gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation der Security Module Card SMC-B Objektsystem

Version:	4.4.0
Revision:	109275
Stand:	15.05.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_SMC-B_ObjSys_G2.1

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitungen der Änderungen gemäß Änderungsliste P18.1

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
4.0.0	21.04.17		Einarbeitung Anpassungen Kartengeneration G2.1	gematik
4.1.0	18.12.17		Einarbeitung von Errata R1.6.4-2 sowie Anpassungen auf Grundlage von P 15.1	gematik
4.2.0	14.05.18		Anpassungen auf Grundlage von P 15.3	gematik
4.3.0	26.10.18		Einarbeitung P 15.9 (C_6562, C_6622)	gematik
			Einarbeitung P18.1	gematik
4.4.0	15.05.19		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an das Objektsystem der Sicherheitsmodulkarte SMC-B. Es beinhaltet die Definition der Anforderungen an die Objektstruktur, die Beschreibung der Kartenschnittstelle der Sicherheitsmodulkarte SMC-B für Institutionen im Gesundheitswesen.

Das Dokument berücksichtigt dabei:

- die DIN-Spezifikation für Chipkarten mit digitaler Signatur
- die ESIGN-Spezifikation für elektronische Signaturen
- die zugehörenden ISO-Standards (speziell ISO/IEC 7816, Teile 1-4, 6, 8, 9 und 15)
- andere Quellen (z. B. Anforderungen der Trustcenter)

Dieses Dokument spezifiziert Anwendungen der Sicherheitsmodulkarte SMC-B unter den folgenden, rein kartenorientierten Gesichtspunkten:

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

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

1.2 Zielgruppe

Das Dokument richtet sich an

- Hersteller, welche die hier spezifizierten Anwendungen für ein bestimmtes Chipkartenbetriebssystem umsetzen,
- Kartenherausgeber, die anhand der hier spezifizierten Anwendungen die elektrische Personalisierung einer Sicherheitsmodulkarte SMC-B planen,
- Hersteller von Systemen, welche unmittelbar mit der Chipkarte kommunizieren.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung des Dokuments

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

Die optische Gestaltung für alle SMCs und damit auch für die SMC-B wird in dem Dokument „Gemeinsame optische Merkmale der SMC“ [gemSpec_SMC_OPT] wird festgelegt.

1.5 Methodik

1.5.1 Nomenklatur

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

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

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

Für die Authentisierung der Zugriffe durch ein CMS auf die dafür vorgesehenen Objekte können entweder symmetrische Verfahren mit AES-Schlüsseln oder alternativ

asymmetrische Verfahren mit CV-Zertifikaten verwendet werden. Für beide Verfahren sind die Schlüsselobjekte in dieser Spezifikation spezifiziert.

Die in diesem Dokument referenzierten Flaglisten cvc_FlagList_CMS und cvc_FlagList_TI sind normativ in [gemSpec_PKI#6.7.5] und die dazugehörenden OIDs oid_cvc_fl_cms und oid_cvc_fl_ti sind normativ in [gemSpec_OID] definiert.

Gemäß [gemSpec_COS#(N022.400)] wird die Notwendigkeit einer externen Rollenauthentisierung für Karten der Generation 2 mit einer Flaglist wie folgt dargestellt: AUT(OID, FlagList) wobei OID stets aus der Menge {oid_cvc_fl_cms, oid_cvc_fl_ti} ist und FlagList ein sieben Oktett langer String, in welchem im Rahmen dieses Dokumentes genau ein Bit gesetzt ist. Abkürzend wird deshalb in diesem Dokument lediglich die Nummer des gesetzten Bits angegeben in Verbindung mit der OID. Ein gesetztes Bit i in Verbindung mit der oid_cvc_fl_cms wird im Folgenden mit flagCMS.i angegeben und ein gesetztes Bit j in Verbindung mit der oid_cvc_fl_ti wird im Folgenden mit flagTI.j angegeben.

Beispiele:

Langform	**Kurzform**
AUT(oid_cvc_fl_cms,'00010000000000')	flagCMS.15
AUT(oid_cvc_fl_ti, '00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')	flagTI.15 OR flagTI.16
PWD(PIN) AND [AUT(oid_cvc_fl_cms,'00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')]	PWD(PIN) AND [flagCMS.15 OR flagTI.16)]
SmMac(oid_cvc_fl_cms, '00800000000000')	SmMac(flagCMS.08)

Um die Zugriffsregeln für administrative Zugriffe in den einzelnen Tabellen übersichtlich darstellen zu können, werden folgende Abkürzungen verwendet:

AUT_CMS	{SmMac(SK.CMS.AES128) OR SmMac(SK.CMS.AES256) OR SmMac(flagCMS.08)} AND SmCmdEnc AND SmRspEnc

AUT_CUP	{SmMac(SK.CUP.AES128) OR SmMac(SK.CUP.AES256)} OR SmMac(flagCMS.10)} AND SmCmdEnc AND SmRspEnc

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

Dabei ist folgendes zu beachten:

1. Für Kommandonachrichten ohne Kommandodaten ist der Term SmCmdEnc sinnlos.
2. Für Antwortnachrichten ohne Antwortdaten ist der Term SmRspEnc sinnlos.
3. Die Spezifikation ist wie folgt zu interpretieren:
   a. Falls eine Kommandonachricht keine Kommandodaten enthält, dann ist es zulässig den Term SmCmdEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
   b. Falls eine Antwortnachricht keine Antwortdaten enthält, dann ist es zulässig den Term SmRspEnc zu ignorieren, falls er in der Spezifikation vorhanden ist.
4. Für die Konformitätsprüfung eines Prüflings gilt bei der Beurteilung von Zugriffsbedingungen:
   a. Falls für eine Zugriffsart keine Kommandodaten existieren, dann ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmCmdEnc zu verwenden.
   b. Falls für eine Zugriffsart keine Antwortdaten existieren, dann ist es für den Prüfling zulässig in der zugehörige Zugriffsregel den Term SmRspEnc zu verwenden.

1.5.2 Verwendung von Schüsselworten

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

Sie werden im Dokument wie folgt dargestellt:

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

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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

1.5.3 Komponentenspezifische Anforderungen

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

Tabelle 1: Tab_SMC-B_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt

Komponente	Beschreibung
K_Initialisierung	Instanz, welche eine Chipkarte im Rahmen der Initialisierung befüllt
K_Personalisierung	Instanz, die eine Chipkarte im Rahmen einer Produktion individualisiert
K_Terminal	eHealth-Kartenterminal
K_COS	Betriebssystem einer Smart Card

2 Optionen und Ausprägungen

Dieses Unterkapitel listet Funktionspakete auf, die für eine Zulassung einer SMC-B der Generation 2 nicht zwingend erforderlich sind.

2.1 Option_Erstellung_von_Testkarten

Card-G2-A_3370 - K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten
Die SMC-B KANN als Testkarte ausgestaltet werden. Soweit in dieser Spezifikation Anforderungen an Testkarten von den Anforderungen an Produktivkarten abweichen, wird dies an der entsprechenden Stelle aufgeführt.
[<=]

2.2 Ausprägung ohne Zugriff auf die eGK

SMC-Bs können auch in Organisationen eingesetzt werden, die an der TI teilnehmen, aber nicht zum Zugriff auf die eGK berechtigt sind. Um zu verhindern, dass eine solche SMC-B den Zugriff auf eine eGK freischalten kann, wird das Rollenzertifikat EF.C.SMC.AUTR_CVC.E256 bei der Personalisierung entweder gar nicht oder mit Nullen befüllt. Ein zugehöriger privater Schlüssel bleibt herstellerspezifisch „unbefüllt“ oder wird mit nicht-nutzbaren Dummy-Daten befüllt.

Dies wird in den entsprechenden Personalisierungsfestlegungen mit dem Zusatz „Ausprägung_ORG“ gekennzeichnet.

3 Lebenszyklus von Karte und Applikation

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

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

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

4 Anwendungsübergreifende Festlegungen

Zur Umsetzung dieses Kartentyps ist ein Betriebssystem hinreichend, welches folgende Optionen enthält:

- Unterstützung von mindestens vier logischen Kanälen.
- Unterstützung von Onboard-RSA-Schlüsselgenerierung

4.1 Mindestanzahl logischer Kanäle

Card-G2-A_2196 - K_Initialisierung: Anzahl logischer Kanäle
Für die Anzahl logischer Kanäle, die von einer SMC-B zu unterstützen ist, gilt:

1. Die maximale Anzahl logischer Kanäle MUSS gemäß [ISO7816-4#Tab.88] in den Historical Bytes in EF.ATR angezeigt werden.
2. Die SMC-B MUSS mindestens vier logische Kanäle unterstützen. Das bedeutet, die in den Bits b3b2b1 gemäß [ISO7816-4#Tab.88] kodierte Zahl MUSS mindestens ‘011’ = 3 oder größer sein.

[<=**]**

Jeder Kanal besitzt seinen eigenen unabhängigen Sicherheitsstatus, d.h., eine externe Authentisierung der Rollenkennung in einem logischen Kanal setzt keinen Sicherheitszustand in irgendeinem anderen Kanal.

4.2 Unterstützung RSA CV-Zertifikate

A_15176 - K_SMC_B: Vorhandensein asymmetrischer Kryptographiealgorithmus RSA für CV Zertifikate
Für eine SMC-B KANN für das Objektsystem ein COS verwendet werden,
1. das die Option_RSA_CVC implementiert hat.
2. das die Option_RSA_CVC nicht implementiert hat.**[**<=**]**

4.3 Unterstützung Onboard-RSA-Schlüsselgenerierung

Card-G2-A_3849 - K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung
Das COS einer SMC-B MUSS die Option_RSA_KeyGeneration implementieren.**[**<=**]**

4.4 Optionale Funktionspakete

4.4.1 Kontaktlose Schnittstelle

Card-G2-A_2138 - K_Terminal: Ausschluss kontaktlose Schnittstelle
Die in der Spezifikation [gemSpec_COS#11.2] zusätzlich zur kontaktbehafteten Schnittstelle gemäß [gemSpec_COS#11.2.1] als optional definierte Schnittstelle zur kontaktlosen Datenübertragung gemäß ISO/IEC 14443 (siehe [gemSpec_COS#11.2.3]) DARF für die SMC-B NICHT genutzt werden.**[<=]**

4.4.2 USB-Schnittstelle (optional)

Card-G2-A_3036 - K_SMC-B: USB-Schnittstelle
Falls eine SMC-B die Option_USB_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_USB_Schnittstelle implementiert hat.**[<=]**

Card-G2-A_3037 - K_SMC-B: Vorhandensein einer USB-Schnittstelle
Falls eine SMC-B die Option_USB_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_USB_Schnittstelle implementiert hat.
b) das die Option_USB_Schnittstelle nicht implementiert hat.
[<=]

4.4.3 Kryptobox (optional)

Card-G2-A_3188 - K_SMC-B: Vorhandensein Option_Kryptobox
Für eine SMC-B KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_Kryptobox implementiert hat.
b) das die Option_Kryptobox nicht implementiert hat.
[<=]

4.4.4 Symmetrischer Kryptographiealgorithmus DES (optional)

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

Card-G2-A_3665 - K_SMC-B: Vorhandensein symmetrischer Kryptographie-algorithmus DES
Für eine SMC-B KANN für das Objektsystem ein COS verwendet werden,
a) das die Option_DES implementiert hat.
b) das die Option_DES nicht implementiert hat.

[<=]

4.5 Attributstabellen

Card-G2-A_2134 - K_Initialisierung: Änderung von Zugriffsregeln
Die in diesem Dokument definierten Zugriffsregeln DÜRFEN in der Nutzungsphase NICHT veränderbar sein.**[<=]**

Card-G2-A_2135 - K_Initialisierung: Verwendung von SE
Alle Objekte MÜSSEN sich in SE#1 wie angegeben verwenden lassen.**[**<=**]**

Card-G2-A_3189 - K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs
Jedes Objekt KANN in SE verwendbar sein, die verschieden sind von SE#1.**[**<=**]**

Card-G2-A_3190 - K_Initialisierung: Eigenschaften der Objekte in anderen SEs
Falls ein Objekt in einem von SE#1 verschiedenen SE verwendbar ist, dann MUSS es dort dieselben Eigenschaften wie in SE#1 besitzen.**[**<=**]**

4.5.1 Attribute eines Ordners

Card-G2-A_2136-01 - K_Initialisierung: Ordnerattribute
Enthält eine Tabelle mit Ordnerattributen einen oder mehrere *applicationIdentifier* (AID), dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
[<=**]**

Card-G2-A_3647 - K_Initialisierung: Herstellerspezifischer ApplicationIdentifier
Enthält eine Tabelle mit Ordnerattributen keinen *applicationIdentifier* (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.

[<=**]**

Card-G2-A_3648 - K_Initialisierung: Fehlender FileIdentifier
Enthält eine Tabelle mit Ordnerattributen keinen *fileIdentifier* (FID), so DARF dieser Ordner NICHT mittels eines *fileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.1] selektierbar sein, es sei denn, es handelt sich um den Ordner *root*, dessen optionaler *fileIdentifier* den Wert ‘3F00’ besitzen MUSS.

[<=**]**

Card-G2-A_3649 - K_Initialisierung: Herstellerspezifischer FileIdentifier
Enthält eine Tabelle mit Ordnerattributen keinen *fileIdentifier* (FID), so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden.

[<=**]**

4.5.2 Attribute einer Datei (EF)

Card-G2-A_2137 - K_Initialisierung: Dateiattribute
Enthält eine Tabelle mit Attributen einer Datei keinen *shortFileIdentifier*, so DARF sich dieses EF NICHT mittels *shortFileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.2] selektieren lassen.**[**<=**]**

Card-G2-A_2668 - K_Initialisierung und K_Personalisierung: Wert von „positionLogicalEndOfFile“
Für transparente EFs MUSS der Wert von „positionLogicalEndOfFile“, soweit nicht anders spezifiziert, auf die Anzahl der tatsächlich belegten Bytes gesetzt werden.**[**<=**]**

4.6 Zugriffsregeln für besondere Kommandos

Gemäß [gemSpec_COS] gilt:

Card-G2-A_2669 - K_Initialisierung: Zugriffsregeln für besondere Kommandos
Die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT MUSS stets ALWAYS sein, unabhängig vom *lifeCycleStatus* und unabhängig vom aktuellen Security Environment.

[<=]

4.7 Attributswerte und Personalisierung

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

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

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

Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:

Card-G2-A_3375 - K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung
Zur Unterstützung herstellerspezifischer Personalisierungsprozessen KÖNNEN die Werte von Attributen eines Kartenproduktes von den Festlegungen dieses Dokumentes abweichen. Hierbei MÜSSEN Abweichungen auf solche beschränkt sein, die hinsichtlich ihrer Wirkung in der personalisierten Karte sowohl fachlich wie sicherheitstechnisch der in der Spezifikation vorgegebenen Werten entsprechen.
[<=]

Card-G2-A_3527 - K_Initialisierung: Schlüsselgenerierung auf der Karte
Die SMC-B MUSS die Generierung von asymmetrischen Schlüsselpaaren auf der Karte ermöglichen.
[<=]

Card-G2-A_3528 - K_Initialisierung: Weitere Verfahren zur Personalisierung von Schlüsseln
Die SMC-B KANN andere Verfahren als das in Card-G2-A_3527 genannte zur Personalisierung asymmetrischer Schlüsselpaare unterstützen.
[<=]

Card-G2-A_3524 - K_Personalisierung: Schlüsselgenerierung auf der Karte
Wenn ein privater Schlüssel für die SMC-B zu personalisieren ist, dann MUSS das Schlüsselpaar von der Smartcard selbst erzeugt werden. Es MUSS sichergestellt sein, dass der private Teil des Schlüssels die Smartcard nie verlässt.
[<=]

4.8 Kartenadministration

In den Kapiteln 5.3.15 und 5.3.16 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen einem Kartenadministrationssystem (z.B. einem CUpS) und einer Karte beschrieben, die bei der Ausgabe der Karte angelegt werden müssen.

Card-G2-A_3035 - Absicherung der Kartenadministration
Bei der Personalisierung MUSS der Schlüssel PuK.RCA.ADMINCMS.CS für die asymmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.**[<=]**

Card-G2-A_3588 - Symmetrische Kartenadministration
Bei der Personalisierung KÖNNEN die Schlüssel (SK.CMS und SK.CUP) für die symmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.**[<=]**

Card-G2-A_3589 - Schlüsselspeicherung
Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die Schlüssel zur Absicherung der Kartenadministration während der gesamten Nutzungsdauer der SMC-B sicher verwahrt werden und bei Bedarf an ein Kartenadministrationssystem (z.B. ein CUpS) übergeben werden können.**[<=]**

5 Spezifikation grundlegender Applikationen

Zu den grundlegenden Applikationen der Sicherheitsmodulkarte SMC-B zählen:

- das Wurzelverzeichnis der SMC, auch Root oder Master File (MF) genannt,
- die Krypto-Anwendung DF.ESIGN

5.1 Attribute des Objektsystems

Das Objektsystem der SMC-B enthält gemäß [gemSpec_COS#9.1] folgende Attribute:

Card-G2-A_2139 - K_Initialisierung: Wert des Attributes root
Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_SMC-B_ObjSys_002 sein.**[**<=**]**

Card-G2-A_2140-01 - K_Initialisierung und K_Personalisierung: Wert des Attributes answerToReset
Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A_3340, Card-G2-A_3341-01, Card-G2-A_3650, Card-G2-A_3342 und Card-G2-A_3343 entsprechen.

[<=**]**

Card-G2-A_2141 - K_Personalisierung: Wert des Attributes iccsn8
Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein.**[**<=**]**

Card-G2-A_2142-01 - K_Initialisierung: Inhalt persistentPublicKeyList
Das Attribut *persistentPublicKeyList* MUSS den Schlüssel PuK.RCA.CS.E256 enthalten.**[**<=**]**

Card-G2-A_3187 - K_Initialisierung: Größe persistentPublicKeyList
Für das Attribut *persistentPublicKeyList* MUSS so viel Speicherplatz bereitgestellt werden, dass mindestens fünf weitere öffentliche Signaturprüfschlüssel einer Root-CA mittels Linkzertifikaten persistent importierbar sind**[**<=**]**

Card-G2-A_3267-01 - K_Initialisierung: Wert von pointInTime
Der Hersteller des Objektsystems MUSS das Attribut *pointInTime* im Rahmen der Initialisierung auf den Wert von CED (Certificate Effective Date) aus dem selbst signierten CV-Zertifikat zu PuK.RCA.CS setzen.
[<=**]**

Card-G2-A_3472 - K_Personalisierung: personalisierter Wert von pointInTime
Das Attribut *pointInTime* MUSS im Rahmen der Personalisierung auf den Wert von CED eines Endnutzerzertifikates gesetzt werden. Falls es mehrere Endnutzerzertifikate gibt, so ist das CED mit dem größten Wert zu verwenden.
[<=**]**

5.1.1 ATR-Kodierung und technische Eigenschaften

Card-G2-A_3340 - K_Initialisierung und K_Personalisierung: ATR-Kodierung
Die ATR-Kodierung MUSS die in Tab_SMC-B_ObjSys_117 dargestellten Werte besitzen.

Tabelle 2: Tab_SMC-B_ObjSys_117 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_COS#N024.100])
TD1	'81'	Interface Character, (T=1, TD2 indication)
TD2	'B1'	Interface Character, (T=1, TA3/TB3/TD3 indication)
TA3	'FE'	Interface Character (IFSC coding)
TB3	'45'	Interface Character, (BWI/CWI coding)
TD3	'1F'	Interface Character, (T=15, TA4 indication)
TA4	'xx'	Interface Character (XI/UI coding)
Ti	HB	Historical Bytes (HB, imax. = 15)
TCK	XOR	Check Character (exclusive OR)

[<=]

Card-G2-A_3341-01 - K_Initialisierung und K_Personalisierung: TC1 Byte im ATR
Der ATR SOLL ein TC1 Byte mit dem Wert 'FF' enthalten.

[<=]

Card-G2-A_3650 - K_Personalisierung und K_Initialisierung: TC1 Byte im ATR
Wenn der ATR ein TC1 Byte mit dem Wert 'FF' enthält, MUSS T0 auf den Wert 'Dx' gesetzt werden.

[<=]

Card-G2-A_3342 - K_Initialisierung und K_Personalisierung: Historical Bytes im ATR
Der ATR SOLL keine Historical Bytes enthalten.

[<=]

Card-G2-A_3343 - K_Initialisierung und K_Personalisierung: Vorgaben für Historical Bytes
Falls der ATR Historical Bytes enthält, dann MÜSSEN

1. diese gemäß [ISO7816-4] kodiert sein.
2. Die dort getroffenen Angaben konsistent sein zu Angaben im EF.ATR.

[<=]

5.2 Allgemeine Struktur

Abb_SMC-B_ObjSys_001 zeigt die allgemeine Struktur der Objekte einer SMC-B.

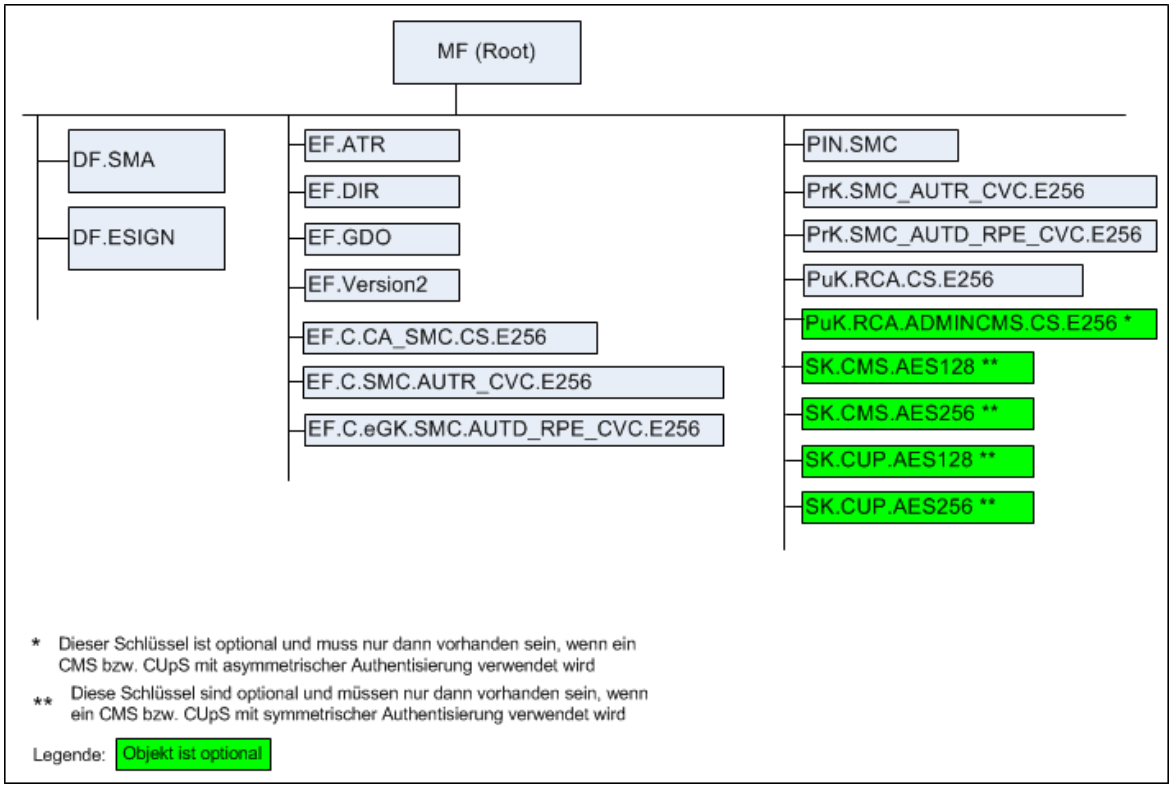

Abbildung 1: Abb_SMC-B_ObjSys_001 Allgemeine Struktur der SMC-B

Eine kryptografische Informationsanwendung (DF.CIA.ESIGN) ist nicht erforderlich, da eine SMC-B stationär gesteckt bleibt und die Anwendung der zuständigen Software bekannt ist.

5.3 Root, die Wurzelapplikation MF

Das MF der SMC-B ist ein “Application Dedicated File” (siehe [gemSpec_COS#8.3.1.3]) mit den in Tab_SMC-B_ObjSys_002 gezeigten Eigenschaften.

Card-G2-A_2146 - K_Initialisierung: Initialisierte: Attribute von MF
MF MUSS die in Tab_SMC-B_ObjSys_002 dargestellten Werte besitzen.

Tabelle 3: Tab_SMC-B_ObjSys_002 Initialisierte Attribute von MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	‘D27600014606’	
fileIdentifier	‘3F 00’	Falls

		vorhanden
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
FINGERPRINT	Wildcard	
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

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

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

Hinweis 4: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.5.

5.3.1 MF / EF.ATR

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

Card-G2-A_2147-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.ATR
EF.ATR MUSS die in Tab_SMC-B_ObjSys_003 dargestellten Werte besitzen.

Tabelle 4: Tab_SMC-B_ObjSys_003 Initialisierte Attribute von MF / EF.ATR

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 01’	siehe Hinweis 6:
shortFileIdentifier	‘1D’= 29	
numberOfOctet	herstellerspezifisch	

positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1]	siehe unten
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY WRITE BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 5: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 6: Der Wert des Attributs fileIdentifier ist in [ISO7816-4] festgelegt.

Card-G2-A_3344 - K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR

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

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

[<=]

5.3.2 MF / EF.DIR

Die Datei EF.DIR enthält eine Liste mit Anwendungs-Templates gemäß [ISO/IEC 7816-4]. Diese Liste wird dann angepasst, wenn sich die Applikationsstruktur durch Löschen oder Anlegen von Anwendungen verändert.

Card-G2-A_3651 - K_Initialisierung: Inhalt der Records von EF.DIR
Für jede im Objektsystem vorhandene Anwendung MUSS die Datei einen eigenen Record besitzen, der den ApplicationIdentifier (AID) dieser Anwendung im Format ´61-L_{61}-{4F-L_{4F}-AID}´ enthält.
Zu jedem Record der Datei MUSS es auf der Karte eine Anwendung geben, deren AID durch diesen Record beschrieben ist.
Record 1 des EF.DIR MUSS den AID des MF enthalten.

[<=]

Card-G2-A_2154-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.DIR
EF.DIR MUSS die in Tab_SMC-B_ObjSys_005 dargestellten Werte besitzen.

Tabelle 5: Tab_SMC-B_ObjSys_005 Initialisierte Attribute von MF / EF.DIR

Attribute	**Wert**	**Bemerkung**
Objekttyp	linear variables Elementary File	
fileIdentifier	‘2F 00’	siehe Hinweis 8:
shortFileIdentifier	‘1E’= 30	siehe Hinweis 8:
numberOfOctet	‘00 5A’ Oktett = 90 Oktett	
maxNumRecords	7 Records	
maxRecordLength	19 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
recordList Record 1 Record 2 und folgende	‘61- 08- (‘4F 06 D27600014606)’ ´61-L_{61}-{4F-L_{4F}-AID}´ für alle Applikationen im Objektsystem	AID.MF
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
APPEND RECORD	AUT_CMS	siehe Hinweis 9:
DELETE RECORD	AUT_CMS	siehe Hinweis 9:
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT_CMS	siehe Hinweis 9:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

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

Hinweis 8: Die Werte von fileIdentifier und shortFileIdentifier sind in ISO/IEC 7816-4 festgelegt.

Hinweis 9: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.5.

5.3.3 MF / EF.GDO

In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte enthält. Die Kennnummer basiert auf [Beschluss190].

Card-G2-A_2156 - K_Initialisierung: Initialisierte Attribute von MF / EF.GDO
EF.GDO MUSS die in Tab_SMC-B_ObjSys_006 dargestellten Werte besitzen.

Tabelle 6: Tab_SMC-B_ObjSys_006 Initialisierte Attribute von MF / EF.GDO

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 02’	
shortFileIdentifier	‘02’= 2	
numberOfOctet	‘00 0C’ Oktett = 12 Oktett	
positionLogicalEndOfFile	Wildcard	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Wildcard	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Card-G2-A_2157-01 - K_Personalisierung: Personalisiertes Attribut von EF.GDO
Bei der Personalisierung von EF.GDO MÜSSEN die in Tab_SMC-B_ObjSys_107 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 7: Tab_SMC-B_ObjSys_107 Personalisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	‘00 0C’ Oktett = 12 Oktett	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1]	

[<=]

5.3.4 MF / EF.Version2

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

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

Die konkrete Befüllung ist in [gemSpec_Karten_Fach_TIP_G2.1] beschrieben.

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

Card-G2-A_2158-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.Version2
EF.Version2 MUSS die in Tab_SMC-B_ObjSys_007 dargestellten Werte besitzen.

Tabelle 8: Tab_SMC-B_ObjSys_007 Initialisierte Attribute von MF / EF.Version2

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 11’	
shortFileIdentifier	‘11’= 17	
numberOfOctet	‘00 3C’ Oktett = 60 Oktett	
positionLogicalEndOfFile	passend zum Inhalt	gemäß [gemSpec_Karten_Fach_TIP_G2.

		1]
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1]	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
UPDATE BINARY SET LOGICAL EOF	AUT_CMS	siehe Hinweis 10:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 10: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.5.

5.3.5 MF / EF.C.CA_SMC.CS.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SMC.CS.E256 einer CA enthält.

Card-G2-A_2160-01 - K_Initialisierung: Initialisierte Attribute MF / EF.C.CA_SMC.CS.E256
EF.C.CA_SMC.CS.E256 MUSS die in Tab_SMC-B_ObjSys_009 dargestellten Werte besitzen.

Tabelle 9: Tab_SMC-B_ObjSys_009 Initialisierte Attribute MF / EF.C.CA_SMC.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 07’	
shortFileIdentifier	‘07’= 7	

numberOfOctet	‘00 DC’ Oktett = 220 Oktett	
positionLogicalEndOfFile	‘0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 12:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 12:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Card-G2-A_3347 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.E256
Bei der Personalisierung von MF / EF.C.CA_SMC.CS.E256 MÜSSEN die in Tab_SMC-B_ObjSys_069 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 10: Tab_SMC-B_ObjSys_069 Personalisierte Attribute von MF / EF.C.CA_SMC.CS.E256

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

[<=]

5.3.6 MF / EF.C.SMC.AUTR_CVC.E256

EF.C.SMC.AUTR_CVC.E256 enthält das CV-Zertifikat der SMC-B für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen SMC-B und eGK. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTR_CVC.E256 ist im Kapitel 5.3.12 definiert. Für die Ausprägung _ORG bleibt diese Datei leer oder wird mit Nullen befüllt.

Card-G2-A_2163 - K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256
EF.C.SMC.AUTR_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_012 dargestellten Werte besitzen.

Tabelle 11: (Tab_SMC-B_ObjSys_012) Initialisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256

Attribute	**Wert**	**Bemerkung**
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 06’	
shortFileIdentifier	‘06’= 6	
numberOfOctet	‘00DE’ Oktett = 222 Oktett	
positionLogicalEndOfFile	‘0’	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 16:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 16:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 15: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5.

Card-G2-A_3389 - K_Personalisierung: Festlegung von CHR in MF / EF.C.SMC.AUTR_CVC.E256
Für die CHR in diesem Zertifikat MUSS CHR = ’00 06’ || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2157].**[**<=**]**

Card-G2-A_3349 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256
Bei der Personalisierung von EF.C.SMC.AUTR_CVC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_072 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 12: Tab_SMC-B_ObjSys_072 Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	‘00DE’ Oktett = 222 Oktett	
positionLogicalEndOfFile Ausprägung_ORG	Wildcard	Entsprechend dem Verfahren des Personalisierers und passend zu body
body	C.SMC.AUTR_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.SMC.AUTR_CVC.E256	
body Ausprägung_ORG	Leer oder ’00 … 00‘	Entsprechend dem Verfahren des Personalisierers und passend zu positionLogicalEndOfFile

[<=**]**

5.3.7 MF / EF.C.SMC.AUTD_RPE_CVC.E256

EF.C.SMC.AUTD_RPE_CVC.E256 enthält das CV-Zertifikat für die Kryptographie mit elliptischen Kurven für die C2C-Geräteauthentisierung zwischen einer lokal vorhandenen SMC-B und einer SMC-B als entferntem PIN-Empfänger. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTD_RPE_CVC.E256 ist im Kapitel 5.3.13 definiert.

Card-G2-A_2169 - K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256
EF.C.SMC.AUTD_RPE_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_018 dargestellten Werte besitzen.

Tabelle 13: (Tab_SMC-B_ObjSys_018) Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘2F 09’	
shortFileIdentifier	‘09’= 9	

numberOfOctet	'00DE' Oktett = 222 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 18:
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 18:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 16: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 17: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5.

Card-G2-A_3390 - K_Personalisierung: Festlegung von CHR in MF / EF.C.SMC.AUTD_RPE_CVC.E256
Für die CHR in diesem Zertifikat MUSS CHR = '00 09' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2157].**[<=]**

Card-G2-A_3350 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256
Bei der Personalisierung von EF.C.SMC.AUTD_RPE_CVC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_074 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 14: Tab_SMC-B_ObjSys_074 Personalisierte Attribute von MF / EF.C.SMC.AUTD_RPE_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00DE' Oktett = 222 Oktett	

body	C. SMC.AUTD_RPE_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK. SMC.AUTD_RPE_CVC.E256	

[<=]

5.3.8 MF / PIN.SMC

Dieses Passwortobjekt wird zur Freischaltung von Schlüsseln und Inhalten der SMC-B verwendet.

Card-G2-A_2171 - K_Initialisierung: Initialisierte Attribute von MF / PIN.SMC
PIN.SMC MUSS die in Tab_SMC-B_ObjSys_020 dargestellten Werte besitzen.

Tabelle 15: Tab_SMC-B_ObjSys_020 Initialisierte Attribute von MF / PIN.SMC

Attribute	**Wert**	**Bemerkung**
Objekttyp	Reguläres Passwortobjekt	
pwdIdentifier	‘01’ = 1	
secret	undefiniert	wird personalisiert
minimumLength	6	
MaximumLength	8	
startRetryCounter	3	
retryCounter	3	
transportStatus	Transport-PIN	
flagEnabled	True	
startSsec	unendlich	
PUK	undefiniert	wird personalisiert
pukUsage	10	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC. P1 AUS DER MENGE {0, 1}	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 18: Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: ACTIVATE, CHANGE REFERENCE DATA, DEACTIVATE, DELETE, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, GET PIN STATUS, RESET RETRY COUNTER, VERIFY, TERMINATE.

Card-G2-A_3351 - K_Personalisierung: Personalisierte Attribute von MF / PIN.SMC
Bei der Personalisierung von PIN.SMC MÜSSEN die in Tab_SMC-B_ObjSys_076 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 16: Tab_SMC-B_ObjSys_076 Personalisierte Attribute von MF / PIN.SMC

Attribute	Wert	Bemerkung
secret	PIN-Wertgemäß [gemSpec_PINPUK_TI]	Transport-PIN
secretLength	5 Ziffern (*minimumLength* - 1)	Länge der Transport-PIN
PUK	PUK-Wert gemäß [gemSpec_PINPUK_TI]	
PUKLength	8 Ziffern	

[<=]

5.3.9 MF / PrK.SMC.AUTR_CVC.E256

PrK.SMC.AUTR_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/eGK. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTR_CVC.E256 ist in C.SMC.AUTR_CVC.E256 (siehe Kapitel 5.3.8) enthalten. Für die Ausprägung _ORG bleibt dieser Schlüssel herstellerspezifisch „unbefüllt“ oder wird mit Zufallswerten befüllt.

Card-G2-A_2180-01 - K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256
PrK.SMC.AUTR_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_022 dargestellten Werte besitzen.

Tabelle 17: Tab_SMC-B_ObjSys_022 Initialisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	‘06’ = 6	

privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge {elcRoleAuthentication}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
INTERNAL AUTHENTICATE	PWD(PIN.SMC)	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 23:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Hinweis 22: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 23: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5

Card-G2-A_3355 - K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256
Bei der Personalisierung von PrK.SMC.AUTR_CVC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_078 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 18: Tab_SMC-B_ObjSys_078 Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
keyAvailable Ausprägung_*ORG*	False, ggf. True	Entsprechend dem Verfahren des Personalisierers
privateElcKey	keyData = Wildcard	
privateElcKey Ausprägung_*ORG*	Herstellerspezifisch „nicht nutzbar“ (z.B. mit Zufallswerten)	Entsprechend dem Verfahren des Personalisierers

[<=]

5.3.10 MF / PrK.SMC.AUTD_RPE_CVC.E256

PrK.SMC.AUTD_RPE_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen einer gSMC-KT und einer SMC-B in der Funktion des PIN-Empfängers. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTD_RPE_CVC.E256 ist in C.SMC.AUTD_RPE_CVC.E256 (siehe Kapitel 5.3.9) enthalten.

Card-G2-A_2189 - K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256
PrK.SMC.AUTD_RPE_CVC.E256 MUSS die in Tab_SMC-B_ObjSys_028 dargestellten Werte besitzen.

Tabelle 19: Tab_SMC-B_ObjSys_028 Initialisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Authentisierungsobjekt ELC 256	Profil 55 (PIN-Empfänger)
keyIdentifier	‘09’ = 9	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Domainparameter = brainpoolP256r1	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	Ein Wert aus der Menge { elcSessionkey4SM, elcAsynchronAdmin}	
numberScenarion	0	
accessRuleSession keys	irrelevant	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 28:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Hinweis 24: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 25: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5:

Card-G2-A_3356 - K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256
Bei der Personalisierung von PrK.SMC.AUTD_RPE_CVC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_080 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 20: Tab_SMC-B_ObjSys_080 Personalisierte Attribute von MF / PrK.SMC.AUTD_RPE_CVC.E256

Attribute	Wert	Bemerkung
privateKey	Domainparameter = brainpoolP256r1	
keyAvailable	True	

[<=]

5.3.11 Sicherheitsanker zum Import von CV-Zertifikaten

Der Sicherheitsanker zum Import von CV-Zertifikaten ist ein öffentliches Signaturprüfobjekt und enthält den öffentlichen Schlüssel der Root-CA für CV-Zertifikate der Telematikinfrastruktur.

5.3.11.1 MF / PuK.RCA.CS.E256

PuK.RCA.CS.E256 ist der öffentliche Schlüssel der Root-CA des Gesundheitswesens für die Kryptographie mit elliptischen Kurven für die Prüfung von CV-Zertifikaten, die von dieser herausgegeben werden.

Card-G2-A_2192-01 - K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256
PuK.RCA.CS.E256 MUSS die in Tab_SMC-B_ObjSys_031 dargestellten Werte besitzen.

Tabelle 21: Tab_SMC-B_ObjSys_031 Initialisierte Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches Signaturprüfobjekt ELC 256	
Für Echtkarten MÜSSEN die vier folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die vier folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	ELC 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes)	
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß [gemSpec_CVC_Root#5.4.2]	
CHAT	OID_{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 00E2'	siehe Hinweis 29:
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP#4.5]	
Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		
oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
lifeCycleStatus	„Operational state (activated)"	
accessRulesPublicSignatureVerificationObject	Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: DELETE --> AUT_CMS OR AUT_CUP PSO Verify Certificate -->	

	ALWAYS	
accessRulesPublicAuthenticationObject	Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: DELETE -->ALWAYS EXTERNAL AUTHENTICATE--> ALWAYS	siehe Hinweis 28:
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO VERIFY CERT.	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 27:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Hinweis 29: Während gemäß den Tabellen in [gemSpec_COS]#H.4] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ‚0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ‚1' gesetzt.

Card-G2-A_3374-01 - K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Bei der Personalisierung von PuK.RCA.CS.E256 für Testkarten MÜSSEN die in Tab_SMC-B_ObjSys_119 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.
Wenn die restlichen Attribute von PuK.RCA.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_gSMC-B_ObjSys_031 personalisiert werden.

Tabelle 22: Tab_SMC-B_ObjSys_119 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Attribute	Wert	Bemerkung
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-CVC-CA	personalisieren gemäß [gemSpec_TK#3.1.2]
keyIdentifier	E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels	
CHAT	• OID_{flags} = oid_cvc_fl_ti	

	• flagList = 'FF 0084 2006 00E2'	
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels	

[<=]

5.3.12 Asymmetrische Kartenadministration

Die hier beschriebene Variante der Administration der SMC-B betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der SMC-B.

Die Administration einer SMC-B erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels asymmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels symmetrischer Verfahren werden in 5.3.16 beschrieben.

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

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

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

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie für die asymmetrische CMS-Authentisierung steht. PuK.RCA.ADMINCMS.CS.E256 wird für den Import weiterer Schlüssel für die elliptische Kryptographie benötigt.

Card-G2-A_3039-01 - K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256
PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab_SMC-B_ObjSys_063 dargestellten Attribute besitzen.

Tabelle 23: Tab_SMC-B_ObjSys_063 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches Signaturprüfobjekt, ELC 256	
Für Echtkarten MÜSSEN die beiden folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		

CHAT	• OID_{flags} = oid_cvc_fl_cms flagList = 'FF AFFF FFFF FFFF'	siehe Hinweis 31:
expirationDate	Identisch zu „expirationDate" von PuK.RCS.CS.E256	
Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	'0000 0000 0000 0013'	
lifeCycleStatus	„Operational state (activated)"	
publicKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Domainparameter = brainpoolP256r1	wird personalisiert
oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
accessRulesPublicSignatureVerificationObject.	Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: DELETE --> AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublicAuthenticationObject.	Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: DELETE --> ALWAYS	siehe Hinweis 28:
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
PSO VERIFY CERTIFICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 32:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
alle	NEVER	

[<=]

Hinweis 30: Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind:
Activate, Deactivate, Delete, PSO Verify Certificate, Terminate

Hinweis 31: Während gemäß den Tabellen in [gemSpec_COS]#H.4] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ‚0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ‚1' gesetzt.

Hinweis 32: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5.

Card-G2-A_3357-01 - K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256
Bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 MÜSSEN die in Tab_SMC-B_ObjSys_083 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.
Wenn die restlichen Attribute von PuK.RCA.ADMINCMS.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_SMC-B_ObjSys_063 personalisiert werden.

Tabelle 24: Tab_SMC-B_ObjSys_083 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
publicKey	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Admin-CVC-Root	
publicKey Option_Erstellung _von_Testkarten	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-Admin-CVC-Root	
CHAT	• OIDflags = oid_cvc_fl_cms • flagList = 'FF AFFF FFFF FFFF'	
expirationDate Option_Erstellung _von_Testkarten	Identisch zu „expirationDate" des personalisierten PuK.RCA.CS.E256	

[<=]

5.3.13 Symmetrische Kartenadministration

Die hier beschriebene Variante der Administration der SMC-B betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der SMC-B.

Die Administration einer SMC-B erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels symmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels asymmetrischer Verfahren werden in 5.3.15 beschrieben.

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

Wenn die symmetrischen Schlüssel (SK.CMS und SK.CUP) für die Authentifizierung des Kartenadministrationssystems genutzt werden, dann MÜSSEN sie

kartenindividuell personalisiert werden, so dass mit einem Schlüssel eines administrierenden Systems genau eine SMC-B administriert werden kann.

Bei der Personalisierung sind nur die Schlüssel zu personalisieren, die tatsächlich benötigt werden.

5.3.13.1 MF / SK.CMS.AES128

SK.CMS.AES128 (optional) ist der geheime Schlüssel für die Durchführung des SMC-B/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel. Die nachfolgende Tabelle Tab_SMC-B_ObjSys_033 zeigt die Eigenschaften des Schlüssels.

Card-G2-A_2194-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128
SK.CMS.AES128 MUSS die in Tab_SMC-B_ObjSys_033 dargestellten Werte besitzen.

Tabelle 25: Tab_SMC-B_ObjSys_033 Initialisierte Attribute von MF / SK.CMS.AES128

Attribute	**Wert**	**Bemerkung**
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'14' = 20	
encKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTUAL AUTHENTICATE	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 34:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	NEVER	

[<=]

Hinweis 33: Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, GET SECURITY STATUS KEY, INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE, TERMINATE.

Hinweis 34: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5:

Card-G2-A_3358 - K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128
Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES128 die in Tab_SMC-B_ObjSys_086 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 26: Tab_SMC-B_ObjSys_086 Personalisierte Attribute von MF / SK.CMS.AES128

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

[<=]

5.3.13.2 MF / SK.CMS.AES256

SK.CMS.AES256 (optional) ist der geheime Schlüssel für die Durchführung des SMC-B / CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.

Card-G2-A_2195-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256
SK.CMS.AES256 MUSS die in Tab_SMC-B_ObjSys_034 dargestellten Werte besitzen.

Tabelle 27: Tab_SMC-B_ObjSys_034 Initialisierte Attribute von MF / SK.CMS.AES256

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	‘18’ = 24	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert

numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTUAL AUTHENTICATE	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 34:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Card-G2-A_3359 - K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256
Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES256 die in Tab_SMC-B_ObjSys_087 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 28: Tab_SMC-B_ObjSys_087 Personalisierte Attribute von MF / SK.CMS.AES256

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

[<=]

5.3.13.3 MF / SK.CUP.AES128

Dieser AES-Schlüssel mit 128 bit Schlüssellänge wird benötigt, um dem CUPS administrative Zugriffe auf die SMC-B bezüglich der Zertifikate zu erlauben.

Card-G2-A_3360-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128

SK.CUP.AES128 MUSS die in Tab_SMC-B_ObjSys_113 dargestellten Initialisierten Attribute besitzen.

Tabelle 29: Tab_SMC-B_ObjSys_113 Initialisierte Attribute von MF / SK.CUP.AES128

Attribute	**Wert**	**Bemerkung**
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'03' = 3	
lifeCycleStatus	„Operational state (activated)“	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
accessRuleSessionkeys	irrelevant	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTUAL AUTHENTICATE	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 34:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Card-G2-A_3361 - K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128
Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CUP.AES128 die in Tab_SMC-B_ObjSys_114 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 30: Tab_SMC-B_ObjSys_114 Personalisierte Attribute von MF / SK.CUP.AES128

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

[<=]

5.3.13.4 MF / SK.CUP.AES256

Dieser AES-Schlüssel mit 256 bit Schlüssellänge wird benötigt, um dem CUPS administrative Zugriffe auf die SMC-B bezüglich der Zertifikate zu erlauben.

Card-G2-A_3362-01 - K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256
SK.CUP.AES256 MUSS die in Tab_SMC-B_ObjSys_115 dargestellten Initialisierten Attribute besitzen.

Tabelle 31: Tab_SMC-B_ObjSys_115 Initialisierte Attribute von MF / SK.CUP.AES256

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	'04' = 4	
lifeCycleStatus	„Operational state (activated)“	
encKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
macKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
accessRuleSessionkeys	irrelevant	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
MUTUAL AUTHENTICATE	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 34:
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Card-G2-A_3363 - K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256
Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CUP.AES256 die in Tab_SMC-B_ObjSys_116 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 32: Tab_SMC-B_ObjSys_116 Personalisierte Attribute von MF / SK.CUP.AES256

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

[<=]

5.4 Die ESIGN-Anwendung DF.ESIGN

5.4.1 Dateistruktur und Dateiinhalt

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

- die Berechnung einer Organisationssignatur (die Signatur ist an die entsprechende Institution im Gesundheitswesen gebunden, nicht an eine einzelne Person, siehe Abbildung 2.
- die Client/Server-Authentisierung z.B. zur Verbindung der Institution im Gesundheitswesen oder eines Teils dieser Institution mit dem VPN des Gesundheitswesens und
- die Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels zur vertraulichen Weitergabe von Dokumenten, welche an die entsprechende Institution im Gesundheitswesen und nicht an eine einzelne Person adressiert sind.

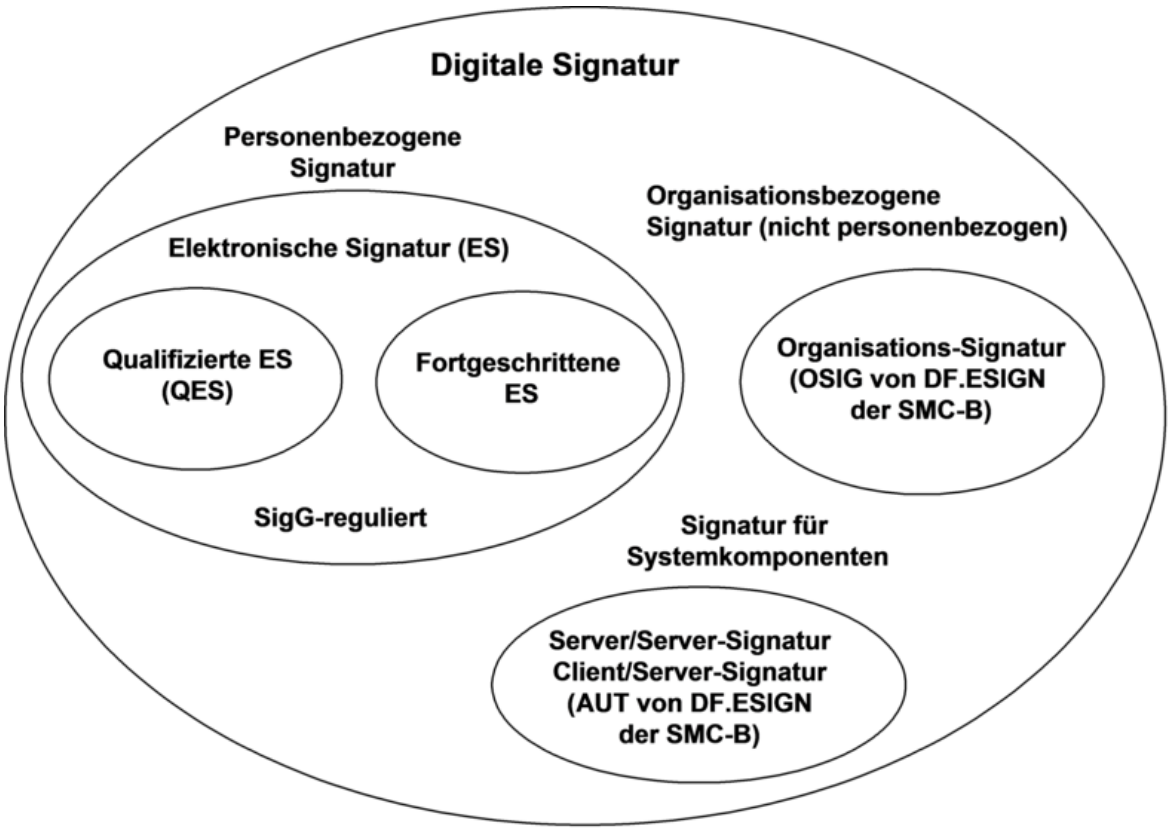

Abbildung 2: (Abb_SMC-B_ObjSys_003) Arten der digitalen Signatur

5.4.2 MF / DF.ESIGN (Krypto-Anwendung ESIGN)

Abbildung 3 zeigt die prinzipielle Dateistruktur der ESIGN-Anwendung gemäß EN14890.

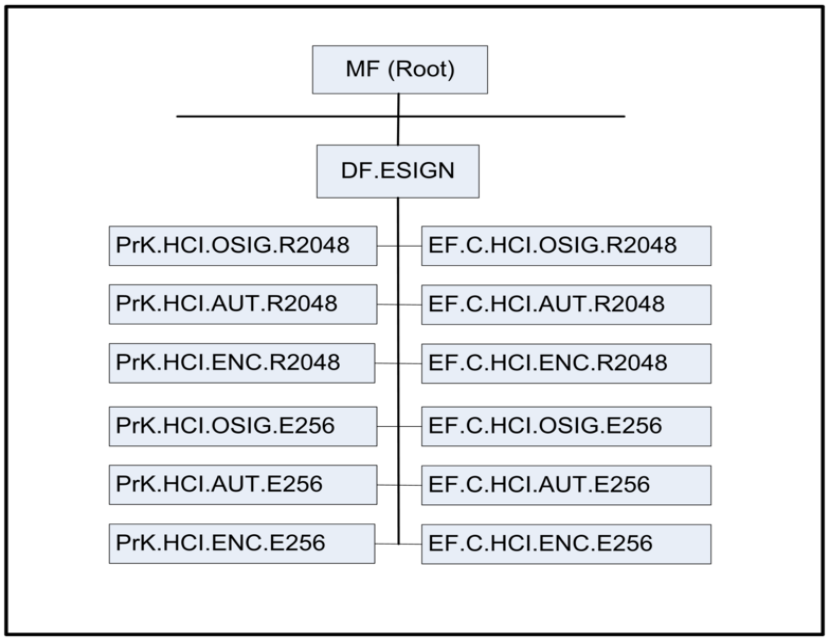

Abbildung 3: (Abb_SMC-B_ObjSys_004) Allgemeine Struktur von MF / DF.ESIGN

Card-G2-A_2203 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN
DF.ESIGN MUSS die in Tab_SMC-B_ObjSys_040 dargestellten Werte besitzen.

Tabelle 33: Tab_SMC-B_ObjSys_040 Initialisierte Attribute von MF / DF.ESIGN

Attribute	**Wert**	**Bemerkung**
Objekttyp	Ordner	
applicationIdentifier	'A000000167 455349474E'	siehe Hinweis 47:
fileIdentifier	–	siehe Hinweis 48:
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 50:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	herstellerspezifisch	

[<=]

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

Hinweis 36: Der Wert des Attributes applicationIdentifier ist in [EN14890-1]festgelegt.

Hinweis 37: herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1]

Hinweis 38: Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, ist dieser Zustand für Objekte im Kapitel 5.4 im Allgemeinen irrelevant.

Hinweis 39: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.5:

5.4.2.1 MF / DF.ESIGN / EF.C.HCI.OSIG.R2048

EF.C.HCI.OSIG.R2048 enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.HCI.OSIG.R2048 zu PrK.HCI.OSIG.R2048 (siehe Kapitel 5.4.2.4).

Card-G2-A_2204 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048
EF.C.HCI.OSIG.R2048 MUSS die in Tab_SMC-B_ObjSys_041 dargestellten Werte besitzen.

Tabelle 34: Tab_SMC-B_ObjSys_041 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'C0 00'	
shortFileIdentifier	'10'= 16	
numberOfOctet	'07 6C' Oktett = 1900 Oktett	
positionLogicalEndOfFile	'0'	wird personalisiert
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 52:

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 40: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 41: Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.5:

Card-G2-A_3371 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048
Bei der Personalisierung von EF.C.HCI.OSIG.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_092 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 35: Tab_SMC-B_ObjSys_092 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HCI.OSIG.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HCI.OSIG.R2048	

[<=]

5.4.2.2 MF / DF.ESIGN / EF.C.HCI.AUT.R2048

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.HCI.AUT.R2048 zu PrK.HCI.AUT.R2048 (siehe Kapitel 5.4.2.5).

Card-G2-A_2207 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048
EF.C.HCI.AUT.R2048 MUSS die in Tab_SMC-B_ObjSys_042 dargestellten Werte besitzen.

Tabelle 36: Tab_SMC-B_ObjSys_042 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C5 00’	
shortFileIdentifier	‘01’= 1	
numberOfOctet	‘07 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	wird personalisiert
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 54:
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 54:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 42: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 43: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5:

Card-G2-A_3365 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048
Bei der Personalisierung von EF.C.HCI.AUT.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_094 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 37: Tab_SMC-B_ObjSys_094 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HCI.AUT.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HCI.AUT.R2048	

[<=]

5.4.2.3 MF / DF.ESIGN / EF.C.HCI.ENC.R2048

Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.HCI.ENC.R2048. Das zugehörende private Schlüsselobjekt PrK.HCI.ENC.R2048 ist in Kapitel 5.4.2.6 definiert.

Card-G2-A_2210-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048
EF.C.HCI.ENC.R2048 MUSS die in Tab_SMC-B_ObjSys_043 dargestellten Werte besitzen.

Tabelle 38: Tab_SMC-B_ObjSys_043 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C2 00’	
shortFileIdentifier	‘02’= 2	
numberOfOctet	‘07 6C’ Oktett = 1900 Oktett	
positionLogicalEndOfFile	’0’	wird personalisiert
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 45:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 44: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Hinweis 45: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.5:

Card-G2-A_3366 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048
Bei der Personalisierung von EF.C.HCI.ENC.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_096 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 39: Tab_SMC-B_ObjSys_096 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HCI.ENC.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HCI.ENC.R2048	

[<=]

5.4.2.4 MF / DF.ESIGN / PrK.HCI.OSIG.R2048

PrK.HCI.OSIG.R2048 ist der private Schlüssel zur Berechnung einer Organisationssignatur. Der zugehörige öffentliche Schlüssel PuK.HCI.OSIG.R2048 ist in C.HCI.OSIG.R2048 (siehe Kapitel 5.4.2.1) enthalten.

Card-G2-A_2217-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048
PrK.HCI.OSIG.R2048 MUSS die in Tab_SMC-B_ObjSys_044 dargestellten Werte besitzen.

Tabelle 40: Tab_SMC-B_ObjSys_044 Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	‘04’ = 4	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz	wird personalisiert

	hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO COMPUTE DIGITAL SIGNATURE	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 47:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Hinweis 46: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 47: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.5:

Card-G2-A_3367 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048

Bei der Personalisierung von PrK.HCI.OSIG.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_100 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 41: Tab_SMC-B_ObjSys_100 Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	

keyAvailable	True	

[<=]

5.4.2.5 MF / DF.ESIGN / PrK.HCI.AUT.R2048

PrK.HCI.AUT.R2048 ist der private Schlüssel für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HCI.AUT.R2048 ist in C.HCI.AUT.R2048 (siehe Kapitel 5.4.2.2) enthalten.

Card-G2-A_2220-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048
PrK.HCI.AUT.R2048 MUSS die in Tab_SMC-B_ObjSys_047 dargestellten Werte besitzen.

Tabelle 42: Tab_SMC-B_ObjSys_047 Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	‘02’ = 2	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
INTERNAL AUTHENTICATE PSO Comp Dig Sig	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 49:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	NEVER	

[<=]

Hinweis 48: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Hinweis 49: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.5:

Card-G2-A_3368 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048
Bei der Personalisierung von PrK.HCI.AUT.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_103 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 43: Tab_SMC-B_ObjSys_103 Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit]	
keyAvailable	True	

[<=]

5.4.2.6 MF / DF.ESIGN / PrK.HCI.ENC.R2048

PrK.HCI.ENC.R2048 ist der private Schlüssel für den PKI-Dienst zur Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC.R2048 ist in C.HCI.ENC.R2048 (siehe Kapitel 5.4.2.3) enthalten.

Card-G2-A_2223 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048
PrK.HCI.ENC.R2048 MUSS die in Tab_SMC-B_ObjSys_050 dargestellten Werte besitzen.

Tabelle 44: Tab_SMC-B_ObjSys_050 Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Entschlüsselungsobjekt	
keyIdentifier	‘03’ = 3	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe	

	[gemSpec_COS] {rsaDecipherOaep}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO Decipher PSO Transcipher	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 62:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Hinweis 50: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Entschlüsselungsobjekt arbeiten, sind:
PSO DECIPHER, PSO TRANSCIPHER

Hinweis 51: Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.5:

Card-G2-A_3369 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048
Bei der Personalisierung von PrK.HCI.ENC.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_106 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 45: Tab_SMC-B_ObjSys_106 Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	
keyAvailable	True	

[<=]

5.4.2.7 MF / DF.ESIGN / EF.C.HCI.OSIG.E256

Die Datei EF.C.HCI.OSIG.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.HCI.OSIG.E256. Das zugehörende private Schlüsselobjekt PrK.HCI.OSIG.E256 ist in Kapitel 5.4.2.10 definiert.

Card-G2-A_3652 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.E256
EF.C.HCI.OSIG.E256 MUSS die in Tab_SMC-B_ObjSys_120 dargestellten initialisierten Attribute besitzen.

Tabelle 46: Tab_SMC-B_ObjSys_120 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'C0 07'	
shortFileIdentifier	'07'= 7	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	True	
flagChecksum	False	
numberOfOctet	'0B B8' Oktett = 3000 Oktett	
positionLogicalEndOfFile	'0'	wird personalisiert
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 41:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 52: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Card-G2-A_3653 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.E256
Bei der Initialisierung von EF.C.HCI.OSIG.E256 MÜSSEN die in Tab_SMC-B_ObjSys_121 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 47: Tab_SMC-B_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.HCI.OSIG.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HCI.OSIG.E256	

[<=]

5.4.2.8 MF / DF.ESIGN / EF.C.HCI.AUT.E256

Die Datei EF.C.HCI.AUT.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.HCI.AUT.E256. Das zugehörende private Schlüsselobjekt PrK.HCI.AUT.E256 ist in Kapitel 5.4.2.11 definiert.

Card-G2-A_3654 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.E256
EF.C.HCI.AUT.E256 MUSS die in Tab_SMC-B_ObjSys_122 dargestellten initialisierten Attribute besitzen.

Tabelle 48: Tab_SMC-B_ObjSys_122 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C5 06’	
shortFileIdentifier	‘06’= 6	
lifeCycleStatus	„Operational state (activated)“	
flagTransactionMode	True	
flagChecksum	False	
numberOfOctet	‘0B B8’ Oktett = 3000 Oktett	
positionLogicalEndOfFile	’0’	wird personalisiert
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 43:
READ BINARY	ALWAYS	

SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 43:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 53: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Card-G2-A_3655 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.E256
Bei der Initialisierung von EF.C.HCI.AUT.E256 MÜSSEN die in Tab_SMC-B_ObjSys_123 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 49: Tab_SMC-B_ObjSys_123 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.AUT.E256

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

[<=]

5.4.2.9 MF / DF.ESIGN / EF.C.HCI.ENC.E256

Die Datei EF.C.HCI.ENC.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.HCI.ENC.E256. Das zugehörende private Schlüsselobjekt PrK.HCI.ENC.E256 ist im Kapitel 5.4.2.12 definiert.

Card-G2-A_3656 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.E256
EF.C.HCI.ENC.E256 MUSS die in Tab_SMC-B_ObjSys_124 dargestellten initialisierten Attribute besitzen.

Tabelle 50: Tab_SMC-B_ObjSys_124 Initialisierte Attribute von MF / DF.ESIGN/ EF.C.HCI.ENC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	

fileIdentifier	'C2 05'	
shortFileIdentifier	'05'= 5	
lifeCycleStatus	„Operational state (activated)"	
flagTransactionMode	True	
flagChecksum	False	
numberOfOctet	'0B B8' Oktett = 3000 Oktett	
positionLogicalEndOfFile	'0'	wird personalisiert
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
READ BINARY	ALWAYS	
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 45:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	

[<=]

Hinweis 54: Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, READ BINARY, SELECT, SET LOGICAL EOF, UPDATE BINARY, TERMINATE, WRITE BINARY

Card-G2-A_3657 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HCI.ENC.E256

Bei der Initialisierung von EF.C.HCI.ENC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_125 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 51: Tab_SMC-B_ObjSys_125 Personalisierte Attribute von MF / DF.ESIGN/ EF.C.HCI.ENC.E256

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

	PrK.HCI.ENC.E256	

[<=]

5.4.2.10 MF / DF.ESIGN / PrK.HCI.OSIG.E256

PrK.HCI.OSIG.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HCI.OSIG.E256 ist in C.HCI.OSIG.E256 (siehe Kapitel 5.5.2.7) enthalten.

Card-G2-A_3658-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E256
PrK.HCI.OSIG.E256 MUSS die in Tab_SMC-B_ObjSys_126 dargestellten, initialisierten Attribute besitzen.

Tabelle 52: Tab_SMC-B_ObjSys_126 Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E256

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'07' = 7	
lifeCycleStatus	„Operational state (activated)"	
privateElcKey	*domainparameter = brainpoolP256r1*	wird personalisiert
privateElcKey	*keyData = AttributNotSet*	
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {signECDSA}	
accessRuleSessionkeys	irrelevant	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO COMPUTE DIGITAL SIGNATURE	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 47:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**

alle	NEVER	

[<=]

Hinweis 55: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Card-G2-A_3659 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E256
Bei der Personalisierung von PrK.HCI.OSIG.E256 MÜSSEN die in Tab_SMC-B_ObjSys_127 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 53: Tab_SMC-B_ObjSys_127 Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.OSIG.E256

Attribute	Wert	Bemerkung
keyAvailable	true	
privateElcKey	keyData = Wildcard	

[<=]

5.4.2.11 MF / DF.ESIGN / PrK.HCI.AUT.E256

PrK.HCI.AUT.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HCI.AUT.E256 ist in C.HCI.AUT.E256 (siehe Kapitel 5.5.2.8) enthalten.

Card-G2-A_3660-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E256
PrK.HCI.AUT.E256 MUSS die in Tab_SMC-B_ObjSys_128 dargestellten initialisierten Attribute besitzen.

Tabelle 70: Tab_SMC-B_ObjSys_128 Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	‘06’ = 6	
lifeCycleStatus	„Operational state (activated)“	
privateElcKey	*domainparameter = brainpoolP256r1*	wird personalisiert
privateElcKey	*keyData = AttributNotSet*	
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {signECDSA}	
accessRuleSessionkeys	irrelevant	

Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
INTERNAL AUTHENTICATE PSO Comp Dig Sig	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 49:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

Hinweis 56: Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, EXTERNAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, INTERNAL AUTHENTICATE, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, TERMINATE

Card-G2-A_3661 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E256
Bei der Personalisierung von PrK.HCI.AUT.E256 MÜSSEN die in Tab_SMC-B_ObjSys_129 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 71: Tab_SMC-B_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.AUT.E256

Attribute	Wert	Bemerkung
keyAvailable	true	
privateElcKey	keyData = Wildcard	

[<=]

5.4.2.12 MF / DF.ESIGN / PrK.HCI.ENC.E256

PrK.HCI.ENC.E256 ist der private Schlüssel für die Kryptographie mit ellptischen Kurven für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Der zugehörige öffentliche Schlüssel PuK.HCI.ENC.E256 ist in C.HCI.ENC.E256 (siehe Kapitel 5.5.2.9) enthalten.

Card-G2-A_3662-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.E256
PrK.HCI.ENC.E256 MUSS die in Tab_SMC-B_ObjSys_139 dargestellten initialisierten Attribute besitzen.

Tabelle 72: Tab_SMC-B_ObjSys_130 Initialisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.E256

Attribute	**Wert**	**Bemerkung**
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'05' = 5	
lifeCycleStatus	„Operational state (activated)"	
privateElcKey	*domainparameter = brainpoolP256r1*	wird personalisiert
privateElcKey	*keyData = AttributNotSet*	
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {elcSharedSecretCalculation}	
accessRuleSessionkeys	irrelevant	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
PSO DECIPHER PSO TRANSCIPHER	PWD(PIN.SMC)	Die Zugriffsregel für PIN.SMC ist auf MF-Ebene definiert.
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 51:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	**Zugriffsbedingung**	**Bemerkung**
alle	NEVER	

[<=]

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

Card-G2-A_3663 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.E256
Bei der Personalisierung von PrK.HCI.ENC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_131 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 73: Tab_SMC-B_ObjSys_131 Personalisierte Attribute von MF / DF.ESIGN / PrK.HCI.ENC.E256

Attribute	Wert	Bemerkung
keyAvailable	true	
privateElcKey	keyData = Wildcard	

[<=]

5.5 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der SMC-B

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien EF.DIR und EF.Version2) oder das Nachladen von Zertifikaten oder das Generieren und Sperren von Schlüsseln nach der Ausgabe der SMC-B von einem Card Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CMS optional. Die Inhalte des Kapitels 14.2.5 in [gemSpec_COS] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe der SMC-B durchgeführt werden müssen.

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AID	Application Identifier (Anwendungskennung)
APDU	Application Protocol Data Unit [ISO7816-3][ISO7816-3]
ASN.1	Abstract Syntax Notation One
ATR	Answer-to-Reset
AUT	Authentisierung
AUTD	CV-basierte Geräteauthentisierung
AUTR	CV-basierte Rollenauthentisierung
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
C	Zertifikat
C2C	Card to Card
CA	Certification Authority (Zertifizierungsdiensteanbieter)
CMS	Card Management System
CAR	Certification Authority Reference
CC	Cryptographic Checksum (kryptographische Prüfsumme)
CER	Canonical Encoding Rules
CH	Cardholder (Karteninhaber)
CHAT	Certificate Holder Autorisation Template
	Liste von Rechten, die ein Zertifikatsinhaber besitzt

COS	Card Operating System (Chipkartenbetriebssystem)
CPI	Certificate Profile Identifier
CRL	Certificate Revocation List (Zertifikatssperrliste)
CUP	Certificate Update
CV	Card Verifiable
CVC	Card Verifiable Certificate
D,DIR	Directory
DER	Distinguished Encoding Rules
DES	Daten Encryption Standard
DF	Dedicated File
DO	Datenobjekt
DS	Digital Signature
DSI	Digital Signature Input
DTBS	Data to be signed
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
eGK	elektronische Gesundheitskarte
ELC	Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven
ENC	Encryption
FCI	File Control Information
FCP	File Control Parameter
FI	Clock rate conversion factor
FID	File Identifier
GDO	Global Data Object
GKV	Gesetzliche Krankenversicherung

GP	Global Platform
HB	Historical Bytes
HBA	Heilberufsausweis (Health Professional Card)
HCI	Health Care Institution (Institution des Gesundheitswesens)
HP	Health Professional (Heilberufler)
HPC	Health Professional Card (Heilberufsausweis)
ICC	Integrated Circuit Card (Chipkarte)
ICCSN	ICC Serial Number (Chipkarten-Seriennummer)
ICM	IC Manufacturer (Kartenhersteller)
ID	Identifier
IIN	Issuer Identification Number
KeyRef	Key Reference
KM	Komfortmerkmal
KT	Karten-Terminal
LCS	Life Cycle Status
LSB	Least Significant Byte(s)
MAC	Message Authentication Code
MF	Master File
MII	Major Industry Identifier
MSE	Manage Security Environment
OCSP	Online Certificate Status Protocol
OD	Object Directory
OID	Object Identifier
OSIG	Organisationssignatur
PIN	Personal Identification Number

PIX	Proprietary Application Provider Extension
PK, PuK	Public Key
PKCS	Public Key Cryptography Standard (hier[PKCS#1])[PKCS#1]
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates (IETF)
PP	Protection Profile (Schutzprofil)
PrK	Private Key
PSO	Perform Security Operation
PUK	Personal Unblocking Key (Resetting Code)
PV	Plain Value
P1	Parameter P1 einer Kommando-APDU
P2	Parameter P2 einer Kommando-APDU
RA	Registration Authority (Registrierungsinstanz)
RAM	Random Access Memory
RC	Retry Counter (Fehlbedienungszähler)
RCA	Root CA
RFC	Request für Comment
RFID	Radio Frequency Identification
RFU	Reserved for future use
RND	Random Number (Zufallszahl)
ROM	Read Only Memory
RPE	Remote PIN-Empfänger
RPS	Remote PIN-Sender
RSA	Algorithmus von Rivest, Shamir, Adleman [RSA][RSA]
SE	Security Environment (Sicherheitsumgebung)

SFID	Short EF Identifier
SIG	Signatur
SK	Secret Key
SM	Secure Messaging
SMC	Security Module Card
SMD	Security Module Data
SSEE	Sichere Signaturerstellungseinheit
SSL	Security Sockets Layer
TLV	Tag Length Value
TC	Trusted Channel
TLS	Transport Layer Security
ZDA	Zertifizierungsdiensteanbieter
3TDES	3-Key-Triple-DES

6.2 Glossar

Das Glossar der Telematikinfrastruktur wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

6.3 Abbildungsverzeichnis

6.4 Tabellenverzeichnis

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS) (elektrische Schnittstelle)
[gemSpec_Karten_Fach_TIP_G2.1]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1
[gemSpec_PINPUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI
[gemSpec_CVC_Root]	gematik: Spezifikation CVC - Root
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_TK]	gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2
[gemSpec_SMC_OPT]	gematik: Gemeinsame optische Merkmale der SMC

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[EN14890-1]	EN 14890-1: 2008 Application Interface for smart cards used as secure signature creation devices, Part 1: Basic services
[DIN_EN_1867]	EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers
[ISO3166-1]	ISO/IEC 3166-1: 2006 Codes for the representations of names of countries and their subdivisions – Part 1: Country codes
[ISO7816-3]	ISO/IEC 7816-3: 2006 Identification cards - Integrated circuit cards with contacts - Part 3: Electrical interface and transmission protocols
[ISO7816-4]	ISO/IEC 7816-4: 2005 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ISO8825-1]	ISO/IEC 8825-1: 2002 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
[PKCS#1]	PKCS #1 RSA Cryptography Standard V2.1: June 14, 2002
[Beschluss190]	Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte
[RFC2119]	Network Working Group, Request for Comments: 2119, S. Bradner Harvard, University, March 1997, Category: Best Current Practice Key words for use in RFCs to Indicate Requirement Levels http://www.apps.ietf.org/rfc/rfc2119.html
[RSA]	R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21 No. 2, 1978
[SD5]	ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19 Register of IC manufacturers http://www.pkicc.de/cms/media/pdfs/IC_manufacturer_ISO_SD5_1962006.pdf