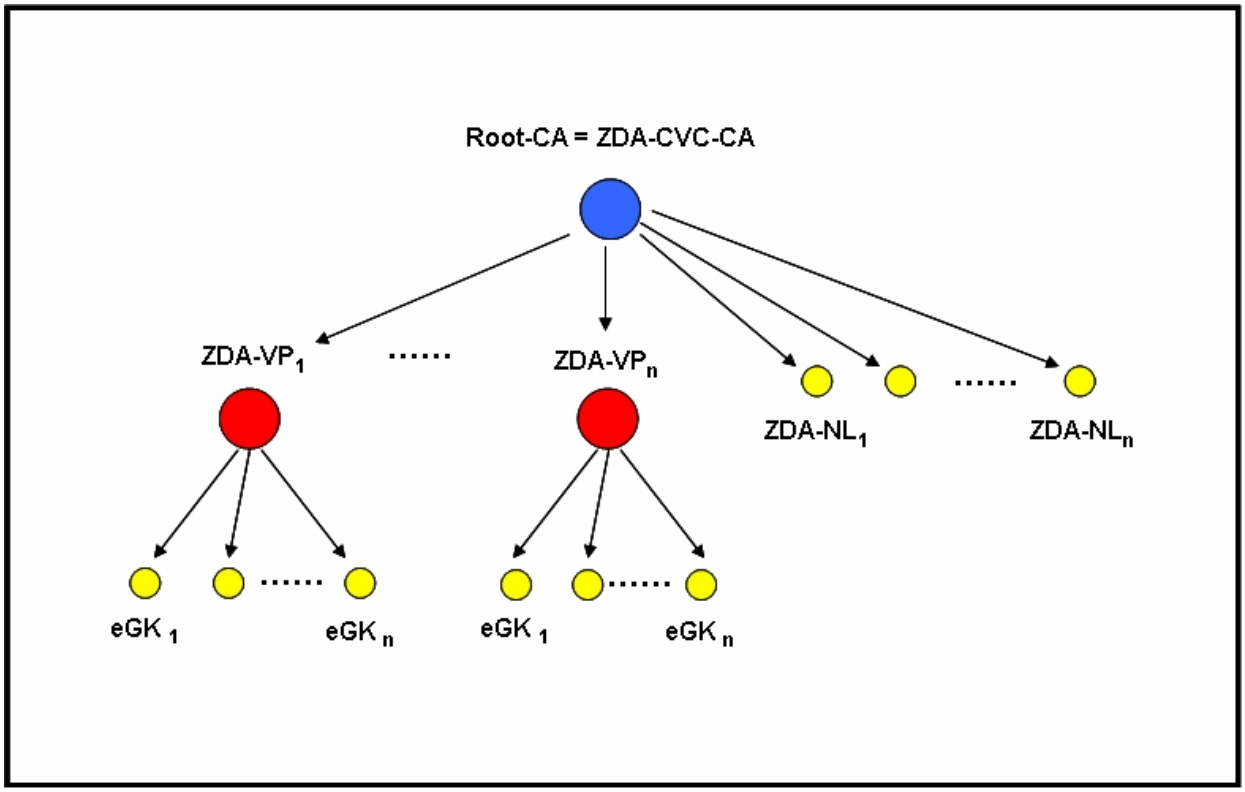

Abbildung 11 - Zertifikatshierarchie CVC für eGK

F.1.5.2.1 Aufbau und Inhalt der CV-Zertifikats-Files

EF.CVC.ZDA_eGK.CS wird für die Aufnahme des Root-CV-Zertifikats CVC.ZDA_eGK.CS genutzt. In EF.CVC.eGK.ZDA_AUT wird das eGK-CVC-Zertifikat abgelegt.

Struktur und Inhalt der Zertifikats-Dateien sind in [gemSpec_eGK_P1] beschrieben.

F.1.5.2.2 Aufbau und Inhalt des CV-Zertifikats CVC.eGK_ZDA.AUT

Die Schlüssellängen in den CV-Zertifikaten sowie der zu verwendende Hash-Algorithmus wurden entsprechend [gemSpec_eGK_P1] gewählt, d.h. es werden CVCs mit den CPI-Werten ’03’ und ’04’ unterstützt.

Anmerkung:
Die Verwendung anderer CVCs erfordert eine Änderung von [gemSpec_eGK_P1].

Aufbau und Inhalt des im Rahmen des Nachladens zu verwendenden CV-Zertifikats CVC.eGK_ZDA.AUT entsprechen der [gemSpec_eGK_P1] Anhang B Tabelle B.13. Hierbei gelten folgende Festlegungen:

Tabelle F.8: Aufbau bestimmter Felder eines CVC der eGK

Feld	Länge in Byte	Inhalt	Bemerkung
CPI	1	'04'	Profil-Kennung des CVC für eine eGK
CAR	8	5 Byte CA Name ||	Im CA-Namen muss die ZDA-Kennung des ZDA-VP stehen

		3 Byte Schlüsselreferenzierung	
CHR	12	2 Byte '00 00' || 10 Byte ICCSN	
CHA	7	'D2760000660100'	Keine Zugriffsrechte auf Daten in Zielkarten (CHA-Präfix = AID der QES-Anwendung, Rollen-Kennung ’00’)
OID	6	gemäß Anhang B [gemSpec_eGK_P1]	

F.1.5.2.3 Aufbau und Inhalt des CV-Zertifikats CVC.ZDA_NN.AUT

Aufbau und Inhalt des CV-Zertifikats CVC.ZDA_NN.AUT des HSM des ZDA-NL sind in [gemSpec_eGK_P1] in Anhang B Tabelle B. 11 beschrieben. Hierbei sind die folgenden Festlegungen zu treffen:

Tabelle F. 9: Aufbau bestimmter Felder eines CVC des ZDA-NL

Feld	Länge in Byte	Inhalt	Bemerkung
CPI	1	’04’	Profil-Kennung des CVC für ein HSM
CAR	8	5 Byte CA Name || 3 Byte Schlüsselreferenzierung	Im CA-Namen muss die ZDA-Kennung der ZDA-CVC-CA stehen
CHR	12	2 Byte '00 00' || 10 Byte IFD-SN	Eindeutige Seriennummer des Hardware-Sicherheitsmoduls
CHA	7	6 Byte Präfix "CSPQES" (ASCII-Codierung) 1 Byte Rollen-ID '01'	Zugriffsrecht des ZDA-NL auf bestimmte Daten in der eGK-Zielkarte gemäß Zugriffsregeln
OID	6	gemäß Anhang B [gemSpec_eGK_P1]	

Die Rollenkennung in dem CV-Zertifikat des HSM des ZDA-NL wird auf '01' festgelegt. Anhand dieser Rollen ID werden dem ZDA-NL von der Chipkarte die für ihn erforderlichen Zugriffsrechte auf die EFs im Verzeichnis der Signaturanwendung eingeräumt.

F.1.5.2.4 Aufbau und Inhalt des CV-Zertifikats CVC.CA_eGK.CS

Tabelle F. 10: Aufbau bestimmter Felder eines CVC der CA des ZDA-VP

Feld	Länge in Byte	Inhalt	Bemerkung
CPI	1	'03'	Profil-Kennung des CVC für eine CA
CAR	8	5 Byte CA Name || 3 Byte Schlüsselreferenzierung	Im CA-Namen muss die ZDA-Kennung der Root-CA, also der ZDA-CVC-CA stehen
CHR	12	4 Byte '00 00 00 00' || 5 Byte CA Name || 3 Byte Schlüsselreferenzierung	Im CA-Namen muss die ZDA-Kennung des ZDA-VP stehen, die Schlüsselreferenzierung ist gemäß Tabelle B.3 [gemSpec_eGK_P1] aufgebaut
CHA	7	6 Byte Präfix gemäß Tabelle B6 || 1 Byte Rollen-ID '00'	
OID	7	gemäß Anhang B [gemSpec_eGK_P1]	

F.1.5.3 C2S-Authentisierung mit CVC und Trusted Channel-Etablierung

Zunächst müssen die CV-Zertifikate, wie in Kapitel 3.2.15 beschrieben, ausgelesen werden. Hierbei werden dieselben SFIDs verwendet (prüfen).

Die Card-to-Server-Authentisierung (C2S-Authentisierung zwischen eGK und ZDA-NL) erfolgt wie in Kapitel 3.6 beschrieben. Hierbei sind jedoch die zur QES-Anwendung gehörenden Schlüsselreferenzen zu benutzen, d.h. entweder

- '88' für PrK.eGK.ZDA_AUT oder
- '10' für PrK.eGK.AUT

in Abhängigkeit von der Anzeige im DO „Anwendungsspezifische Daten".

F.1.5.4 Abholen des Public Keys mit dem GENERATE ASYMMETRIC KEY PAIR - Kommando

Wurde im DO „Anwendungspezifische Daten" das Auslesen des PuK.CH.QES mit dem GENERATE ASYMMETRIC KEY PAIR-Kommando angezeigt, dann ist das folgende Kommando zu senden:

Tabelle F. 11: GENERATE ASYMMETRIC KEY PAIR Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'46' = GENERATE ASYMMETRIC KEY PAIR
P1	'83' = Antwort Abholen entsprechend Headerliste
P2	'00'
Lc	Nicht vorhanden

Datenfeld	Nicht vorhanden
Le	'00' bzw. '0000'

Tabelle F. 12: GENERATE ASYMMETRIC KEY PAIR Antwort

Datenfeld	'7F49' -L-('81'-L-'xx…xx' || '82'-L-'xx…xx') = DO Public Key Data Objects (DO Modulus || DO Public Exponent)
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

F.1.5.5 QES-Zertifikatserstellung und -eintragung in die eGK

Der ZDA erstellt nun das X.509-QES-Zertifikat, das anschließend mit dem UPDATE BINARY-Kommando in die eGK eingetragen wird.

Tabelle F. 13: UPDATE BINARY Kommando

CLA	Wie in ISO/IEC 7816-4 definiert
INS	'D6' = UPDATE BINARY
P1	'81' = b8-b6: 100, b5-b1: 00001 SFID von EF.C.CH.QES: 1
P2	'00' = Offset
Lc	'xx' = Länge des nachfolgenden Datenfeldes
Datenfeld	Zertifikats-Daten
Le	Nicht vorhanden

Tabelle F. 14: UPDATE BINARY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Statusbytes, siehe [gemSpec_eGK_P1]

Das Kommando ist mit fortgeschriebenem Offset in P1-P2 (bit b8 in P1 = 0) zu wiederholen, bis das QES-X.509-Zertifikat komplett eingetragen ist.

F.1.5.5.1 Auslesen von EF.BVD

Zum Auslesen von EF.BVD wird das READ BINARY-Kommando verwendet.

F.1.5.5.2 NULL-PIN-Aktivierung

Wird das Komplettierungs-Verfahren in Verbindung mit dem NULL-PIN-Verfahren verwendet (siehe Anzeige im DO „Anwendungsspezifische Daten"), dann darf die NULL-PIN erst nach Komplettierung

auf die normale PIN.QES umstellbar sein. Konzeptionell ist hierzu des PIN-Life-Cycle-Status von „deactivated“ auf „activated“ zu setzen. Hierzu fehlen jedoch entsprechende Festlegungen in ISO/IEC 7816.

Es kann daher hier keine herstellerneutrale „PIN-Aktivierung“ dargestellt werden. Daher sind herstellerspezifische Lösungen zu verwenden. Welche herstellerspezifische Kommando-Sequenz hierfür zu verwenden ist (z.B. Nutzung des ACTIVATE FILE-Kommandos zum Setzen des PIN-Life Cycle Satus auf „activated“), ergibt sich aus der ZDA-Kartentyp-ID.

F.1.5.5.3 QES-Schlüsselgenerierung in der eGK

Für eGKs mit evaluiertem Schlüsselgenerator kann das QES-Schlüsselpaar „Just-in-Time“ auf der eGK erzeugt werden. Das Kommando hierfür ist in Anhang E beschrieben und ist dann anstelle des in Kapitel 9.5.8 dargestellten Kommandos zu senden. Anschließend erfolgt wie bei dem vorgenerierten QES-Schlüsselpaar die X.509-QES-Zertifikatserstellung und -eintragung.

F.1.5.5.4 Nutzung von Gütesiegeln

Im Prinzip ist eine Nutzung von Gütesiegeln auch bei dem CVC-Verfahren möglich.

F.1.5.5.5 EFs unter DF.QES

Tabelle F. 15: DF.QES-Dateien und ihre Eigenschaften

Datei	FID / SFID	Datei-struktur	Dateigröße (Dateilänge)	Zugriffsregel-Referenz
EF.ARR (Access Rule References)	FID COS-spezifisch	linear variabel	4 Records	Interner Zugriff und ARR #1
EF.C.CH.QES (X.509-QES-Zertifikat)	‘C000’ /1	trans-parent	1536 Byte oder Länge des Zertifikats	ARR #2
EF.ASD (Anwendungspezifische Daten)	‘D00A’ /10	trans-parent	11 Byte	ARR #1
EF.BVD (Benutzerverifikationsdaten)	‘D00B’ /11	trans-parent	13 Byte	ARR #3
EF.CVC.eGK.ZDA_AUT (anwendungsspezifisches CVC der eGK)	‘CC01’ /3	trans-parent	210 Byte	ARR #1
EF.CVC.ZDA_eGK.CS (CVC der ZDA-NL)	‘CC02’ /4	trans-parent	210 Byte	ARR #1

F.1.5.5.6 Zugriffsregeln

Tabelle F. 16: Inhalt von EF.ARR

Rec-Nr.	Wert	Bedeutung
1	’80 01 01 9000'	AM: READ RECORD/SEARCH RECORD SC: Always Referenziert in EF.ARR, EF.CVC.eGK.ZDA_AUT, EF. CVC.ZDA_eGK.CS und EF.ASD
2	’80 01 01 9000’ ’80 01 02 AF 14 A4 0D 950180 5F4C 07' CSPQES '01 B4 03 950130'	AM: READ BINARY/SEARCH BINARY SC: Always AM: UPDATE BINARY SC: AND Template {AT (UQ = Ext. Auth, CHA = “CSPQES” || ‘01’) || CCT (UQ = CC in SM-Kommando und SM-Antwort)} Referenziert in EF.C.CH.QES
3	'80 01 01 'AF 19 A4 0D 950180 5F4C 07 'CSPQES' 01 B4 03 950130 B8 03 950130' 'AF 12 A4 06 950180 83 01 89 B4 03 950130 B8 03 950130'	AM: READ BINARY SC: AND Template {AT (UQ = Ext. Auth, CHA = "CSPQES"||'01') || CCT (UQ = CC in SM-Kommando und SM-Antwort) || CT (UQ = CG in SM-Kommando und SM-Antwort)} SC: AND Template {AT (UQ = Ext. Auth, KeyRef='89') || CCT (UQ = CC in SM-Kommando und SM-Antwort) || CT (UQ = CG in SM-Kommando und SM-Antwort)} Referenziert in EF.BVD
4	‘86 02 2A9E A4 06 950108 830181’	AM: PSO: COMPUTE DS SC: AT (UQ = User authentication, Key Ref = PIN.QES) Die Zugriffsregel ist COS-spezifisch so zu erweitern, dass vor jeder Signaturberechnung die Präsentation von PIN.QES erforderlich ist. Referenziert bei PrK.CH.QES in EF.PrK
5	'86 06 2000 2400 2C01 9000’	AM: VERIFY, CHANGE RD (Option '00'), RESET RC (Option '01') SC: Always Referenziert bei PIN.QES in EF.PIN

Rec-Nr.	Wert	Bedeutung
6	'84 01 46 AF 12 A4 06 950180 83 01 89 B4 03 950130 B8 03 950130' AF 19 A4 0D 950180 5F4C 07 'CSPQES' 01 B4 03 950130 B8 03 950130'	AM: GENERATE ASYMMETRIC KEY PAIR SC: AND Template {AT (UQ = Ext. Auth, Key Ref = '89') ‖ CCT (UQ = CC in SM-Kommando und SM-Antwort) ‖ CT (UQ = CG in SM-Kommando und SM-Antwort)} SC: AND Template {AT (UQ = Ext. Auth, CHA = CHA.CSPQES) ‖ CCT (UQ = CC in SM-Kommando und SM-Antwort) ‖ CT (UQ = CG in SM-Kommando und SM-Antwort)} Referenziert bei Kommandos
7	'84 01 82 9000'	AM: MUTUAL AUTHENTICATE SC: Always Referenziert bei SK.ZDA in EF.SK, falls vorhanden
8	'84 02 88 82 9000'	AM: INTERNAL AUTHENTICATE SC: Always Referenziert bei PrK.eGK_ZDA.AUT
9	'87 03 2A 00 AE 9000'	AM: VERIFY CERTIFICATE SC: Always Referenziert bei PuK.ZDA_CVC_CA.CS

F.1.6 eGK mit Gütesiegel

F.1.6.1 Transportzustand eGK Sicherheitsanker GS

Im Folgenden werden für das Nachladen qualifizierter Zertifikate die Ergänzungen bzw. Festlegungen zu der eGK Spezifikation aufgeführt, wenn als Sicherheitsanker Gütesiegel benutzt werden.

F.1.6.2 Festlegungen für Dateien im DF.QES

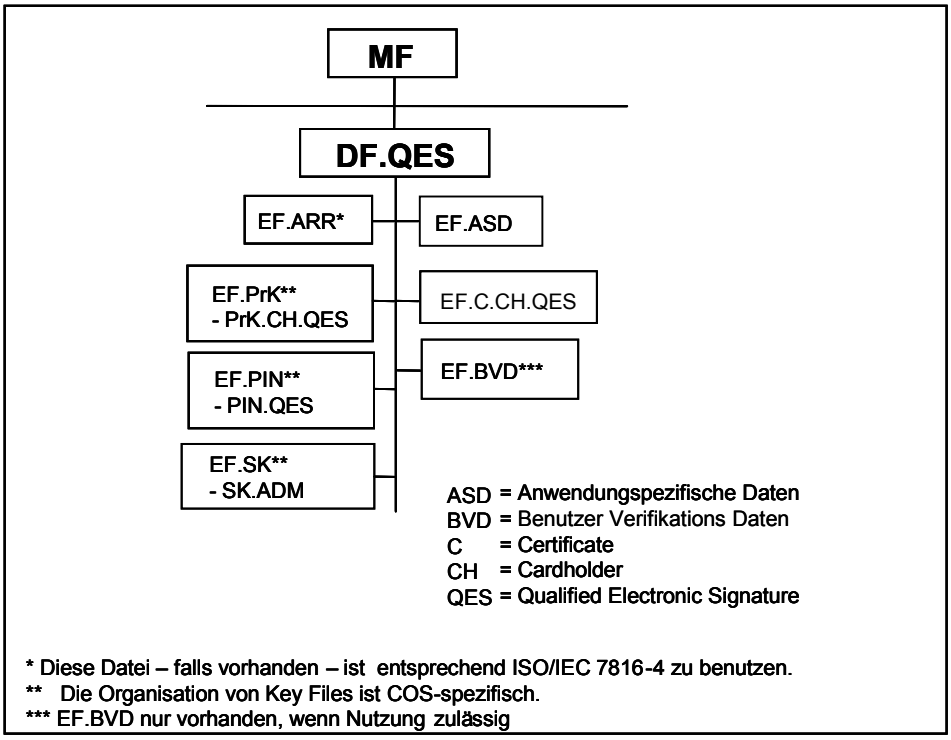

Abbildung 12 – Dateistruktur der Anwendung DF.QES bei Aktivierung mit Gütesiegel-Zertifikat

Die Datei-Struktur entspricht Abbildung 10 – Dateistruktur der Anwendung DF.QES bei Aktivierung mit CVC

, es gibt jedoch zusätzlich EF.SK. Soweit nicht anders beschrieben, gelten die Ausführungen bezüglich der Files wie oben.

F1.6.2.1 EF.PrK

In EF.PrK is bereits der private Signaturschlüssel PrK.CH.QES bei Auslieferung der eGK vorhanden.

F1.6.2.2 EF.SK

Für die gegenseitige Authentisierung mit TC Etablierung im Rahmen der Interaktion zwischen eGK und ZDA-NL wird ein 3DES-Schlüssel-Paar (3DES-Schlüssel für Verschlüsselung und MAC-Berechnung) bereitgestellt, siehe [gemSpec_eGK_P1], E.4.

Tabelle F. 17: Referenzen auf geheime Schlüssel

Name des Schlüssels	KeyRef
SK.ADM.ENC / SK.ADM.MAC	'89'

Der Masterkey zur Ableitung des 3DES-Schlüsselpaars SK.ADM.ENC / SK.ADM.MAC muss vom ZDA-VP an die ZDA-NL übergeben werden.

F1.6.2.3 EF.C.CH.QES

In diesem EF ist das Gütesiegel (spezielles X.509v3-Zertifikat) abgelegt, das den Signaturprüfschlüssel des Karteninhabers (d.h. PuK.CH.QES) enthält. Das Gütesiegel wird bei der QES-Komplettierung durch das QES-X.509-Zertifikat ersetzt.

F1.6.2.4 GS-Zertifikatshierarchie

Zur Ausstellung von Gütesiegel-Zertifikaten 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 GS abgelegt). Ein GS des ZDA X kann von jeder anderen für diesen Anwendungskontext zugelassenen ZDA Y geprüft werden.

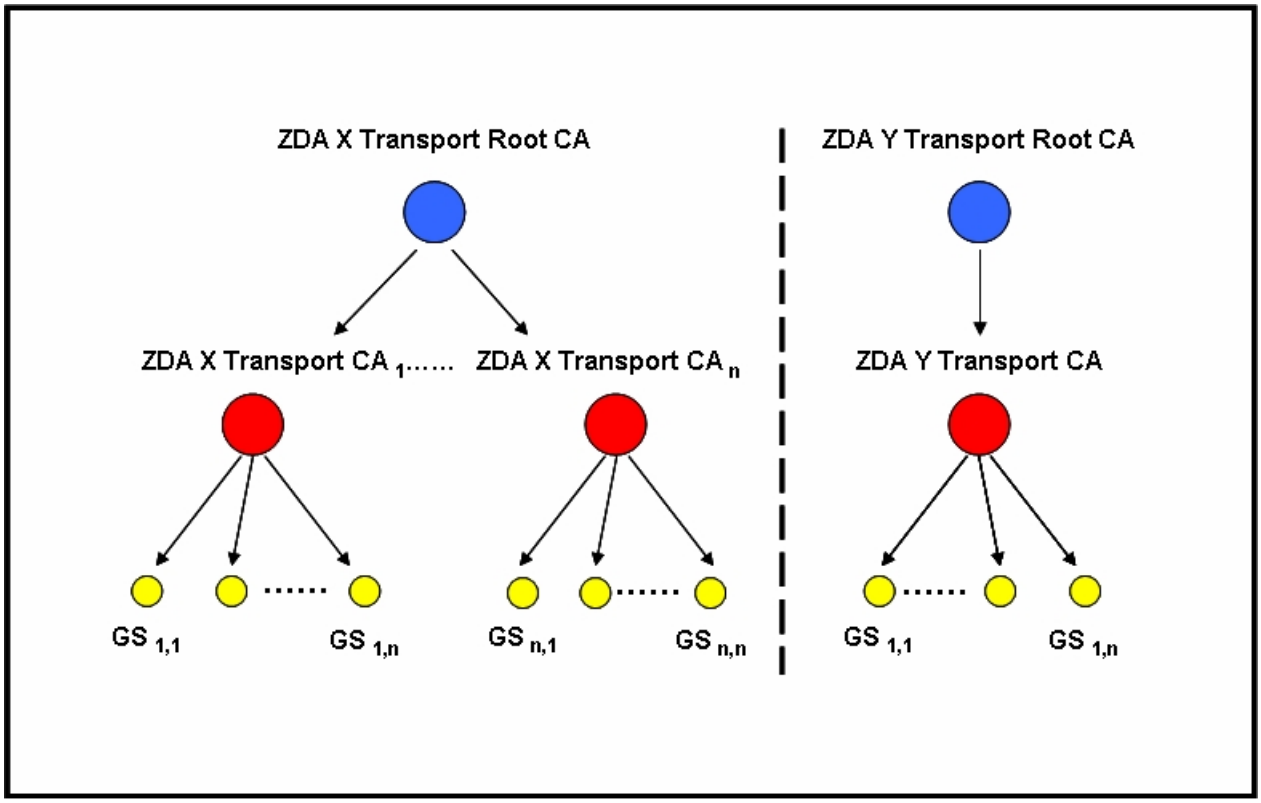

Abbildung 13 - Zertifikatshierarchie Gütesiegel-Zertifikate

Ein Transport-Signer bietet den Vorteil, dass ein einfaches Sperrmanagement von ganzen Mengen von GS möglich wird, indem ein solcher Signer ggf. ganz gesperrt werden kann. Ein solcher Transport-Signer kann z.B. auch im Auftrag eines ZDA bei einem Kartenproduzenten stehen und dann bei Missbrauch vollständig abgeschaltet werden.

Diese Struktur bietet den Vorteil, dass die gegenseitige Anerkennung verschiedener ZDAs flexibel gehandhabt werden kann. So kann z.B. ein ZDA anhand der Root eines anderen ZDAs die gesamte Transport-PKI-Hierarchie dieses ZDAs in sein Sicherheitskonzept integrieren, während ein weiterer ZDA ggf. 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.

F1.6.2.5 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-Gütesiegel-Zertifikaten handelt, müssen die "CommonNames" (CN) folgendem Schema folgen:

- Root-CA-Zertifikate: CN = [ZDA] Transport Root [Jahr]

  Bsp. "XY-ZDA Transport Root 05"

- CA-Zertifikate: CN = [ZDA] Transport Signer [Jahr]

  Bsp. "XY-ZDA Transport Signer 05"

Für die Gütesiegel-Zertifikate soll ein Zertifikatsprofil zu [X.509V3] mit folgenden Merkmalen verwendet werden:

Tabelle F. 18: X.509 Zertifikatsprofil 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>	

F.1.6.2.5.1 C2S-Authentisierung mit sym. Verfahren und TC-Etablierung

Falls in EF.ASD das symmetrische Authentisierungsverfahren mit dynamischer SM-Schlüsselvereinbarung angezeigt wurde, dann erfolgt die Card-to-Server-Authentisierung (C2S-Authentisierung zwischen eGK und ZDA-NL) wie in Kapitel 3.7. beschrieben unter Nutzung des in [gemSpec_eGK_P1] definierten Verfahrens. Hierbei ist jedoch die zur QES-Anwendung gehörende Schlüsselreferenz zu benutzen, d.h. ’89’ für SK.ADM.

Anmerkung: Ein statisches SM-Verfahren ist nicht in [gemSpec_eGK_P1] beschrieben und daher im Sinne der eGK-Spezifikation nicht spezifikationsgerecht.

F.1.6.2.5.2 Auslesen des Gütesiegels

Zum Lesen des Gütesiegels wird das READ BINARY-Kommando verwendet, siehe Kapitel 0 (FID/SFID: siehe Kapitel F.1.4.6).

F.1.6.3 QES-Zertifikatserstellung und -eintragung in die eGK

Das Schreiben des Zertifikats erfolgt wie in Kapitel F.1.3.5 beschrieben.

F.1.6.4 Auslesen von EF.BVD

Falls EF.BVD verwendet wird, sind die Daten mit dem READ BINARY-Kommando auszulesen.

F.1.6.5 NULL-PIN-Aktivierung

Die NULL-PIN-Aktivierung ist herstellerspezifisch, siehe Kapitel F.1.3.5.2.

F.1.6.6 EFs unter DF.QES

Tabelle F. 19: DF.QES-Dateien und ihre Eigenschaften

Datei	FID / SFID	Dateistruktur	Dateigröße (Dateilänge)	Zugriffsregel-Referenz
EF.ARR (Access Rule References)	FID COS-spezifisch	linear variabel	5 Records	Interner Zugriff und ARR #1
EF.C.CH.QES (X.509-QES-Zertifikat)	‘C000’ /1	transparent	1536 Byte oder Länge des Zertifikats	ARR #2
EF.ASD (Anwendungspezifische Daten)	‘D00A’ /10	transparent	11 Byte	ARR #1
EF.BVD (Benutzerverifikationsdaten)	‘D00B’ /11	transparent	13 Byte	ARR #3

Anmerkung: EF.BVD nur vorhanden, falls auch eine Nutzung gegeben.

F.1.6.7 Zugriffsregeln

Tabelle F. 20: Inhalt von EF.ARR

Rec-Nr.	Wert	Bedeutung
1	’80 01 01 9000'	AM: READ BINARY/READ RECORD/SEARCH BINARY/SEARCH RECORD SC: Always Referenziert in EF.ARR und EF.ASD
2	’80 01 01 9000’ ’80 01 02 AF 0C A4 06 950180 83 01 14 B4 03 950130'	AM: READ BINARY/SEARCH BINARY SC: Always AM: UPDATE BINARY SC: AND Template {AT (UQ = Ext. Auth, KeyRef = ‘89’) || CCT (UQ = CC in SM-Kommando und SM-Antwort)}

Rec -Nr.	Wert	Bedeutung
		Referenziert in EF.C.CH.QES Anmerkung: Die Zugriffsregel bezieht sich auf das in [gemSpec_eGK_P1] spezifizierte Verfahren mit dynamische SM-Schlüsselvereinbarung
3	’80 01 01 'AF 12 A4 06 950180 83 01 89 B4 03 950130 B8 03 950130'	AM: READ BINARY/SEARCH BINARY SC: AND Template {AT (UQ = Ext. Auth, KeyRef='89') || CCT (UQ = CC in SM-Kommando und SM-Antwort) || CT (UQ = CG in SM-Kommando und SM-Antwort)} Referenziert in EF.BVD
4	‘86 02 2A9E A4 06 950108 830181’	AM: PSO: COMPUTE DS SC: AT (UQ = User authentication, Key Ref = PIN.QES) Die Zugriffsregel ist COS-spezifisch so zu erweitern, dass vor jeder Signaturberechnung die Präsentation von PIN.QES erforderlich ist. Referenziert bei PrK.CH.QES in EF.PrK
5	'86 06 2000 2400 2C01 9000’	AM: VERIFY, CHANGE RD (Option '00'), RESET RC (Option '01') SC: Always (gilt bei NULL-PIN-Verfahren nur für den PIN-Life Cycle Status „activated“) Referenziert bei PIN.QES in EF.PIN Anmerkung: Beim NULL-PIN-Verfahren ist die Zugriffsregel hinsichtlich des Setzens des PIN-Life Cycle Status auf „activated“ zu erweitern.

Anhang G
(informativ)
eTickets und Abläufe mit eRezept- und MDO-Server

G.1 eTickets für eRezepte

Abb. G.1 zeigt den prinzipiellen Aufbau des eRezept-Ticket-Files mit bis zu 8 eTickets für eRezepte bei dem Transport über die eGK. Außerdem ist das eRezept-Container-File mit der Pointer-Struktur für die Speicherung der eRezepte dargestellt.

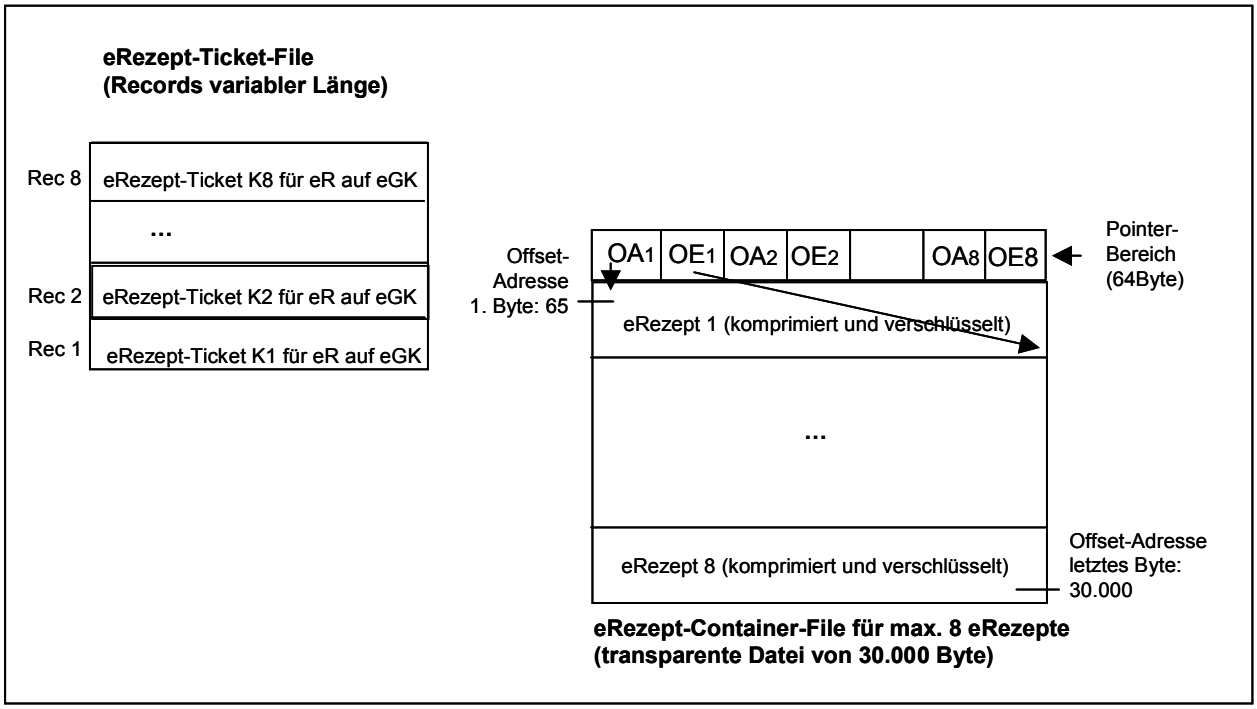

Abbildung 14 – eRezept-Tickets und eRezept-Container

G.2 Aufbau von eTickets und eRezept_Container

Der genaue Aufbau der eRezeptTickets und des eRezept_Containers wird im Dokument [gem-FA_VODM] beschrieben.

Anhang H

H1 - Abkürzungen

Kürzel	Erläuterung
AID	Application Identifier
AKP	Asymmetric Key Pair
AlgRef.	Algorithmus Referenz
AM	Zugriffsmodus (Access Mode)
AMS	Anwendungs-Management-System (Application Management System) sh. Auch CAMS
AMTS	Arzneimitteltherapie-Sicherheit
ARR	Access Rule Reference
ASD	Anwendungsspezifische Daten
ASN.1	Abstract Syntax Notation One
AT	Authentication Template
ATR	Answer-to-Reset
AUT	Authentisierung (Authentication)
Auth	Authentisierung (Authentication)
AUTN	Authentisierung für Nachrichten (pseudonymisiert)
AVS	Apothekenverwaltungssystem
B	Byte
BA	Berufsausweis für Mitarbeiter im Gesundheitswesen
BCD	Binär kodierte Dezimalzahl (Binary Coded Decimal)
BER	Basic Encoding Rules
BVD	Benutzer-Verifikationsdaten
BVG	Bundesversorgungsgesetz
C	Zertifikat (Certificate)
CA	Zertifizierungsinstanz (Certification Authority)
CAMS	Karten-Anw.-Managementsystem (Card Application Management System) sh.auch AMS
CMS	Karten-Management-System (Card Management System)
CAR	Referenz der Zertifizierungsinstanz (Certification Authority Reference)
CBC	Cipher Block Chaining
CC	kryptografische Prüfsumme (Cryptographic Checksum)

Kürzel	Erläuterung
CDB	Check Digit Byte
CE	Zertifikatserweiterungen (Certificate Extensions)
CG	Kryptogramm (Cryptogram)
CH	Karteninhaber (Cardholder)
CHA	Berechtigung des Karteninhabers (Certificate Holder Authorization)
CHR	Referenz des Karteninhabers (Certificate Holder Reference)
CIA	kryptografische Informationsanwendung (Cryptographic Information Application)
CIO	kryptografische Informationsobjekte (Cryptographic Information Objects)
CLA	Class-Byte eines Befehls
COS	Kartenbetriebssystem (Card Operating System)
CPI	Kennung des Zertifikatsprofils (Certificate Profile Identifier)
CRT	Control Reference Template
CS	CertSign (CertificateSigning)
CSP	Zertifizierungsdiensteanbieter (Certificate Service Provider)
CT	Confidentiality Template
CV	Card Verifiable (Zertifikat)
CWA	CEN Workshop Agreement
C2C	Card-to-Card
C2S	Card-to-Server
D, DIR	Verzeichnis (Directory)
DE	Datenelement
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DF	Dedicated File
DI	Baud rate adjustment factor
DM	Display Message
DMP	Disease Management Program
DO	Datenobjekt
DSI	Digital Signature Input
DST	Digital Signature Template
EAL	Evaluation Assurance Level
EF	Elementary File
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card
EHIC	European Health Insurance Card

Kürzel	Erläuterung
ENC	Verschlüsselung (Encryption)
ENC( )	verschlüsselte Daten (Encrypted data)
ENCV	Verschlüsselung für Verordnungen
EOF	Dateiende (End-of-File)
ES	Elektronische Signatur
FCP	File Control Parameter
FI	Clock rate conversion factor
FID	Dateikennung (File Identifier)
FM	Dateimanagement (File Management)
GKV	Gesetzliche Krankenversicherung
GP	Global Platform
HB	Historical Bytes
HBA	Heilberufsausweis
HCA	Gesundheitsanwendung (Health Care Application)
HI	Krankenversicherung (Health Insurance)
HIA	Geschäftsstelle der Krankenversicherung (Health Insurance Agency)
HID	Versichertendaten (Health Insurance Data)
HP	Heilberufler (Health Professional)
HPC	Heilberufsausweis (Health Professional Card)
ICC	Integrated Circuit Card
ICCSN	ICC Serial Number
ICM	IC-Herstellerkennung (IC Manufacturer)
ID	Identifier
IFD	Interface Device
IFSC	Information Field Size Card
IFSD	Information Field Size Device
IIN	Kennung des Kartenanbieters (Issuer Identification Number)
IV	Initial Value
KD	Key derivation Data
Key Ref.	Schlüssel-Referenz (Key Reference)
KVK	KrankenVersichertenKarte
KVNR	Krankenversicherten-Nummer
LSB	Least Significant Byte(s)
MAC	Message Authentication Code
MDO	Medizinisches DatenObjekt
MF	Master File

Kürzel	Erläuterung
MII	Major Industry Identifier
MSE	Manage Security Environment
OID	Objektkennung (Object Identifier)
PI	Padding Indicator
PIN	Personenkennung (Personal Identification Number)
PIX	Proprietary Appl. Prov. Extension
PK,PuK	Öffentlicher Schlüssel (Public Key)
PKI	Public Key Infrastructure
PKV	Private Krankenversicherung
PP	Schutzprofil (Protection Profile)
PPS	Protocol Parameter Selection
PrK	Privater Schlüssel (Private Key)
PRND	Padding Random Number
PSO	Perform Security Operation
PuK	Public Key
PUK	Personal Unblocking Key (Resetting Code)
PVS	Praxisverwaltungssystem
Q	Qualifiziert
QES	Qualifizierte Elektronische Signatur
R	Rollenkennung
RA	Registration Authority
RC	Retry Counter
RCA	Wurzelinstanz (Root CA)
RD	Referenzdaten (Reference Data)
RF	Radio Frequency
RFC	Request for Comment
RID	Registered Application Provider Id.
RND	Zufallszahl (Random Number)
RSA	Algorithmus von Rivest, Shamir, Adleman
S2C	Server-to-Card
SC	Sicherheitsbedingung (Security Condition)
SE	Sicherheitsumgebung (Security Environment)
SFID	Short EF Identifier
SIG	Signatur (Signature)
SK	geheimer Schlüssel (Secret Key)
SM	Secure Messaging

Kürzel	Erläuterung
SMC	Sicherheitsmodulkarte (Security Module Card)
SMK	SM-Schlüssel (SM key)
SN	Serien-Nummer (Serial Number)
SSC	Send Sequence Counter
SSCD	Sichere Signaturerstellungseinheit (Secure Signature Creation Device)
SSL	Security Sockets Layer
SST	Self Service Terminal (eKiosk)
SVA	Sozialversicherungsabkommen (der EU)
SVR	Server
TCE	Trusted Channel Establisment
TLV	Tag Length Value
TC	sicherer Kanal (Trusted Channel)
UID	Benutzerkennung (User Identification)
UQ	Usage Qualifier
UTF8	8-bit Unicode Transformation Format
VODD	Verordnungsdatendienst
VSD	Versichertenstammdaten
VSDD	Versichertenstammdaten-Dienst
ZDA	Zertifizierungs-Dienste-Anbieter
ZDA-NL	Zertifizierungs-Dienste-Anbieter-Nachladen
ZDA-VP	Zertifizierungs-Dienste-Anbieter-Vorpersonalisierung
3DES	Triple-DES

H2 - Glossar

Die Begriffserläuterungen des Projektes zur Einführung der Gesundheitskarte werden in einem zentralen Glossar veröffentlicht.

H3 - Abbildungsverzeichnis

H4 - Tabellenverzeichnis

H5 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Algorithmenkatalog 2005 vom 02.01.2005, 30. März 2005, Bundesanzeiger Nr. 59, S. 4695-4696 , siehe www.bundesnetzagentur.de
[CWA14890-1]	Application Interface for SmartCards used as Secure Signature Creation Devices, Part 1 – Basic Requirements March 8th 2004
[CWA14890-2]	Application Interface for SmartCards used as Secure Signature Creation Devices, Part 2 – Additional services March 12th 2004
[DIN66291-4]	DIN V66291-4: 2002 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG/SigV Teil 4: Grundlegende Sicherheitsdienste
[EN1867]	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
[gemeGK_Fach]	gematik (15.05.2007): Einführung der Gesundheitskarte – Speicherstrukturen der eGK für Gesundheitsanwendungen Version 1.2.0
[gemFA_AMTS]	gematik (Draft 2007): Einführung der Gesundheitskarte – Facharchitektur Arzneimitteltherapiesicherheit (in Vorbereitung)
[gemFA_ePA]	gematik (Draft 2007): Einführung der Gesundheitskarte – Facharchitektur elektronische Patientenakte (in Vorbereitung)
[gemFA_NFDM]	gematik (15.05.2007): Einführung der Gesundheitskarte – Facharchitektur Notfalldatenmanagement Version 1.2.0
[gemFA_VfA]	gematik (Draft 2007): Einführung der Gesundheitskarte – Facharchitektur Verwaltung freiwilliger Anwendungen (in Vorbereitung)
[gemFA_VODM]	gematik (15.05.2007): Einführung der Gesundheitskarte – Facharchitektur Verordnungsdatenmanagement Version 1.1.0
[gemFA_VSDM]	gematik (04.05.2007): Einführung der Gesundheitskarte – Facharchitektur Versichertenstammdatenmanagement Version 2.1.0
[gemSpec_eGK_P1]	gematik (2006): Spezifikation elektronische Gesundheitskarte –

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Teil 1 – Kommandos, Algorithmen und Funktionen des Kartenbetriebssystems Version 1.1.0
[gemSpec_Vers]	gematik (04.05.07): Einführung der Gesundheitskarte – Spezifikation von Versionsnummern in Schnittstellenspezifikationen und Software-Komponenten Version 1.1.0
[gemX.509_eGK]	gematik (05.06.2007): Einführung der Gesundheitskarte - Festlegungen zu den X.509-Zertifikaten der Versicherten, Version 1.3.0
[GMG]	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG), Drucksache 15/1525, 8.09.2003, online unter http://www.bmgs.bund.de/deu/gra/gesetze/
[HPC]	German Health Professional Card and Security Module Card Specification Part 1 – 3, Version 2.1
[ISO10118-2]	ISO/IEC 10118-2:2000 Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher
[ISO3166]	ISO/IEC 3166: Codes for the representations of names of countries
[ISO7816-4]	ISO/IEC 7816-4: 2004 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ISO7816-8]	ISO/IEC 7816-8: 2004 (2nd edition) Identification cards - Integrated circuit cards - Part 8: Commands for security operations
[ISO7816-15]	ISO/IEC 7816-15: 2004 Identification cards - Integrated circuit cards - Part 15: Cryptographic information application
[PKCS#1]	PKCS #1 RSA Cryptography Standard V2.1: June 14, 2002
[PP_eHC]	Protection Profile eHC Version xx
[Resolution190]	Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte
[SigG01]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt Nr. 22, 2001, S.876
[SigV01]	Verordnung zur elektronischen Signatur – SigV, 2001, Bundesgesetzblatt Nr. 509, 2001, S. 3074
[X.509]	ITU-T X.509: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, 1997