gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation der gSMC-KT

Objektsystem

Version:	3.9.0
Revision:	\main\rel_online\rel_ors1\rel_opb1\11
Stand:	24.08.2016
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_gSMC-KT_ObjSys]

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.9.15	05.06.12		Erstellung der Spezifikation für Generation 2	PL P71
3.0.0.	19.09.12		freigegeben	gematik
3.1.0	17.01.13		Harmonisierung mit der Struktur der anderen ObjSys-Spezifikationen	PL P71
3.2.0 RC	13.11.13		Fehlerkorrekturen, AFO Card-G2-A_2520 und AFO Card-G2-A_2521 gestrichen, AFOs zu *persisten-PublicKeyList* hinzugefügt, Attribut *shareable* wurde für alle Ordner und Date ien hinzugefügt, Ändern der Flaglist-Darstellung, Bearbeitung gemäß Kommentaren, Aufnahme des Kommandos LIST PUBLIC KEY FÜR MF, Einfügen Kommando TERMINATE für Schlüssel, bei denen es noch nicht vorgesehen war	gematik
3.3.0 RC	19.12.13		Zuordnung der AFOs zu Initialisierung und Personalisierung, Umstrukturierung der Option Lange Lebensdauer, Überarbeitung der Struktur, Einfügen von EF.KeyInfo, Modifizieren von EF.ATR, EF.DIR und EF.Version, Einfügen Option Testkarten, Modifizieren von EF.GDO,	gematik
3.4.0	21.02.14		Einfügen einer Liste offener Punkte, Einfügen der Option_PACE_PCD (optional), Kommentare, Expiration Date für Sicherheitsanker festgelegt, Kommentare Iteration 2b	gematik
3.5.0	27.03.14		Einarbeitung Fehlerkorrektur Iteration 2b	gematik
3.6.0	06.06.14		Einarbeitung Änderungen Iteration 3	gematik
3.7.0	26.08.14		Einarbeitung weitere Änderungen Iteration 3, Änderungen Iteration 4	gematik
3.8.0	17.07.15		Folgende Errata eingearbeitet: R.1.4.1, R1.4.2, R1.4.3	Technik / SPE
3.8.9	18.12.15		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
3.9.0	24.08.16		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Dieses Dokument spezifiziert die Objektstruktur der gSMC-KT und definiert die Anforderungen an die Kartenschnittstelle zur gerätespezifischen Security Module Card Typ KT (gSMC-KT) zum Einsatz in eHealth-Kartenterminals.

Es werden die anwendungsspezifischen Strukturen der gSMC-KT, die bei der Initialisierung und Personalisierung in die gSMC-KT geladen werden sowie die Zugriffsrechte auf Elemente der gSMC-KT festgelegt.

Die Spezifikation behandelt Anwendungen der gSMC-KT unter den folgenden, rein kartenorientierten Gesichtspunkten:

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

Somit definiert dieses Dokument eine Reihe von Datencontainern, Schlüsselobjekten und Passwörtern. Zudem werden hier die Sicherheitsmechanismen für diese Objekte festgelegt, d. h. es wird festgelegt, welchen Instanzen es unter welchen Voraussetzungen möglich ist, auf Inhalte der Container zuzugreifen, Operationen mit den Schlüsselobjekten durchzuführen etc. Die Semantik und die Syntax der Inhalte in Datencontainern ist dagegen nicht Gegenstand dieses Dokumentes.

1.2 Zielgruppe

Das Dokument richtet sich an

- Hersteller, welche die hier spezifizierten Anwendungen herstellerspezifisch für eine bestimmtes Chipkartenbetriebssystem umsetzen,
- Kartenherausgeber, die anhand der hier spezifizierten Anwendungen die elektrische Personalisierung eines Sicherheitsmoduls für Kartenterminals planen,
- Hersteller von Systemen, die Programme entwickeln, welche unmittelbar mit der Chipkarte kommunizieren,
- Kartenterminalhersteller.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren

Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung des Dokuments

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

Im Teil „Gemeinsame optische Merkmale der SMC“ (siehe [gemSpec_SMC_OPT]) wird die optische Gestaltung für alle SMCs und damit auch für die gSMC-KT festgelegt.

1.5 Methodik

1.5.1 Nomenklatur

Dieses Dokument verwendet dieselbe Nomenklatur wie [gemSpec_COS].

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

In [gemSpec_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 definiert.

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

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

Beispiele:

Langform	**Kurzform**
Informativ: AUT(CHA.1)	C.1
Informativ: AUT(CHA.7)	C.7
Informativ: AUT(CHA.2) OR AUT(CHA.3)	C.2.3
Informativ: PWD(PIN) AND [AUT(CHA.2) OR AUT(CHA.3)]	PWD(PIN) AND [C.2.3]
AUT(oid_cvc_fl_cms,'00010000000000')	flagCMS.15
AUT(oid_cvc_fl_ti, '00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')	flagTI.15 OR flagTI.16
PWD(PIN) AND [AUT(oid_cvc_fl_cms,'00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')]	PWD(PIN) AND [flagCMS.15 OR flagTI.16)]
SmMac(oid_cvc_fl_cms, '00800000000000')	SmMac(flagCMS.08)

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:

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

⌦ **Card-G2-A_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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_gSMC-KT_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_COS	Betriebssystem einer Smartcard
K_Terminal	eHealth-Kartenterminal

2 Optionen

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

2.1 Lange Lebensdauer im Feld

Card-G2-A_3018 Option_lange_Lebensdauer_im_Feld

Falls beabsichtigt ist, eine gSMC-KT länger als die Nutzungsdauer eines kryptographischen Schlüssels im Feld zu nutzen, sind zusätzliche Zertifikats- und Schlüsselobjekte anzulegen. Die dazugehörenden Schlüssellängen entsprechen der nächsten Stufe im jeweiligen Verfahren, also R3072 beim RSA-Verfahren und E384 bei ELC.

Die gSMC-KT KANN die Option_lange_Lebensdauer_im_Feld unterstützen.⌫

Card-G2-A_3019 Vorgaben für die Option_lange_Lebensdauer_im_Feld

Falls eine gSMC-KT die Option_lange_Lebensdauer_im_Feld

1. unterstützt, dann MÜSSEN zusätzlich zu allen nicht gekennzeichneten Anforderungen auch alle Anforderungen erfüllt werden, die mit Option_lange_Lebensdauer_im_Feld gekennzeichnet sind.
2. nicht unterstützt, dann DÜRFEN mit Option_lange_Lebensdauer_im_Feld gekennzeichnete Anforderungen NICHT relevant für funktionale Tests sein. ⌫

2.2 Kartenadministration

In den Kapiteln 5.4.14 und 5.4.15 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen einem Kartenadministrationssystem (z.B. einem CMS) und einer Karte beschrieben.

Card-G2-A_3024 K_Personalisierung Auswahl der Absicherung der Kartenadministration

Wenn die gSMC-KT Online administriert werden soll und die Option_lange_Lebensdauer_im_Feld nicht genutzt werden soll, MUSS ein Kartenherausgeber bei der Personalisierung Schlüssel für mindestens eines der beiden Verfahren

a. symmetrische Authentifizierung (SK.CMS und SK.CUP)
b. asymmetrische Authentifizierung (PuK.RCA.ADMIN.CS)

in die Karte einbringen und sicherstellen, dass das dazugehörende Kartenadministrationssystem (z.B. ein CMS oder ein CUpS) über die entsprechenden Schlüssel verfügt.

Wenn für die gSMC-KT die Option_lange_Lebensdauer_im_Feld genutzt werden soll, MUSS ein Kartenherausgeber bei der Personalisierung einen Schlüssel für die

asymmetrische Authentifizierung in die Karte einbringen und sicherstellen, dass das dazugehörende Kartenadministrationssystem (z.B. ein CMS oder ein CUpS) über den dazugehörenden Schlüssel verfügt. ⌫

⌦ **Card-G2-A_3470 K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten**

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

3 Lebenszyklus von Karte und Applikation

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

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

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 erforderlich, welches folgende Optionen enthält:

- Unterstützung von mindestens vier logischen Kanälen.
- Unterstützung der Kryptobox-Funktionalität.

4.1 Mindestanzahl logischer Kanäle

⌦ **Card-G2-A_2475 K_Initialisierung: Anzahl logischer Kanäle**

Für die Anzahl logischer Kanäle, die von einer gSMC-KT zu unterstützen ist, gilt:

a) Die maximale Anzahl logischer Kanäle MUSS gemäß [ISO7816-4#Tab.88] in den Historical Bytes in EF.ATR angezeigt werden.

b) Die gSMC-KT 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. ⌫

4.2 Kryptobox

⌦ **Card-G2-A_2876 K_gSMC-KT: Kryptobox**

Für das Objektsystem der gSMC-KT MUSS ein COS verwendet werden, das die Kryptobox implementiert hat.⌫

4.3 Optionale Funktionspakete

4.3.1 Kontaktlose Schnittstelle

⌦ **Card-G2-A_2476 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 gSMC-K NICHT genutzt werden.⌫

4.3.2 USB-Schnittstelle (optional)

⌦ **Card-G2-A_3026 K_gSMC-KT: USB-Schnittstelle**

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

⌦ **Card-G2-A_2877 K_gSMC-KT: Vorhandensein einer USB-Schnittstelle**

Falls eine gSMC-K 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.⌫

4.3.3 Option_PACE_PCD (optional)

⌦ **Card-G2-A_3473 K_gSMC-KT: Option_PACE_PCD**

Falls eine gSMC-KT die Option_PACE_PCD nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_PACE_PCD implementiert hat.⌫

4.4 Attributstabellen

⌦ **Card-G2-A_2469 K_Initialisierung: Änderung von Zugriffsregeln**

Die in diesem Dokument definierten Zugriffsregeln DÜRFEN in der Nutzungsphase NICHT veränderbar sein.⌫

Dieses Dokument legt das Verhalten aller Objekte im Security Environment SE#1 normativ fest. Das Verhalten in Security Environments mit einer anderen Nummer als SE#1 wird durch dieses Dokument nicht festgelegt.

Alle Angaben zu Objekten (Ordnern, Dateien, Passwörtern und Schlüsseln) in diesem Dokument beziehen sich ausschließlich auf das Security Environment SE#1.

⌦ **Card-G2-A_2470 K_Initialisierung: Verwendung von SE**

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

⌦ **Card-G2-A_3194 K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs**

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

⌦ **Card-G2-A_3195 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.⌫

4.4.1 Attribute eines Ordners

⌦ **Card-G2-A_2472 K_Initialisierung: Ordnerattribute**

Enthält eine Tabelle mit Ordnerattributen

- keinen *applicationIdentifier* (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.
- einen oder mehrere AID, dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
- keinen *fileIdentifier* (FID),

- so DARF dieser Ordner NICHT mittels eines *fileIdentifiers* 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.
- so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden.⌫

4.4.2 Attribute einer Datei (EF)

⌦ **Card-G2-A_2473 K_Initialisierung: SFID nicht vorhanden**

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_2849 K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile"**

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

4.5 Zugriffsregeln für besondere Kommandos

Gemäß [gemSpec_COS] wird festgelegt:

⌦ **Card-G2-A_2474 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. ⌫

4.6 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_3276 K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung

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

5 Dateisystem der gSMC-KT

Zu den grundlegenden Applikationen der Sicherheitsmodulkarte gSMC-KT zählen:

- das Wurzelverzeichnis, auch *root* oder Master File (MF) genannt und
- die Kartenterminalanwendung DF.KT mit Schlüsselmaterial und Zertifikaten zum Aufbau einer sicheren Verbindung zwischen Konnektor und Kartenterminal.

⌦ **Card-G2-A_2477 K_Personalisierung: weitere Applikationen**

Die Komponente gSMC-KT KANN Applikationen enthalten, die in diesem Dokument nicht genannt sind.⌫

⌦ **Card-G2-A_2478 K_Personalisierung: Zusätzliche Objekte**

Jeder Ordner, der in diesem Dokument spezifiziert ist, KANN zusätzliche Objekte (Ordner, Dateien, Passwörter oder Schlüssel) enthalten.⌫

5.1 Attribute des Objektsystems

Das Objektsystem der Komponente gSMC-KT enthält gemäß [gemSpec_COS] folgende Attribute:

⌦ **Card-G2-A_3273 K_Initialisierung: Wert des Attributes *root***

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

⌦ **Card-G2-A_3274 K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset**

Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A_2481, Card-G2-A_2482, Card-G2-A_3027 und Card-G2-A_2483 entsprechen. ⌫

⌦ **Card-G2-A_2479 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_3196 K_Initialisierung: Inhalt persistentPublicKeyList**

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

⌦ **Card-G2-A_3197 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_3269 K_Initialisierung: Wert von *pointInTime***

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

⌦ **Card-G2-A_3515 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.⌫

5.2 ATR-Kodierung und technische Eigenschaften

Für die gSMC-KT gelten die Konventionen für die technischen Eigenschaften, ATR und Übertragungs¬protokolle aus [gemSpec_COS] für die elektrische Schnittstelle. Die gSMC-KT ist als Plug-In-Karte (ID-000) für die Nut¬zung in entsprechenden Kartenterminals vorgesehen.

⌦ **Card-G2-A_2481 K_Personalisierung und K_Initialisierung: ATR-Kodierung**

Die ATR-Kodierung MUSS die in Tab_gSMC-KT_ObjSys_002 dargestellten Werte besitzen.

Tabelle 2: Tab_gSMC-KT_ObjSys_002 ATR-Kodierung

Zeichen	Wert	Bedeutung
TS	‘3B’	Initial Character (direct convention)
T0	‘9x’	Format Character (TA1/TD1 indication, x = no. of HB)
TA1	‘xx’	Interface Character (FI/DI, erlaubte Werte: siehe gemSpec_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_2482 K_Personalisierung und K_Initialisierung: TC1-Byte in ATR**

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

⌦ **Card-G2-A_3027 K_Personalisierung und K_Initialisierung: Historical Bytes im ATR**

Das Attribut answerToReset SOLL keine Historical Bytes enthalten. ⌫

⌦ Card-G2-A_2483 K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes

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

5.3 Allgemeine Struktur

Die Abbildung Abb_gSMC-KT-ObjSys_001 zeigt die allgemeine Struktur der gSMC-KT.

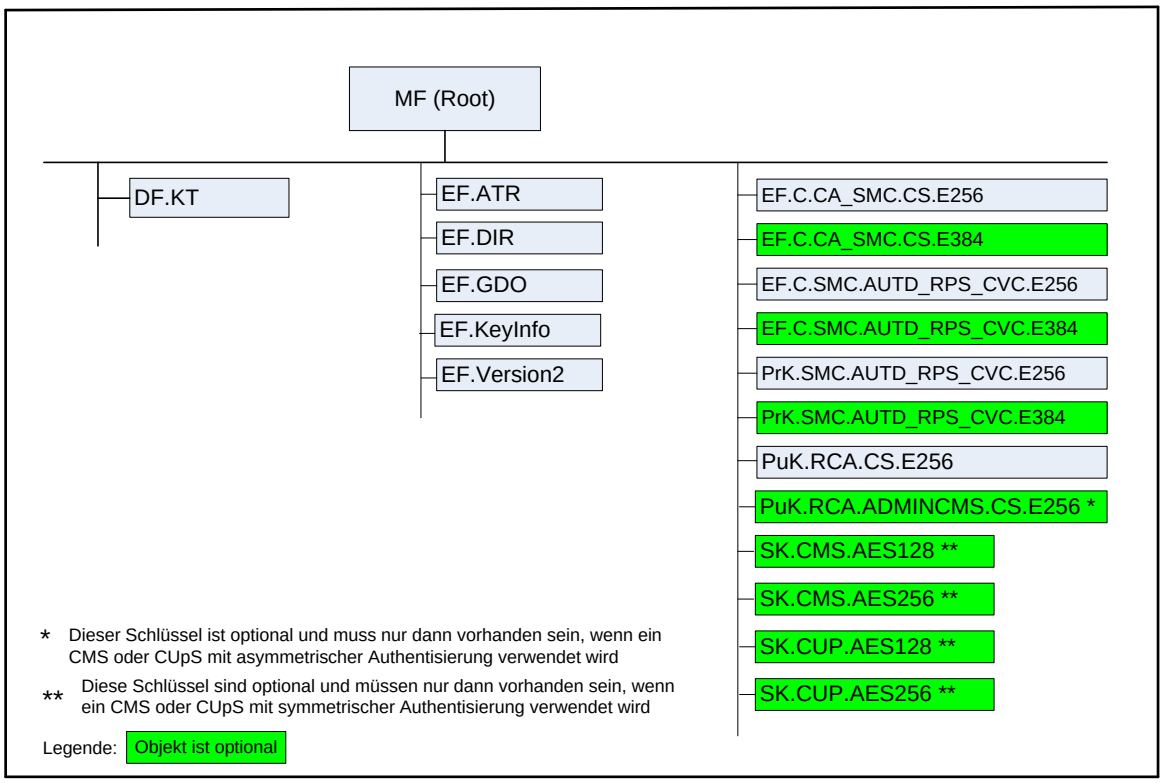

Abbildung 1: Abb_gSMC-KT-ObjSys_001 Objektstruktur einer gSMC-KT auf oberster Ebene

5.4 Root-Anwendung und Dateien auf MF-Ebene

5.4.1 MF

Das MF der gSMC-KT ist ein “Application Dedicated File” (siehe [gemSpec_COS#8.3.1.3]).

⌦ Card-G2-A_2487 Initialisierung: Initialisierte von MF

MF MUSS die in Tab_gSMC-KT_ObjSys_004 dargestellten Attribute besitzen.

Tabelle 3: Tab_gSMC-KT_ObjSys_004 Initialisierte Attribute von MF

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
applicationIdentifier	'D276 0001 4480 03'	
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 (3)
alle	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsbedingung	Bemerkung	
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (1) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (2) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.4 im Allgemeinen irrelevant.

Hinweis (3) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap.5.6

5.4.2 MF / EF.ATR

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

⌦ **Card-G2-A_2488 K_Initialisierung: Initialisierte Attribute von MF / EF.ATR**

EF.ATR MUSS die in Tab_gSMC-KT_ObjSys_005 dargestellten Attribute besitzen.

Tabelle 4: Tab_gSMC-KT_ObjSys_005 Initialisierte Attribute von MF / EF.ATR

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 01'	siehe Hinweis (5)

shortFileIdentifier	'1D'= 29	
numberOfOctet	herstellerspezifisch	
positionLogi-calEndOfFile	Zahl der tatsächlich belegten Oktette	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	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	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

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

⌦ Card-G2-A_3471 K_Initialisierung: Initialisiertes Attribut *numberOfOctet* von MF / EF.ATR

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

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

5.4.3 MF / EF.DIR

Die Datei EF.DIR enthält eine Liste mit Anwendungstemplates gemäß [ISO 7816–4]. Da weder das Nachladen von Anwendungen vorgesehen ist, noch das Löschen bestehender Anwendungen, ist es nicht erforderlich, dass die Liste veränderbar ist.

⌦ **Card-G2-A_2504 K_Initialisierung: Initialisierte Attribute von MF / EF.DIR**

EF.DIR MUSS die in Tab_gSMC-KT_ObjSys_012 dargestellten Attribute besitzen.

Tabelle 5: Tab_gSMC-KT_ObjSys_012 Initialisierte Attribute von MF / EF.DIR

Attribute	Wert	Bemerkung
Objekttyp	linear variables Elementary File	
fileIdentifier	'2F 00'	siehe Hinweis (7)
shortFileIdenfier	'1E'= 30	siehe Hinweis (7)
numberOfOctet	'50' Oktett = 80 Oktett	
maxNumRecords	5 Records	
maxRecordLength	32 Oktette	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
recordList Rekord 1 Rekord 2 …	'61- 09-(4F 07 D2760001448003)' '61- 08-(4F 06 D27600014400)' herstellerspezifisch, falls weitere Anwendungen verfügbar	MF, siehe 5.4 DF.KT, siehe 5.5
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS	siehe Hinweis (9)
READ RECORD SEARCH RECORD	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (6) 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 (7) Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO 7816–4] festgelegt.

Hinweis (8) *Die beiden derzeit definierten Rekords benötigen je 21 Oktette.*

Hinweis (9) *Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.6.*

5.4.4 MF / EF.GDO

In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte enthält.

⌦ **Card-G2-A_2506 K_Initialisierung: Initialisierte Attribute von MF / EF.GDO**

EF.GDO MUSS die in Tab_gSMC-KT_ObjSys_013 dargestellten Attribute besitzen.

Tabelle 6: Tab_gSMC-KT_ObjSys_013 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	
positionLogi-calEndOfFile	Wildcard	c)
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	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (10) *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.*

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

⌦ **Card-G2-A_2507** K_Personalisierung: Personalisiertes Attribut von EF.GDO

Bei der Personalisierung von EF.GDO MÜSSEN die in Tab_gSMC-KT_ObjSys_060 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 7: Tab_gSMC-KT_ObjSys_060 Personalisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
positionLogi-calEndOfFile	'000C' Oktett = 12 Oktett	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	

⌫

5.4.5 MF / EF.KeyInfo

Die Datei EF.KeyInfo enthält die Information darüber, welche Datei- und Schlüsselreferenzen aktuell zu verwenden sind und welches Gültigkeitsende sie haben.

⌦ **Card-G2-A_3453 K_Initialisierung: Attribute von MF / EF.KeyInfo**

EF.KeyInfo MUSS die in Tab_gSMC-KT_ObjSys_059 dargestellten initialisierten Attribute besitzen.

Tabelle 8: Tab_gSMC-KT_ObjSys_059 Initialisierte Attribute von MF / EF.KeyInfo

Attribute	Wert	Bemerkung
Objekttyp	linear fixes Elementary File	
fileIdentifier	'2F 1A'	
shortFileIdentifier	'1A'= 26	
maxNumRecords	30 Rekord	
maxRecordLength	36 Oktett	
flagRecordLCS	False	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
recordList Rekord 1 Rekord 2 … Rekord 30	 'XX…YY' 'XX…YY' …' 'XX…YY	Der Rekordinhalt wir in [gemSpec_Karten_Fach_TIP] festgelegt.
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		

Attribute	Wert	Bemerkung
Zugriffsart	Zugriffsbedingung	Bemerkung
READ RECORD SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT_CMS OR AUT_CUP	siehe Hinweis (12)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

⌫

Hinweis (11) Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate

Hinweis (12) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar

5.4.6 MF / EF.Version2

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

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

Die konkrete Befüllung ist in [gemSpec_Karten_Fach_TIP] beschrieben.

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

⌦ **Card-G2-A_2509 K_Initialisierung: Initialisierte Attribute von MF / EF.Version2**

EF.Version2 MUSS die in Tab_gSMC-KT_ObjSys_014 dargestellten Attribute besitzen.

Tabelle 9: Tab_gSMC-KT_ObjSys_014 Initialisierte Attribute von MF / EF.Version2

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	

fileIdentifier	'2F 11'	
shortFileIdentifier	'11'= 17	
numberOfOctet	'003C' Oktett = 60 Oktett	
positionLogi-calEndOfFile	passend zum Inhalt	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP]	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
UPDATE BINARY SET LOGICAL EOF	AUT_CMS	siehe Hinweis (14)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (13) Kommandos, die gemäß [gemSpec_COS] mit einem linear fixen EF arbeiten, sind: Activate, Activate Record, Append Record Deactivate, Deactivate Record, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Update Record, Terminate

Hinweis (14) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.6

5.4.7 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. Das Zertifikat lässt sich mittels PuK.RCA.CS.E256 (siehe Kapitel 5.4.13.1) prüfen. Der im Zertifikat enthaltene öffentliche Schlüssel dient der Verifizierung von weiteren Zertifikaten, die im Dateisystem enthalten sind (siehe zum Beispiel Kapitel 5.4.9).

⌦ **Card-G2-A_2496 K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E256**

EF.C.CA_SMC.CS.E256 MUSS die in Tab_gSMC-KT_ObjSys_007 dargestellten Attribute besitzen.

Tabelle 10: Tab_gSMC-KT_ObjSys_007 Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 07'	
shortFileIdentifier	'07' = 7	
numberOfOctet	011D' Oktett = 285 Oktett	
positionLogi-calEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	undefiniert	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (16)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (16)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (15) 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 (16) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap.5.6.

⌦ **Card-G2-A_3455 K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.E256**

Bei der Personalisierung von EF.C.CA_SMC.CS.E256 MÜSSEN die in Tab_gSMC-KT_ObjSys_035 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 11: Tab_gSMC-KT_ObjSys_035 Personalisierte Attribute von MF / EF.C.CA_SMC.CS.E256

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

⌫

5.4.8 MF / EF.C.CA_SMC.CS.E384 (Option_lange_Lebensdauer_im_Feld)

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SMC.CS.E384 einer CA enthält. Das Zertifikat lässt sich mittels PuK.RCA.CS.E384 (wird später nachgeladen) prüfen. Der im Zertifikat enthaltene öffentliche Schlüssel dient der Verifizierung von weiteren Zertifikaten, die im Dateisystem enthalten sind (siehe zum Beispiel Kapitel 5.4.10).

⌦ **Card-G2-A_2497 K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E384 (Option_lange_Lebensdauer_im_Feld)**

Die Datei EF.C.CA_SMC.CS.E384 MUSS bei der Ausgabe der gSMC-KT angelegt werden. EF.C.CA_SMC.CS.E384 MUSS die in Tab_gSMC-KT_ObjSys_008 dargestellten Attribute besitzen.

Tabelle 12: Tab_gSMC-KT_ObjSys_008 Initialisierte Attribute von MF / EF.C.CA_SMC.CS.E384

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 0D'	
shortFileIdentifier	'0D' = D	
numberOfOctet	'011D' Oktett = 285 Oktett	
positionLogi-calEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	undefiniert	wird später nachgeladen
Zugriffsregeln		
accessRules	identisch zu EF.C.CA_SMC.CS.E256	

⌫

5.4.9 MF / EF.C.SMC.AUTD_RPS_CVC.E256

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.SMC.AUTD_RPS_CVC.E256 zum zugehörigen privaten Schlüssel (siehe Tab_gSMC-KT_ObjSys_016) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_SMC.CS.E256 (siehe Tab_gSMC-KT_ObjSys_007) prüfen.

⌦ **Card-G2-A_2501 K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256**

EF.C.SMC.AUTD_RPS_CVC.E256 MUSS die in Tab_gSMC-KT_ObjSys_010 dargestellten Attribute besitzen.

Tabelle 13: Tab_gSMC-KT_ObjSys_010 Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 0A'	
shortFileIdentifier	'0A' = 10	
numberOfOctet	'01 1F' Oktett = 287 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	undefiniert	wird personalisiert
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (19)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (19)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (17) 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 (18) Das Zertifikat enthält die Rolle CHAT = Remote PIN Sender (RPS), d.h. in der Flagliste cvc_FlagList_TI ist Flag 54 gesetzt.

Hinweis (19) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

⌦ **Card-G2-A_2500 K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUTD_RPS_CVC.E256**

Für die CHR des Zertifikates MUSS CHR = '000A' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2507].⌫

⌦ **Card-G2-A_3456 K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256**

Bei der Personalisierung von EF.C.SMC.AUTD_RPS_CVC.E256 MÜSSEN die in Tab_gSMC-KT_ObjSys_037 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 14: Tab_gSMC-KT_ObjSys_037 Personalisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00 DE' Oktett = 222 Oktett	
body	C.SMC.AUTD_RPS_CVC.E256 gemäß [gemSpec_PKI]	
body Option_Erstellung_von_Testkarten	C.SMC.AUTD_RPS_CVC.E256 gemäß [gemSpec_PKI] von Test-CVC-CA	

⌫

5.4.10 MF / EF.C.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld)

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.SMC.AUTD_RPS_CVC.E384 zum zugehörigen privaten Schlüssel (siehe Tab_gSMC-KT_ObjSys_017) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_SMC.CS.E384 (siehe Tab_gSMC-KT_ObjSys_008) prüfen.

⌦ **Card-G2-A_2503 K_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld)**

Die Datei F.C.SMC.AUTD_RPS_CVC.E384 muss bei der Ausgabe der gSMC-KT angelegt werden. EF.C.SMC.AUTD_RPS_CVC.E384 MUSS die in Tab_gSMC-KT_ObjSys_011 dargestellten Attribute besitzen.

Tabelle 15: Tab_gSMC-KT-ObjSys_011 Initialisierte Attribute von MF / EF.C.SMC.AUTD_RPS_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 0F'	
shortFileIdentifier	'0F' = 15	
numberOfOctet	'01 1F' Oktett = 287 Oktett	
positionLogi-calEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)"	
shareable	True	
body	undefiniert	wird später nachge-laden
Zugriffsregeln		
accessRules	identisch zu EF.C.SMC.AUTD_RPS_CVC.E256	

⌫

⌦ **Card-G2-A_2502 K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld)**

Für die CHR des Zertifikates MUSS CHR = '000F' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS wie das Wertfeld *body* aus [Card-G2-A_2507].⌫

5.4.11 MF / PrK.SMC.AUTD_RPS_CVC.E256

Dieser Schlüssel wird für die Kryptographie mit elliptischen Kurven im Rahmen von asymmetrischen Authentisierungsprotokollen verwendet. Der zugehörige öffentliche Schlüssel befindet sich in einem CV-Zertifikat, das in der Datei EF.C.SMC.AUTD_RPS_CVC.E256 gespeichert ist (siehe Kapitel 5.4.9).

⌦ **Card-G2-A_2511 K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256**

PrK.SMC.AUTD_RPS_CVC.E256 MUSS die in Tab_gSMC-KT_ObjSys_016 dargestellten Attribute besitzen.

Tabelle 16: Tab_gSMC-KT_ObjSys_016 Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt ELC 256	
keyIdentifier	'0A' = 10	
privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	

keyAvailable	WildCard	
numberScenario	0	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]#16.1 {elcAsynchronAdmin, elcSessionkey4TC, elcSessionkey4SM}	
accessRulesSessionkeys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung= AUT(flagTI.53)	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
DEACTIVATE	AUT_CMS OR AUT_CUP	siehe Hinweis (21)
ACTIVATE	ALWAYS AUT_CMS OR AUT_CUP	
GENERATE ASYMMETRIC KEY PAIR P1=‘81’	ALWAYS	
GENERATE ASYMMETRIC KEY PAIR P1=´C4´ ODER P1=’C0’	AUT_CMS OR AUT_CUP	
GENERAL AUTHENTICATE	ALWAYS	siehe Hinweis (22) siehe Hinweis (23)
DELETE	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (20) 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 (21) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

Hinweis (22) Diese Rolle ist einem Gerät für Stapel- und Komfortsignatur zugewiesen. Dabei wird die PIN.QES des "Remote"-Gerätes dorthin übertragen.

Hinweis (23) *Diese Rolle ist einem Remote-PIN-Empfänger zugewiesen.*

⌦ **Card-G2-A_3457 K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256**

Bei der Personalisierung von PrK.SMC.AUTD_RPS_CVC.E256 MÜSSEN die in Tab_gSMC-KT_ObjSys_042 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 17: Tab_gSMC-KT_ObjSys_042 Personalisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
privateElcKey	keyData = Wildcard	

⌫

5.4.12 MF / PrK.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld)

Dieser Schlüssel wird für die Kryptographie mit elliptischen Kurven im Rahmen von asymmetrischen Authentisierungsprotokollen verwendet. Der zugehörige öffentliche Schlüssel befindet sich in einem CV-Zertifikat, das in der Datei EF.C.SMC.AUTD_RPS_CVC.E384 gespeichert ist (siehe Kapitel 5.4.10).

⌦ **Card-G2-A_2512 K_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E384 (Option_lange_Lebensdauer_im_Feld)**

PrK.SMC.AUTD_RPS_CVC.E384 MUSS die in Tab_gSMC-KT_ObjSys_017 dargestellten Attribute besitzen.

Tabelle 18: Tab_gSMC-KT_ObjSys_017 Initialisierte Attribute von MF / PrK.SMC.AUTD_RPS_CVC.E384

Attribute	Wert	Bemerkung
Objekttyp	privates ELC Schlüsselobjekt	
keyIdentifier	'0F' = 15	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
numberScenario	0	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]#16.1 { elcAsynchronAdmin, elcSessionkey4TC, elcSessionkey4SM }	
accessRulesSessionkeys	Für alle logischen LCS Werte gilt Zugriffsart= PSO → Zugriffsbedingung=	

	AUT(flagTI.53)	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SMC.AUTD_RPS_CVC.E256	

⌫

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

5.4.13 Sicherheitsanker zum Import von CV-Zertifikaten

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

5.4.13.1 MF / PuK.RCA.CS.E256

Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA für die Kryptographie mit elliptischen Kurven, welche an der Wurzel der CVC-Hierarchie steht. Der öffentliche Schlüssel dient der Überprüfung von Zertifikaten, welche von dieser Root-CA ausgestellt wurden (siehe zum Beispiel Kapitel 5.4.3).

⌦ **Card-G2-A_2514 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**

PuK.RCA.CS.E256 MUSS die in Tab_gSMC-KT_ObjSys_019 dargestellten Attribute besitzen.

Tabelle 19: Tab_gSMC-KT_ObjSys_019 Initialisierte Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Signaturprüfobjekt	
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	E 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]	
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP[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}	
CHAT	• $OIDf_{lags}$ = oid_cvc_fl_ti • flagList = 'FF 0084 2006 07C4'	siehe Hinweis (27)
lifeCycleStatus	„Operational state (activated)"	
accessRulesPublic SignatureVerificationObject.	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE → AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublic AuthenticationObject	Für alle Interfaces und alle Werte von lifeCycleStatus gilt: DELETE → ALWAYS EXTERNAL AUTHENTICATE → ALWAYS GENERAL AUTHENTICATE → ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (26)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)

⌫

Hinweis (25) Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: PSO Verify Certificate, TERMINATE.

Hinweis (26) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

Hinweis (27) Während gemäß den Tabellen in [gemSpec_COS]#H.4] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten auf ‚0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ‚1' gesetzt.

⌦ **Card-G2-A_3275 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_gSMC-KT_ObjSys_058 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-KT_ObjSys_019 personalisiert werden.

Tabelle 20: Tab_gSMC-KT_ObjSys_058 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Attribute	Wert	Bemerkung
publicKey	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test-CVC-CA	personalisieren gemäß [gemSpec_TK#3.1.2]
keyIdentifier	E 256 Root-CA-Kennung (5 Bytes) || Erweiterung (3 Bytes); Wert gemäß keyIdentifier des personalisierten Schlüssels	
CHAT	• OIDflags = oid_cvc_fl_ti • flagList = 'FF 0084 2006 07C4'	
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels	

⌫

5.4.14 Asymmetrische Kartenadministration

Die hier beschriebene optionale Variante der Administration der gSMC-KT betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-KT.

Die Administration einer gSMC-KT 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 5.4.15 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.

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

5.4.14.1 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_3028 K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab_gSMC-KT_ObjSys_031 dargestellten Attribute besitzen.

Tabelle 21: Tab_gSMC-KT_ObjSys_031 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches Signaturprüfobjekt, ELC 256	
Für Echtkarten MÜSSEN die beiden folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die beiden folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
CHAT	▪ OID_{flags} = oid_cvc_fl_cms ▪ flagList = 'FF BFFF FFFF FFFF'	siehe Hinweis (29)
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 Life Cycle State und in SE#1 gilt: DELETE → AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublicAuthenticationObject.	Für alle Life Cycle State und in SE#1 gilt: DELETE → ALWAYS GENERAL AUTHENTICATE → ALWAYS	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)" kontaktbehaftet		
PSO Verify Certificate	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (30)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state" kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

⌫

Hinweis (28) Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind:
ACTIVATE, DEACTIVATE, DELETE, PSO Verify Certificate, TERMINATE

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.

Hinweis (30) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap.5.6.

⌦ **Card-G2-A_3458 K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**

Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 die in Tab_gSMC-KT_ObjSys_044 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_gSMC-KT_ObjSys_031 personalisiert werden.

Tabelle 22: Tab_gSMC-KT_ObjSys_044 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

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

⌫

5.4.15 Symmetrische Kartenadministration

Die hier beschriebene optionale Variante der Administration einer gSMC-KT betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-KT.

Die Administration einer gSMC-KT 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 5.4.14 beschrieben.

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

Während die Schlüssel auf Smartcards typischerweise kartenindividuell sind, ist es denkbar, dass mit einem Schlüssel eines administrierenden Systems genau eine, oder mehre-

re oder alle Smartcards administriert werden. Das Sicherheitskonzept des administrierenden Systems erscheint die geeignete Stelle zu sein um eine Variante auszuwählen.

5.4.15.1 MF / SK.CMS.AES128

SK.CMS.AES128 (optional) ist der geheime Schlüssel für die Durchführung des SMC-KT / CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.

⌦ **Card-G2-A_2518 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128**

SK.CMS.AES128 MUSS die in Tab_gSMC-KT_ObjSys_023 dargestellten Attribute besitzen.

Tabelle 23: Tab_gSMC-KT_ObjSys_023 Initialisierte Attribute von MF / SK.CMS.AES128

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'14' = 20	
encKey	undefiniert	wird personalisiert
macKey	undefiniert	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	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (32)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	siehe Hinweis (2)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

⌫

Hinweis (31) 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 (32) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

⌦ **Card-G2-A_3459 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 MÜSSEN die in Tab_gSMC-KT_ObjSys_045 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 24: Tab_gSMC-KT_ObjSys_045 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]	

⌫

5.4.15.2 MF / SK.CMS.AES256

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

⌦ **Card-G2-A_2519 K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256**

SK.CMS.AES256 MUSS die in Tab_gSMC-KT_ObjSys_024 dargestellten Attribute besitzen.

Tabelle 25: Tab_gSMC-KT_ObjSys_024 Initialisierte Attribute von MF / SK.CMS.AES256

Attribute	**Wert**	**Bemerkung**
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	‘18’ = 24	
encKey	undefiniert	wird personalisiert
macKey	undefiniert	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	

⌫

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.

⌦ **Card-G2-A_3460 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_gSMC-KT_ObjSys_046 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 26: Tab_gSMC-KT_ObjSys_046 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]	

⌫

5.4.15.3 MF / SK.CUP.AES128

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

⌦ **Card-G2-A_3461 K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128**

SK.CUP.AES128 MUSS die in Tab_gSMC-KT_ObjSys_054 dargestellten Initialisierten Attribute besitzen.

Tabelle 27: Tab_gSMC-KT_ObjSys_054 Initialisierte Attribute von MF / SK.CUP.AES128

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-128	
keyIdentifier	'03' = 3	
lifeCycleStatus	„Operational state (activated)“	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	

⌫

⌦ **Card-G2-A_3462 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_gSMC-KT_ObjSys_055 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 28: Tab_gSMC-KT_ObjSys_055 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]	

⌫

5.4.15.4 MF / SK.CUP.AES256

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

⌦ **Card-G2-A_3463 K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256**

SK.CUP.AES256 MUSS die in Tab_gSMC-KT_ObjSys_056 dargestellten initialisierten Attribute besitzen.

Tabelle 29: Tab_gSMC-KT_ObjSys_056 Initialisierte Attribute von MF / SK.CUP.AES256

Attribute	Wert	Bemerkung
Objekttyp	Symmetrisches Authentisierungsobjekt	
keyType	AES-256	
keyIdentifier	'04' = 4	
lifeCycleStatus	„Operational state (activated)“	
encKey	…	wird personalisiert
macKey	…	wird personalisiert
numberScenario	0	
algorithmIdentifier	aesSessionkey4SM, siehe [gemSpec_COS]	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln		
accessRules	identisch zu SK.CMS.AES128	

⌫

⌦ **Card-G2-A_3464 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_gSMC-KT_ObjSys_057 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 30: Tab_gSMC-KT_ObjSys_057 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]	

⌫

5.5 MF / DF.KT (Kartenterminalanwendung)

5.5.1 Dateistruktur und Dateiinhalt

DF.KT wird verwendet für:

- die Authentisierung zur Anbindung des Kartenterminals an einen bestimmten Konnektor.

Die folgende Abbildung zeigt die Dateistruktur von DF.KT

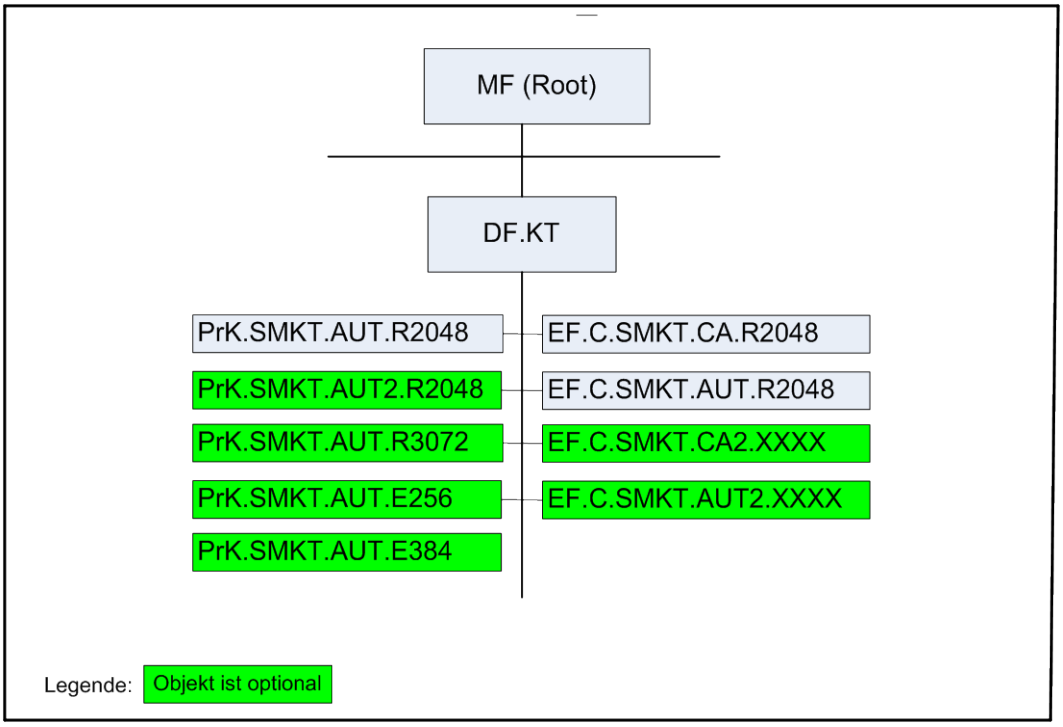

Abbildung 2: Abb_gSMC-KT-ObjSys_002 Dateistruktur von DF.KT

Es MUSS möglich sein, die Funktionalität von DF.KT in mehr als einem logischen Kanal zu nutzen, d. h. die von DF.KT bereitgestellten Funktionen MÜSSEN parallel nutzbar sein.

⌦ **Card-G2-A_2522 K_Initialisierung: Initialisierte Attribute von MF / DF.KT**

DF.KT MUSS die in Tab_gSMC-KT_ObjSys_025 dargestellten Attribute besitzen.

Tabelle 31: Tab_gSMC-KT_ObjSys_025 Initialisierte Attribute von MF / DF.KT

Attribute	Wert	Bemerkung
Objekttyp	Ordner	

applicationIdentifier	'D276000144 00'	
fileIdentifier	–	
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 (36)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	siehe Hinweis (35)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

⌫

Hinweis (34) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind: ACTIVATE, DEACTIVATE, DELETE, FINGERPRINT, LIST PUBLIC KEY, LOAD APPLICATION, SELECT, TERMINATE DF.

Hinweis (35) Es ist möglich, dass die Kartenterminalanwendung DF.KT in einer anderen Komponente als gSMC-KT installiert ist. Dort ist es denkbar, dass das übergeordnete Verzeichnis deaktivierbar ist. Deshalb ist dieser Zustand für Objekte im Kapitel 5.5 zu berücksichtigen.

Hinweis (36) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.6.

5.5.2 MF / DF.KT / EF.C.SMKT.CA.R2048

Die Datei EF.C.SMKT.CA.R2048 enthält ein X.509-Zertifikat C.SMKT.CA.R2048 für die Kryptographie mit RSA, welches den öffentlichen Schlüssel PuK.SMKT.CA.R2048 enthält. Dieser Schlüssel ist dazu geeignet, dass in EF.C.SMKT.AUT.R2048 (siehe Kapitel 5.5.3) gespeicherte Zertifikat zu prüfen.

⌦ **Card-G2-A_2523 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048**

EF.C.SMKT.CA.R2048 MUSS die in Tab_gSMC-KT_ObjSys_026 dargestellten Attribute besitzen.

Tabelle 32: Tab_gSMC-KT_ObjSys_026 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	

fileIdentifier	'C5 02'	
shortFileIdentifier	'02'= 2	
numberOfOctet	'08 02' Oktett = 2050 Oktett	
positionLogi-calEndOfFile	'0'	wird personalisiert
flagTransaction-Mode	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 (38)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (38)
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	NEVER	siehe Hinweis (38)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
Andere	NEVER	

⌫

Hinweis (37) 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 (38) Es ist möglich, dass die Kartenterminalanwendung DF.KT in einer anderen Komponente als gSMC-KT installiert ist. Dort ist es denkbar, dass das übergeordnete Verzeichnis deaktivierbar ist. Deshalb ist dieser Zustand für Objekte im Kapitel 5.5 zu berücksichtigen.

Hinweis (39) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

⌦ **Card-G2-A_3465 K_Personalisierung: Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048**

Bei der Personalisierung von EF.C.SMKT.CA.R2048 MÜSSEN die in Tab_gSMC-KT_ObjSys_047 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 33: Tab_gSMC-KT_ObjSys_047 Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048

Attribute	Wert	Bemerkung
positionLogi-calEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.SMKT.CA.R2048 gemäß [gemSpec_PKI]	

⌫

5.5.3 MF / DF.KT / EF.C.SMKT.AUT.R2048

Die Datei EF.C.SMKT.AUT.R2048 enthält ein X.509-Zertifikat C.SMKT.AUT.R2048 für die Kryptographie mit RSA, welches den öffentlichen Schlüssel PuK.SMKT.AUT.R2048 zum privaten Schlüssel PrK.SMKT.AUT.R2048 (siehe Kapitel 5.5.4) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.SMKT.CA.R2048 (siehe Kapitel 5.5.2) prüfen.

Dieses Zertifikat, der darin enthaltene öffentliche Schlüssel sowie der zugehörige private Schlüssel werden beim Pairing des Kartenterminals mit dem Konnektor und zur sicheren Identifikation und Authentisierung des Kartenterminals durch den Konnektor verwendet.

⌦ **Card-G2-A_2526 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048**

EF.C.SMKT.AUT.R2048 MUSS die in Tab_gSMC-KT_ObjSys_027 dargestellten Attribute besitzen.

Tabelle 34: Tab_gSMC-KT_ObjSys_027 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	‘C5 01’	
shortFileIdentifier	‘01’= 1	
numberOfOctet	‘08 02’ Oktett = 2050 Oktett	
positionLogi-calEndOfFile	’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 (41)

READ BINARY	ALWAYS	
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	NEVER	siehe Hinweis (41)
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

⌫

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) Es ist möglich, dass die Kartenterminalanwendung DF.KT in einer anderen Komponente als gSMC-KT installiert ist. Dort ist es denkbar, dass das übergeordnete Verzeichnis deaktivierbar ist. Deshalb ist dieser Zustand für Objekte im Kapitel 5.5 zu berücksichtigen.

Hinweis (42) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.6.

⌦ **Card-G2-A_3466 K_Personalisierung: Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048**

Bei der Personalisierung von EF.C.SMKT.AUT.R2048 MÜSSEN die in Tab_gSMC-KT_ObjSys_049 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 35: Tab_gSMC-KT_ObjSys_049 Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette	
body	C.SMKT.AUT.R2048 gemäß [gemSpec_PKI	

⌫

5.5.4 MF / DF.KT / PrK.SMKT.AUT.R2048

PrK.SMKT.AUT.R2048 ist der private Authentisierungsschlüssel zur Anbindung des Kartenterminals an einen bestimmten Konnektor.

⌦ **Card-G2-A_2529 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048**

PrK.SMKT.AUT.R2048 MUSS die in Tab_gSMC-KT_ObjSys_028 dargestellten Attribute besitzen.

Tabelle 36: Tab_gSMC-KT_ObjSys_028 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
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]#16.1 sign9796_2_DS2, signPKCS1_V1_5, signPSS	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregel für logischen LCS „Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
DEACTIVATE	AUT_CMS OR AUT_CUP	
ACTIVATE	ALWAYS AUT_CMS OR AUT_CUP	herstellerspezifisch ist eine der beiden Varianten erlaubt
GENERATE ASYMMETRIC KEY PAIR P1=´C4´ oder P1='C0'	AUT_CMS OR AUT_CUP	siehe Hinweis (43)
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
PSO COMPUTE DIGITALSIGNATURE	ALWAYS	
TERMINATE	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)"		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE	AUT_CMS OR AUT_CUP	
DEACTIVATE	NEVER AUT_CMS OR AUT_CUP	herstellerspezifisch ist eine der beiden Varianten erlaubt
andere	NEVER	
Zugriffsregel für logischen LCS „Termination state"		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

⌫

Hinweis (43) 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 (44) Es ist möglich, dass die Kartenterminalanwendung DF.KT in einer anderen Komponente als gSMC-KT installiert ist. Dort ist es denkbar, dass das übergeordnete Verzeichnis deaktivierbar ist. Deshalb ist dieser Zustand für Objekte im Kapitel 5.5 zu berücksichtigen.

Hinweis (45) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

⌦ **Card-G2-A_3467 K_Personalisierung: Personalisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048**

Bei der Personalisierung von PrK.SMKT.AUT.R2048 MÜSSEN die in Tab_gSMC-KT_ObjSys_051 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 37: Tab_gSMC-KT_ObjSys_051 Personalisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048

Attribute	Wert	Bemerkung
privateKey	Schlüssel mit Moduluslänge 2048 Bit	
keyAvailable	True	

⌫

5.5.5 MF / DF.KT / EF.C.SMKT.CA2.XXXX (Option_lange_Lebensdauer_im_Feld)

Die Datei EF.C.SMKT.CA2.XXXX enthält das X.509-Zertifikat der Zertifizierungsinstanz, die das X.509-Zertifikat C.SMKT.AUT2.XXXX ausgegeben hat.

⌦ **Card-G2-A_2524 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.XXXX (Option_lange_Lebensdauer_im_Feld)**

Das Objekt EF.C.SMKT.CA2.XXXX MUSS bei der Ausgabe der gSMC-KT mit den in Tab_gSMC-KT_ObjSys_032 dargestellten Attributen angelegt werden.

Tabelle 38: Tab_gSMC-KT_ObjSys_032 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA2.XXXX

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	’C5 03’	
shortFileIdentifier	‘03’= 3	
numberOfOctet	‘08 02’ Oktett = 2050 Oktett	
positionLogi-	’0’	wird später nachge-

calEndOfFile		laden
flagTransaction-Mode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird beim Nachladen eingetragen
Zugriffsregel für logischen LCS „Operational state (activated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (47)
READ BINARY	ALWAYS	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (47)
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)”		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	NEVER	siehe Hinweis (38)
Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Andere	NEVER	

⌫

Hinweis (46) 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 (47) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.6.

5.5.6 MF / DF.KT / EF.C.SMKT.AUT2.XXXX (Option_lange_Lebensdauer_im_Feld)

Die Datei EF.C.SMKT.AUT2.XXXX muss bei der Ausgabe der gSMC-KT angelegt werden. Die zu den jeweiligen Verfahren gehörenden privaten Schlüsselobjekte sind in den Kapiteln 5.5.7, 5.5.8, 5.5.9 und 5.5.10 zu finden.

⌦ **Card-G2-A_2527 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.XXXX (Option_lange_Lebensdauer_im_Feld)**

Das Objekt EF.C.SMKT.AUT.XXXX MUSS bei der Ausgabe der gSMC-KT mit den in Tab_gSMC-KT_ObjSys_033 dargestellten Attributen angelegt werden.

Tabelle 39: Tab_gSMC-KT_ObjSys_033 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.XXXX

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	’C5 04’	
shortFileIdentifier	‘04’= 4	
numberOfOctet	‘08 02’ Oktett = 2050 Oktett	
positionLogi-calEndOfFile	’0’	wird später nachge-laden
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird beim Nachladen eingetragen
Zugriffsregeln		
accessRules	identisch zu EF.C.SMKT.CA.XXXX	

⌫

Hinweis (48) 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.

5.5.7 MF / DF.KT / PrK.SMKT.AUT2.R2048 (Option_lange_Lebensdauer_im_Feld)

PrK.SMKT.AUT2.R2048 ist der private Authentisierungsschlüssel für die Kryptographie mit RSA zur Anbindung des Kartenterminals an einen bestimmten Konnektor. Er wird mit dem Kommando Generate Asymmetric Key Pair generiert, wenn die Gültigkeitsdauer des Schlüssels PrK.SMKT.AUT.R2048 und die Kryptograohie mit R2048 weiter genutzt werden soll.

⌦ **Card-G2-A_3468 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT2.R2048 (Option_lange_Lebensdauer_im_Feld)**

PrK.SMKT.AUT2.R2048 MUSS die in Tab_gSMC-KT_ObjSys_061 dargestellten Attribute besitzen.

Tabelle 40: Tab_gSMC-KT_ObjSys_061 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT2.R2048

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	

keyIdentifier	'05' = 5	
privateKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]#16.1 sign9796_2_DS2, signPKCS1_V1_5, signPSS	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregeln		
accessRules	identisch zu PrK.SMKT.AUT.R2048	

⌫

Hinweis (49) 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

5.5.8 MF / DF.KT / PrK.SMKT.AUT.R3072 (Option_lange_Lebensdauer_im_Feld)

PrK.SMKT.AUT.R3072 ist der private Authentisierungsschlüssel für die Kryptographie mit RSA zur Anbindung des Kartenterminals an einen bestimmten Konnektor.

⌦ **Card-G2-A_2530 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R3072 (Option_lange_Lebensdauer_im_Feld)**

PrK.SMKT.AUT.R3072 MUSS die in Tab_gSMC-KT_ObjSys_029 dargestellten Attribute besitzen.

Tabelle 41: Tab_gSMC-KT_ObjSys_029 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R3072

Attribute	Wert	Bemerkung
Objekttyp	privates RSA Schlüsselobjekt	
keyIdentifier	'03' = 3	
privateKey	herstellerspezifisch „unbefüllt", Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 3072 Bit	wird später mit Generate Asymmetric Key Pair erzeugt
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]#16.1 sign9796_2_DS2, signPKCS1_V1_5, signPSS	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregeln		

accessRules	identisch zu PrK.SMKT.AUT.R2048	

⌫

Hinweis (50) 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

5.5.9 MF / DF.KT / PrK.SMKT.AUT.E256 (Option_lange_Lebensdauer_im_Feld)

PrK.SMKT.AUT.E384 ist der private Authentisierungsschlüssel für die Kryptographie mit mit elliptischen Kurven zur Anbindung des Kartenterminals an einen bestimmten Konnektor.

⌦ **Card-G2-A_3469 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E256 (Option_lange_Lebensdauer_im_Feld)**

PrK.SMKT.AUT.E256 MUSS die in Tab_gSMC-KT_ObjSys_062 dargestellten Attribute besitzen.

Tabelle 42: Tab_gSMC-KT_ObjSys_062 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt ELC 256	
keyIdentifier	‘06’ = 6	
privateElcKey	domainparameter = brainpoolP256r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]#16.1 {signECDSA}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln		
accessRules	identisch zu PrK.SMKT.AUT.R2048	

⌫

Hinweis (51) 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 (52) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

5.5.10 MF / DF.KT / PrK.SMKT.AUT.E384 (Option_lange_Lebensdauer_im_Feld)

PrK.SMKT.AUT.E384 ist der private Authentisierungsschlüssel für die Kryptographie mit mit elliptischen Kurven zur Anbindung des Kartenterminals an einen bestimmten Konnektor.

⌦ **Card-G2-A_2531 K_Initialisierung: Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E384 (Option_lange_Lebensdauer_im_Feld)**

PrK.SMKT.AUT.E384 MUSS die in Tab_gSMC-KT_ObjSys_030 dargestellten Attribute besitzen.

Tabelle 43: Tab_gSMC-KT_ObjSys_030 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E384

Attribute	Wert	Bemerkung
Objekttyp	Schlüsselobjekt ELC 384	
keyIdentifier	'04' = 4	
privateElcKey	domainparameter = brainpoolP384r1	wird später mit Generate Asymmetric Key Pair erzeugt
privateElcKey	keyData = AttributNotSet	
keyAvailable	False	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS]#16.1 {signECDSA}	
lifeCycleStatus	„Operational state (activated)"	
Zugriffsregeln		
accessRules	identisch zu PrK.SMKT.AUT.R2048	

⌫

Hinweis (53) 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

5.6 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der gSMC-KT

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 gSMC-KT von einem Card Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CMS optional. Die Inhalte des Kapitels 13 in [gemSpec_COS] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe der gSMC-KT durchgeführt werden müssen.

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AID	Application Identifier
CHA	Certificate Holder Autorisation
CHAT	Certificate Holder Autorisation Template
CMS	Card Management System
COS	Chip card Operating System, Betriebssystem einer Chipkarte
CUP	Certificate Update
DER	Distinguished Encoding Rules, siehe [ISO8825–1]
DF	Dedicated File, Ordner
DO	Datenobjekt bestehend aus Tag, Länge und Wert
EF	Elementary File, Datei
ELC	Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven
FID	File Identifier
LCS	Life Cycle Status
MF	Master File, Wurzelverzeichnis
PrK	Private Key, privater Teil eines asymmetrischen Schlüsselpaares
PuK	Public Key, öffentlicher Teil eines Schlüsselpaares
SE#1	Security Environment Number 1, Sicherheitsumgebung mit der Nummer 1
SFI	Short File Identifier

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_COS]	gematik: Spezifikation COS Spezifikation der elektrischen Schnittstelle
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in 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_SMC_OPT]	gematik: Gemeinsame optische Merkmale der SMC
[gemSpec_TK]	gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO 3166]	ISO/IEC 3166-1:1997 Codes for the representations of names of countries
[ISO 7816–4]	ISO/IEC 7816–4: 2005 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ISO8825–1]	ISO/IEC 8825-1: 1995 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf
[EN 1867]	EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers DIN EN 1867:1997 Maschinenlesbare Karten – Anwendungen im Gesundheitswesen –

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Benummerungssystem und Registrierungsverfahren für Kartenausgeberschlüssel
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[SD5]	ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2007-09-28 Register of IC manufacturers http://sit.sit.fraunhofer.de/_karten_ident/SIT/pdfs/IC_manufacturer_ISO_SD5_28.9.2007.pdf